Model theory and algebra of positive characteristic Hahn fields



Victor Lisinski

Corpus Christi College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Michaelmas 2021

Tillägnad Ruben Elliot
för att just du kom till just oss.

Acknowledgements

This research would not have been possible without the help and support from many people. First of all, I wish to thank my supervisor Jochen Koenigsmann for introducing me to this topic of research and for continued guidance and proofreading throughout the work. I also wish to thank my supervisor Ehud Hrushovski for insightful comments, in particular for suggesting to use the work on finite automata. The junior members of the logic group have provided a friendly and encouraging environment to which I am very grateful. In particular, I thank Konstantinos Kartas for many fruitful discussions and insightful remarks. I am also thankful to Sebastian Eterović, Viktor Henriksson and Brian Tyrrell for proofreading at a late stage of the thesis. My doctoral studies was made possible thanks to the financial support from the Engineering and Physical Sciences Research Council, Corpus Christi College Oxford, and the Royal Swedish Academy of Sciences, for which I am very grateful. Finally, I thank Elsa Gomis for our journey together, in life and academia.

Abstract

This thesis mainly explores model theoretic and algebraic properties of positive characteristic Hahn fields. We show that any positive characteristic tame Hahn field $\mathbb{F}((t^{\Gamma}))$ containing t is decidable in $\mathcal{L}_t$, the language of valued fields with a constant symbol for t, if $\mathbb{F}$ and Γ are decidable. In particular, we obtain decidability of $\mathbb{F}_p((t^{1/p^{\infty}}))$ and $\mathbb{F}_p((t^{\mathbb{Q}}))$ in $\mathcal{L}_t$. This uses a new AKE-principle for equal characteristic tame fields in $\mathcal{L}_t$, building on work by Kuhlmann, together with Kedlaya's work on finite automata and algebraic extensions of function fields. In the process, we obtain an AKE-principle for tame fields in mixed characteristic and extend a theorem by Rayner on the relative algebraic closure of function fields inside Hahn fields. Furthermore, for any Hahn field containing $\mathbb{F}_p((t))$, we use an approximation method described originally by Lampert to obtain a bound on the order type of elements that are algebraic over $\mathbb{F}_p((t))$.

Contents

1 Introduction **1**

1.1 Background and motivation 1

1.2 New results 2

1.3 Preliminaries 4

1.3.1 Valued fields 4

1.3.2 Algorithms, languages and model theory 7

1.3.3 Hahn fields 11

1.3.4 Additive polynomials 13

1.3.5 Kaplansky fields 14

1.3.6 Tame fields 18

1.3.7 Finite automata 21

1.3.8 Arithmetic of finite automata through an example 39

2 Algebraicity of generalised power series **42**

2.1 On the support of algebraic elements 42

2.1.1 Approximating roots 43

2.1.2 Order type of the support of algebraic elements 48

2.1.3 A result by Rayner 51

2.2 A note on Diophantine approximation in Hahn fields 54

3 The $\mathcal{L}_t$-theories of tame Hahn fields **56**

3.1 An AKE-principle for tame fields in $\mathcal{L}_t$ 56

3.2 Decidability of $\mathbb{F}((t^{1/p^\infty}))$ 61

3.3 Decidability of general positive characteristic tame Hahn fields 64

Bibliography **66**

Chapter 1

Introduction

1.1 Background and motivation

In [Hil00], Hilbert posed twenty-three problems that still today continue to greatly influence the directions of mathematics. This research project is related to Hilbert's tenth problem, which originated with work by Diophantus in the 3$^{\text{rd}}$ century. In its modern formulation, Hilbert's tenth problem asks to find a general algorithm that, for any polynomial equation over the integers, determines whether or not it has an integer-valued solution.

The combined work of Davis, Putnam & Robinson [DPR61] and Matiyasevich [Mat70] has established that Hilbert's original tenth problem is not solvable, because no such algorithm can exist. However, one can now pose the same question over domains other than the integers. In many cases we still do not know if the problem is solvable or not. The general form for Hilbert's tenth problem is then as follows, with S being a subset of a ring R.

H10 for R over S
Is there a general algorithm that, for any polynomial equation in several variables over S, determines whether or not the equation has a solution of elements in R?

With this formulation, Hilbert's original problem is H10 for $\mathbb{Z}$ over $\mathbb{Z}$. One of the most notable unsolved questions versions is whether or not H10 for $\mathbb{Q}$ over $\mathbb{Z}$ has a positive answer. For a review of Hilbert's tenth problem in its original and subsequent versions, see [Koe14].

This thesis takes its start from another major unsolved version of Hilbert's tenth problem, namely H10 for $\mathbb{F}_p((t))$ over $\mathbb{F}_p[t]$, where $\mathbb{F}_p((t))$ is the field of formal Laurent series over $\mathbb{F}_p$. This field arises naturally in number theory as the unique local field

of characteristic p with residue field $\mathbb{F}_p$, as shown in [Ser79]. That H10 for $\mathbb{F}_p((t))$ over $\mathbb{F}_p[t]$ remains open stands in stark contrast to the mixed characteristic analogue $\mathbb{Q}_p$, for which decidability is known thanks to the work by Ax and Kochen [AK65b] and, independently, Ershov [Ers65]. This is particularly puzzling since the first order theory of $\mathbb{F}_p((t))$ is asymptotically equal to that of the p-adic numbers $\mathbb{Q}_p$, in a sense made precise in [AK65a]. However, some recent progress has been made. Denef and Shoutens showed that H10 for $\mathbb{F}_p((t))$ over $\mathbb{F}_p[t]$ is answered in the positive, assuming resolution of singularities in characteristic p [DS03]. Anscombe and Fehm showed that H10 for $\mathbb{F}_p((t))$ over $\mathbb{F}_p$ has an unconditional positive answer [AF16]. The latter work uses the results by [Kuh16] on the model theory of tame fields, in particular decidability of the Hahn field $\mathbb{F}_p((t^{\mathbb{Q}}))$ in the language of valued fields $\mathcal{L}_{\text{val}}$, and the fact that finite extensions of $\mathbb{F}_p((t))$ inside $\mathbb{F}_p((t^{\mathbb{Q}}))$ are isomorphic to $\mathbb{F}_p((t))$ itself.

1.2 New results

The important connection between the first order theories of $\mathbb{F}_p((t))$ and $\mathbb{F}_p((t^{\mathbb{Q}}))$ in the language of valued fields served as a motivation to this thesis for looking more closely at the first order theory of $\mathbb{F}_p((t^{\mathbb{Q}}))$ in $\mathcal{L}_t$, the language of valued fields together with a distinguished constant symbol for t. A first step to establish a similar connection in this language is to characterise the $\mathcal{L}_t$-theory of $\mathbb{F}_p((t^{\mathbb{Q}}))$, and more generally of equal characteristic tame valued fields containing $\mathbb{F}_p(t)$. To arrive at such a characterisation in Chapter 3, we will first devote Chapter 2 to purely algebraic results on the relative algebraic closure of function fields, and their completions, in Hahn fields. More precisely, we use an approximation procedure by Lampert [Lam86] to show that the support of such elements has bounded ramification away from the characteristic (reproving a result by Rayner), and bounded order type. In particular, we obtain an abundance of elements in $\mathbb{F}_p((t^{\mathbb{Q}}))$ that are transcendental over $\mathbb{F}_p((t))$.

In Chapter 3, we will then show the following.

Theorem 1.2.1. *Let $\mathbb{F}$ be a perfect field of characteristic p which is decidable in the language of rings and let Γ be a p-divisible ordered abelian group that is decidable in the language of ordered groups with a distinguished constant symbol 1. Then $\mathbb{F}((t^{\Gamma}))$ is decidable in $\mathcal{L}_t$.*

In particular, this gives a positive answer to H10 for $\mathbb{F}_p((t^{\mathbb{Q}}))$ over $\mathbb{F}_p[t]$. It should be noted that for $\mathbb{F}_p((t))$, the analogue of H10 for $\mathbb{Q}_p$ over $\mathbb{Z}$ is arguably to consider polynomial equations over $\mathbb{F}_p[t]$ rather than $\mathbb{F}_p$, since $\mathbb{F}_p[t]$ in $\mathbb{F}_p((t))$ is the analogue of

$\mathbb{Z}$ in $\mathbb{Q}_p$. Further motivating this analogy, Kartas has recently showed that decidability results of equal characteristic fields in $\mathcal{L}_t$ can be transferred to decidability results for mixed characteristic fields in the language of valued fields [Kar20]. Hence, 1.2.1 can be used to obtain decidability results for tame fields in mixed characterstic, which was previously unknown and has seemed to be inaccessible working in the language of rings.

To show Theorem 1.2.1, we obtain a new Ax-Kochen-Ershov principle for certain tame fields in $\mathcal{L}_t$, extending results by Kuhlmann. This principle shows that the type of t is axiomatised by determining solutions to one variable polynomial equations, in the following sense.

Theorem 1.2.2. *Let (L, v) be a tame field containing $\mathbb{F}_p(t)$, with $v(t) > 0$ and let T be the $\mathcal{L}_t$-theory of (L, v). Let (K, v) be the relative algebraic closure of $\mathbb{F}_p(t)$ in L. Suppose that (K, v) is algebraically maximal and that vL/vK is torsion free. Let*

$$S = \Big\{ \exists X \left(f(X) = 0 \wedge v(X) \geq 0 \right) \;\mid\; f(X) \text{ monic in } F_p[t][X] \Big\} \cap T.$$

Let (F, w) be a tame field containing $\mathbb{F}_p(t)$ such that $(F, w) \models S$. Suppose that $vL \equiv wF$ in the language of ordered groups with a distinguished constant symbol π, interpreted as $v(t)$ and $w(t)$ respectively. Suppose that $Lv \equiv Fw$ in the language of rings. Then $(L, v) \equiv (F, w)$ in the language $\mathcal{L}_t$.

While this principle was obtained with equal characteristic p in mind, we also show that the following modified version of the result holds in mixed characteristic.

Theorem 1.2.3. *Let (L, v) be a tame field of mixed characteristic $(0, p)$ and let T be the $\mathcal{L}_{val}$-theory of (L, v). Let (K, v) be the relative algebraic closure of $\mathbb{Q}$ in L. Suppose that (K, v) is algebraically maximal and that vL/vK is torsion free. Let*

$$S = \Big\{ \exists X \left(f(X) = 0 \wedge v(X) \geq 0 \right) \;\mid\; f(X) \text{ monic in } \mathbb{Z}[X] \Big\} \cap T.$$

Let (F, w) be a tame field of mixed characteristic $(0, p)$ such that $(F, w) \models S$. Suppose that $vL \equiv wF$ in the language of ordered groups with a distinguished constant symbol π, interpreted as $v(p)$ and $w(p)$ respectively. Suppose that $Lv \equiv Fw$ in the language of rings. Then $(L, v) \equiv (F, w)$ in the language $\mathcal{L}_{val}$.

Theorem 1.2.2 is combined with the work by Kedlaya on algebraic extensions of function fields [Ked06] and the approximation method by Lampert to obtain Theorem 1.2.1. Earlier versions of the results in Chapter 3 appears in [Lis21].

1.3 Preliminaries

1.3.1 Valued fields

With a valuation on a field, we mean an additive valuation as defined for example in [EP05].

For a valued field (K, v), i.e. a field K with an associated valuation v, we will denote its value group by vK and its residue field by Kv. We say that (K, v) has equal characteristic if $\text{char}(K) = \text{char}(Kv)$, and that (K, v) has mixed characteristic if $\text{char}(K) \neq \text{char}(Kv)$. For an element $\gamma \in vK$, a symbol $\bowtie \in \{<, \leq, >, \geq\}$, and a subset S of K, we write

$$S_{\bowtie \gamma} = \{x \in S \mid v(x) \bowtie \gamma\}.$$

In particular, the valuation ring of K is written as $K_{\geq 0}$. For an element $a \in K_{\geq 0}$, we write $\bar{a} \in Kv$ for the projection of a under the residue map.

For any $\gamma \in vK$, define the following sets

$$V_\gamma := K_{>\gamma}$$

$$W_\gamma := K_{\geq \gamma}.$$

Then $\{V_\gamma, W_\gamma \mid \gamma \in vK\}$ is a fundamental system of a Hausdorff topology on K, making it into topological ring. For details, see Theorem 20.16 in [War89]. We call this topology the **valuation topology** on (K, v). There is a unique topological field $\widehat{K}$ which is complete as a topological space and in which K is dense under the valuation topology. There is also a unique valuation $\hat{v}$ on $\widehat{K}$ that extends v and defines the topology on $\widehat{K}$. We will denote $\hat{v}$ by v as well. For details, see Theorem 20.19 in [War89].

We will mainly be considering the t-adic valuation v_t on fields consisting of formal expansions in t, such as $\mathbb{F}_p(t)$, $\mathbb{F}_p((t))$ and $\mathbb{F}_p((t^{\mathbb{Q}}))$ (see Section 1.3.3 for definitions). This valuation sends an element $\sum_\gamma a_\gamma t^\gamma$ to the minimal γ_0 such that $a_{\gamma_0} \neq 0$. When the t-adic valuation has image in $\mathbb{R} \cup \{\infty\}$, we call the norm defined by $|x| = e^{-v_t(x)}$ the t-adic norm.

If (L, v) is a valued field, we say that (E, w) is a valued subfield of (L, v) if E is a subfield of L and if $v|_E = w$. For a subfield K of L, we will write (K, v) to mean the valued subfield $(K, v|_K)$ of (L, v).

Let (K, v) be a valued field and let L be a finite extension of (K, v) of degree n. Then v has finitely many extensions to v, call them $v_1, \ldots, v_s$. With $e_i := (v_i L : vK)$

and $f_i := [Lv_i : Kv]$, we have that n satisfy the **fundamental inequality**

$$n \geq \sum_{i=1}^{s} e_i f_i.$$

Definition 1.3.1. *Let (K, v) be a valued field. A finite extension L/K of valued fields is **defectless** (with respect to v) if the fundamental inequality is an equality. We say that (K, v) is **defectless** if any finite extensions of (K, v) is defectless.*

Definition 1.3.2. *Let (K, v) be a valued field. A valued field extension (L, v) of (K, v) is an **immediate extension** if $[Lv : Kv] = 1$ and $(vL : vK) = 1$. If (K, v) does not admit any proper (algebraic) immediate extension, then (K, v) is said to be **(algebraically) maximal**.*

For a field K, we denote its algebraic closure by $\overline{K}$. The following standard result for approximating roots of polynomials over valued fields is found for example as Theorem 4.1.7 in [EP05].

Theorem 1.3.3 (Krasner's Lemma)**.** *Let (K, v) be a valued field and let $x_0 \in \overline{K}$ and suppose that its minimal poynomial*

$$f(X) = \prod_{i=0}^{n} (X - x_i) \in K[X]$$

is separable. Let $y \in \overline{K}$ be such that $v(y - x_0) > \max_{i \neq 0}\{v(x_0 - x_i)\}$. Then, $x_0 \in K(y)$.

The following result will be used to apply Krasner's Lemma by taking approximations of separable polynomials.

Theorem 1.3.4 ([EP05, Theorem 2.4.7])**.** *Let (K, v) be a valued field and lef*

$$f(X) = a_0 + \cdots + a_{n-1}X^{n-1} + X^n \in K[X]$$

be a polynomial with distinct roots $x_1, \ldots, x_n \in K$. Let $\alpha \in vK$. Then, there exists $\gamma \in vK$ such that for any polynomial

$$g(X) = \prod_{i=1}^{n} (X - y_i) = b_0 + \cdots + b_{n-1}X^{n-1} + X^n$$

with $y_1, \ldots, y_n \in K$ such that

$$\min_{0 \leq i < n} \{v(a_i - b_i)\} > \gamma,$$

we have that for any $i \in \{1, \ldots, n\}$ there exists a $j \in \{1, \ldots, n\}$ with $v(x_i - y_j) > \alpha$. Furthermore, if $\alpha \geq \max_{i \neq j}\{v(x_i - x_j)\}$, then there exists only one j such that $v(x_i - x_j) > \alpha$.

This thesis mainly considers henselian fields, for which we use the following definition.

Definition 1.3.5. *A valued field (K, v) is called* ***henselian*** *if the valuation v admits a unique extension to any algebraic extension of K.*

We will also use the following equivalent characterisation (see for example [EP05, Theorem 4.1.3]).

Theorem 1.3.6. *The following are equivalent.*

1. *(K, v) is henselian.*
2. *Let $f, g, h \in K_{\geq 0}[X]$ satisfy $\bar{f} = \bar{g}\bar{h}$, with $\bar{g}$, $\bar{h}$ relatively prime in $Kv[X]$. Then, there exist $g_1, h_1 \in K_{\geq 0}[X]$ with $f = g_1 h_1$, $\overline{g_1} = \bar{g}$, $\overline{h_1} = \bar{h}$ and $\deg g_1 = \deg \bar{g}$.*
3. *For each $f \in K_{\geq 0}[X]$ and $\alpha \in Kv$ with $\bar{f}(\alpha)$ and $\bar{f}'(\alpha) \neq 0$, there exists an element $a \in K_{\geq 0}$ such that $\bar{a} = \alpha$ and $f(a) = 0$.*

We will often use the following, appearing in Theorem 5.2.2. and Theorem 5.2.5. in [EP05].

Theorem 1.3.7. *For a valued field (K, v), there is a minimal immediate henselian algebraic extension K^h of K, called the* ***henselisation*** *of K, which is unique up to valuation preserving isomorphism over K.*[1]

With K^s being the separable closure of K and v_s being an extension of v to K_s, the henselisation K^h of K is defined as the fixed field of the subgroup of the absolute Galois group $G(K^s/K)$ which preserves the valuation ring $K^s_{\geq 0}$. In particular, K^h is contained in K^s.

The **rank** of v is the rank of vK, i.e. the number of proper convex subgroups of vK. When v is of rank one, then $(\widehat{K}, v)$ is henselian (see for example [EP05, Proposition 2.1.1] together with [EP05, Proposition 1.2.2]).

[1] Minimal in the sense that K^h embedds uniquely over (K, v) into any henselian extension of (K, v).

1.3.2 Algorithms, languages and model theory

An **alphabet** is a non-empty set of symbols. A **string** over Σ is a finite sequence with elements in Σ. We denote by Σ^* the set of strings over Σ. If $s = s_1 \cdots s_n \in \Sigma^*$, we will sometimes consider expressions of the form $s_1 \dots s_0$ when iterating over substrings of s. This should be understood as the empty string. A subset of Σ^* is called a **formal language** over Σ. We use the term formal language to distinguish from the notion of language in first order logic. With an **algorithm**, we mean a Turing machine.

We will write algorithms in pseudocode using the syntax as exemplified here.

AN_ALGORITHM(input with specifications)

```
▷ A comment.
x ← 0                                  ▷ Assign 0 to the variable x.
while x ≤ n do                         ▷ Verify condition on x.
    for k ∈ {x, ..., n} do             ▷ Iterate over elements.
        if P(x) then
            return Q
    x ← x + 1
```

In many situations, we will define algorithms that implicitly depend on a parameter, for example a prime number p. When it is clear from context, we will not mention this parameter when using the algorithm, but rather assume that the correct version of the algorithm is used.

Definition 1.3.8. *Let $\mathcal{L}$ be a formal language over a finite alphabet Σ. We say that $\mathcal{L}$ is **recursively enumerable** if there is an algorithm with input alphabet Σ which on input $w \in \Sigma^*$ returns* TRUE *if and only if $w \in L$.*

We will use this alternative characterisation of recursively enumerable, which is essentially Theorem 3.13 in [Sip13]. For this, we identify $\mathbb{N}$ with the set of strings over the alphabet $\{*\}$ (or any alphabet of size 1), by mapping $n \in \mathbb{N}$ to the string $* \cdots *$ of length n.

Lemma 1.3.9. *A formal language $\mathcal{L}$ over a finite alphabet Σ is recursively enumerable if and only if there is an algorithm* ENUMERATE *with input alphabet $\{*\}$ which on input $n \in \mathbb{N}$ returns an element $s \in \mathcal{L}$, and such that* ENUMERATE *is surjective as a function from $\mathbb{N}$ to $\mathcal{L}$.*

Proof. Suppose that $\mathcal{L}$ recursively enumerable and let ALG be the corresponding algorithm from Definition 1.3.8. Let $\Sigma = \{s_1, \dots, s_m\}$ with $|\Sigma| = m$. Let $(p_n)_{n \geq 1}$ be

the sequence of all prime numbers in increasing order. Consider the encoding of Σ^* which associates a string $\prod_{j=1}^{k} s_{i_j} \in \Sigma^*$ with the unique natural number $\prod_{j=1} p_j^{p_{i_j}}$. This encoding induces a well-order $<_\Sigma$ on Σ^*. Write $\Sigma^* = \{w_i \mid i \in \mathbb{N}\}$, where $w_i <_\Sigma w_j$ whenever $i < j$. For $n \in \mathbb{N}$, we now define ENUMERATE(n) as follows. Let R be an empty list, to which we will add strings $w \in \mathcal{L}$.[2] For $i = 1, 2, 3, \dots$, run ALG for i steps on inputs $w_1, \dots, w_i$. At each iteration, add to R any such string for which ALG returns TRUE after i steps. Continue this until R contains n strings. By construction, this procedure will halt. The output of ENUMERATE(n) is then the n:th string on R. If $w \in \mathcal{L}$, then $w =$ ENUMERATE(n) for some $n \in \mathbb{N}$. In fact, $w =$ ENUMERATE(n) for infinitely many n, since if ALG returns TRUE on input w after i steps, it also returns TRUE on input w after j steps for all $j > i$.

Conversely, suppose that ENUMERATE is as described. We can then repeatedly compare w to ENUMERATE(n) for $n \in \mathbb{N}$. We define ALG to return TRUE on input $w \in \Sigma^*$ if (and only if) $w =$ ENUMERATE(n) for some $n \in \mathbb{N}$. Since ENUMERATE is surjective as a function from $\mathbb{N}$ to $\mathcal{L}$, we get that $\mathcal{L}$ is recursively enumerable. □

In the situation of Lemma 1.3.9, we say that ENUMERATE **enumerates** $\mathcal{L}$.

Definition 1.3.10. *Let $\mathcal{L}$ be a formal language over a finite alphabet Σ. We say that $\mathcal{L}$ is **decidable** if there is an algorithm with input alphabet Σ which on input $w \in \Sigma^*$ returns* TRUE *if $w \in L$ and* FALSE *if $w \notin L$.*

It follows that if $\mathcal{L}$ is decidable, then $\mathcal{L}$ is recursively enumerable by the same algorithm. We note that for any finite alphabet Σ, the set of strings Σ^* is trivially decidable by an algorithm which returns TRUE on every input.

For a finite field $\mathbb{F}_q$, where $q = p^n$ for some prime p and some positive integer n, we will view $\mathbb{F}_q$ as a finite alphabet by fixing an irreducible polynomial f of degree n over $\mathbb{F}_p$. The alphabet $\mathbb{F}_q$ then consists of expressions of the form $a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$, where $a_i \in \{0, \dots, p-1\}$.

For model theoretic terminology, we mostly follow the conventions in [TZ12]. To clarify the two somewhat conflicting notions of language that we use, a first-order language $\mathcal{L}$ is an alphabet and the set of $\mathcal{L}$-sentences is a formal language over $\mathcal{L}$. We will refer to first-order languages simply as languages. The languages we will consider can be seen as finite alphabets by using $*$ instead of $\mathbb{N}$ when necessary. For example, X_n will be an abbreviation for the string $X * \cdots *$ of length $n + 1$.

[2] More precisely, R is a blank tape on a two tape Turing machine which only writes strings to R in one direction, and uses some delimiter to distinguish between strings.

If $\mathcal{L}$ is a language and A and B are $\mathcal{L}$-structures, we write $A \equiv B$ if A and B have the same $\mathcal{L}$-theories. Furthermore, if C is a set which embeds in both A and B, we write $A \equiv_C B$ if A and B have the same $\mathcal{L}(C)$-theories, where $\mathcal{L}(C)$ denotes the language $\mathcal{L}$ extended by adjoining constant symbols for the elements in C, interpreted by the respective embeddings into A and B. In this situation, we will often for simplicity say that C is a common subset of A and B and assume the embeddings to be inclusions. If C is a singleton $\{c\}$, we write $A \equiv_c B$ instead of $A \equiv_C B$.

For an $\mathcal{L}$-structure A and a subset C of L, denote by $\mathrm{acl}_A(C)$ the model theoretic algebraic closure of C in A. The following lemma is mentioned in the context of fields in [Dit18, p. 92]. The provided proof follows closely the proof of Lemma 5.6.4 in [TZ12] and was suggested by Ehud Hrushovski.

Lemma 1.3.11. *Let $\mathcal{L}$ be a language and let A and B be $\mathcal{L}$-structures with a common subset C such that $A \equiv_C B$. Then, there is a bijection between $acl_A(C)$ and $acl_B(C)$ such that $A \equiv_{acl_A(C)} B$.*

Proof. Let f be a partial embedding from $\mathrm{acl}_A(C)$ to $\mathrm{acl}_B(C)$ extending the identity on C. Consider B as an $\mathcal{L}(C')$-structure by interpreting any constant symbol corresponding to $c \in C'$ by $f(c)$. Suppose that the domain C' of f is maximal with respect to inclusion and suppose that f is such that $A \equiv_{C'} B$. Since the identity on C satisfies these properties, we have that such a map f exists.

Let a be a tuple of elements in $\mathrm{acl}_A(C)$ and let M be a saturated elementary extension of A. Since a is algebraic over C', there is an $\mathcal{L}(C')$-formula $\phi(X)$ such that $A \models \phi(a)$. Take ϕ to be minimal, in the sense that the cardinality of $\phi(M)$ is minimal. We then have that ϕ isolates the type $\mathrm{tp}(a/C')$. Indeed, suppose that there is an element $a' \in \phi(M)$ such that $\mathrm{tp}(a/C') \neq \mathrm{tp}(a'/C')$. Then, there is an $\mathcal{L}(C')$ formula ϕ' such that $a \in \phi'(M)$ but $a' \notin \phi'(M)$. Hence, $(\phi \wedge \phi')(M)$ is a non-empty proper subset of $\phi(M)$, contradicting minimality of ϕ. Since $A \equiv_{C'} B$, there is an element $b \in \phi(B)$. Since ϕ isolates $\mathrm{tp}(a/C')$, we have for any $\psi \in \mathrm{tp}(a/C')$ that $A \models \forall X(\phi(X) \to \psi(X))$. This implies that $B \models \forall X(\phi(X) \to \psi(X))$ as well, so $\mathrm{tp}(b/C') = \mathrm{tp}(a/C')$. Thus, we can extend f by sending a to b, so $a \in C'$ by maximality of f. This shows that $C' = \mathrm{acl}_A(C)$ and f is the embedding we are looking for. □

We denote by $\mathcal{L}_{\mathrm{ring}} = \{+, -, \cdot, 0, 1\}$ the language of fields and by $\mathcal{L}_{\mathrm{og}} = \{+, <, 0\}$ the language of ordered groups. We extend $\mathcal{L}_{\mathrm{ring}}$ to the language of valued fields $\mathcal{L}_{\mathrm{val}} = \{+, -, \cdot, ^{-1}, 0, 1, \mathrm{div}\}$, where div is a binary relation symbol. For a valued field

(K, v) and elements $a, b \in K$, the relation $\mathrm{div}(a, b)$ is interpreted as $v(a) \geq v(b)$. While v is not a symbol in $\mathcal{L}_{\mathrm{val}}$, we will for simplicity write $v(X) = 0$ as a shorthand for the $\mathcal{L}_{\mathrm{val}}$-formula $\mathrm{div}(1, X) \wedge \mathrm{div}(X, 1)$, since this formula defines the set of all elements with valuation 0 in (K, v). When we talk about the theories of Kv and vK, we mean the $\mathcal{L}_{\mathrm{ring}}$-theory and $\mathcal{L}_{\mathrm{og}}$-theory respectively, if not stated otherwise.

We let $\mathcal{L}_t = \mathcal{L}_{\mathrm{val}} \cup \{t\}$, where t is a constant symbol not in $\mathcal{L}_{\mathrm{val}}$. A Hahn field $\mathbb{F}((t^\Gamma))$ containing t is an $\mathcal{L}_t$-structure by considering the t-adic valuation on $\mathbb{F}((t^\Gamma))$, as described in Section 1.3.3.

If $\mathcal{L}$ is a recursively enumerable language, then the set of $\mathcal{L}$-sentences is also recursively enumerable. If A is an $\mathcal{L}$-structure, we say that A is decidable if its $\mathcal{L}$-theory is decidable. We will use the fact that a recursively enumerable complete theory is decidable, which is seen by using the algorithm which enumerates T to determine which one of ϕ and $\neg\phi$ are in T. If T has a recursively enumerable axiomatisation, then T is recursively enumerable, by listing the (finitely many) sentences with derivations of length at most n that one can deduce from the first n axioms of T, and then repeat for $n + 1$, and so on.

Using results on the $\mathcal{L}_{\mathrm{og}}$-theories of ordered abelian groups in [RZ60], we get the following lemma.

Lemma 1.3.12. *The $\mathcal{L}_{og}(1)$-theories of $\frac{1}{p^\infty}\mathbb{Z}$ and $\mathbb{Q}$ are decidable.*

Proof. Let $\mathcal{L}_{\mathrm{og}}^+$ be the language obtained by adding to $\mathcal{L}_{\mathrm{og}}$ predicates D_n for each n coprime to p. These predicates are intepreted as

$$D_n(x) \Leftrightarrow \exists y(ny = x).$$

Both $\frac{1}{p^\infty}\mathbb{Z}$ and $\mathbb{Q}$ are regularly dense, in the sense of [RZ60]. That is, they are archimedean and have no smallest positive element. From Theorem 4.6 in [RZ60] and its preceding discussion, we have recursively enumerable axiomatisations of the $\mathcal{L}_{\mathrm{og}}^+$-theories of $\frac{1}{p^\infty}\mathbb{Z}$ and $\mathbb{Q}$. From the proof of the same theorem, they are also model complete. Call these theories T_{1/p^∞} and $T_{\mathbb{Q}}$ respectively. In particular, all models of T_{1/p^∞} are p-divisible and all models of $T_{\mathbb{Q}}$ are divisible. We now claim that the $\mathcal{L}_{\mathrm{og}}^+(1)$-theories of $\frac{1}{p^\infty}\mathbb{Z}$ and $\mathbb{Q}$ are axiomatised by

$$T_{1/p^\infty} \cup \{1 > 0\} \cup \left\{\forall X(nX \neq 1) \mid n \in \mathbb{N} \setminus p\mathbb{N}\right\}$$

and

$$T_{\mathbb{Q}} \cup \{1 > 0\}$$

respectively. Indeed, any model of these extended theories contain $\frac{1}{p^\infty}\mathbb{Z}$ respectively $\mathbb{Q}$ as submodels. By model completeness of the $\mathcal{L}_{\text{og}}^+$-theories, these are elementary substructures as $\mathcal{L}_{\text{og}}^+$-structures. Hence, they are also elementary substructures as $\mathcal{L}_{\text{og}}^+(1)$-structures. In other words, they are prime models of the respective $\mathcal{L}_{\text{og}}^+(1)$-theories, and so the theories are complete. Since we added a recursively enumerable set of sentences to the recursively enumerable axiomatisations, we have that the $\mathcal{L}_{\text{og}}^+(1)$-theories also have recursively enumerable axiomatisations. Hence they are recursively enumerable and decidable, as described above. Since the $\mathcal{L}_{\text{og}}(1)$-theories are subsets of these theories, the result follows. □

1.3.3 Hahn fields

The main objects of study in this thesis are Hahn fields, or fields of generalised power series. Introduced in [Hah07], they are constructed in the following way. Let $\mathbb{F}$ be a field, let Γ be an ordered abelian group and let t be transcendental over $\mathbb{F}$. A generalised powers series in t with coefficients in $\mathbb{F}$ and exponents in Γ is a formal expression of the form

$$x = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$$

where the support, i.e. the set $\{\gamma \in \Gamma \mid a_\gamma \neq 0\}$, is well-ordered. The Hahn field $\mathbb{F}((t^\Gamma))$ is then the set of all such expressions together with term-wise addition and multiplication defined by

$$\left(\sum_{\gamma \in \Gamma} a_\gamma t^\gamma\right)\left(\sum_{\gamma \in \Gamma} b_\gamma t^\gamma\right) = \sum_{\gamma \in \Gamma} \sum_{\alpha+\beta=\gamma} a_\alpha b_\beta t^\gamma.$$

Note that multiplication is well defined since the supports are well-ordered. As the name suggests, $\mathbb{F}((t^\Gamma))$ is a field under these operations.

For a generalised power series $x = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$, we will interchangeably use the notations

$$x = \sum_{\gamma \geq \gamma_0} a_\gamma t^\gamma, \qquad x = \sum_{i \in I} a_i t^{\gamma_i}, \qquad x = \sum_{i < \sigma} a_i t^{\gamma_i}$$

where γ_0 is minimal such that $a_{\gamma_0} \neq 0$, I is a well-ordered index set, and σ is an ordinal. For $r \in \Gamma$, we write

$$x_{<r} = \sum_{\gamma \in \Gamma_{<r}} a_\gamma t^\gamma$$

$$x_{\leq r} = \sum_{\gamma \in \Gamma_{\leq r}} a_\gamma t^\gamma.$$

Similarly, with the notations $x = \sum_{i \in I} a_i t^{\gamma_i}$ and $x = \sum_{i < \sigma} a_i t^{\gamma_i}$, we write $x_{<i} = x_{<\gamma_i}$ and $x_{\leq i} = x_{\leq \gamma_i}$. We say that y is an **approximation** of x if $y = x_{<\lambda}$ for some λ and $y \neq x$. We say that y is a **better approximation** of x than z if y is an approximation of x and z is an approximation of y.

Throughout, we will assume that $t \in \mathbb{F}((t^\Gamma))$. More precisely, this amounts to choosing a positive element $\gamma \in \Gamma$ and defining $t = t^\gamma$. Just as fields of formal Laurent series, $\mathbb{F}((t^\Gamma))$ admits a natural valuation v by setting

$$v\left(\sum_{\gamma \geq \gamma_0} a_\gamma t^\gamma\right) = \gamma_0.$$

Under this valuation, $\mathbb{F}$ is the residue field and Γ is the value group.

A standard result (see for example Theorem 1 in [Poo93]) is that $\mathbb{F}((t^\Gamma))$ is maximal. It follows that $\mathbb{F}((t^\Gamma))$ algebraically closed if $\mathbb{F}$ is algebraically closed and Γ is divisible [Poo93, Corollary 4]. If $\mathbb{F}$ is algebraically closed and Γ is divisible and non-trivial, then $\mathbb{F}((t^\Gamma))$ is universal, i.e. any field with the same cardinality and same characteristic embeds as a subfield in $\mathbb{F}((t^\Gamma))$ [Mac39]. More useful for us will be to consider algebraic extensions of $\mathbb{F}(t)$ inside the Hahn field $\mathbb{F}((t^\Gamma))$ as follows.

Lemma 1.3.13. *Let $\mathbb{F}$ be a field of characteristic p and let Γ be a non-trivial ordered abelian group. Let K be the relative algebraic closure of $\mathbb{F}_p(t)$ in $\mathbb{F}((t^\Gamma))$. Then K is contained in $Kv((t^{vK}))$.*

Proof. Let Γ' be the divisible hull of Γ. We can view $\mathbb{Q}$ as a subgroup of Γ', by using the general assumption that $t \in \mathbb{F}((t^\Gamma))$ and identifying $\mathbb{Q}$ with the divisible hull of $\langle v(t) \rangle$ in Γ'. Consider $\overline{\mathbb{F}}_p((t^{\mathbb{Q}}))$ and $\mathbb{F}((t^\Gamma))$ as subfields of the Hahn field $\overline{\mathbb{F}}((t^{\Gamma'}))$. Since $\overline{\mathbb{F}}_p((t^{\mathbb{Q}}))$ is algebraically closed and contains $\mathbb{F}_p(t)$, we have that K is a subfield of

$$\overline{\mathbb{F}}_p((t^{\mathbb{Q}})) \cap \mathbb{F}((t^\Gamma)) = E((t^G)),$$

where $E = \overline{\mathbb{F}}_p \cap \mathbb{F}$ and G is the relative divisible hull of $v(t)$ in Γ. In particular, Kv is contained in E, since Kv is algebraic over $\mathbb{F}_p$. On the other hand, since E is an algebraic extension of $\mathbb{F}_p$ inside $\mathbb{F}$, we also have that E is contained in Kv. We thus get that $E = Kv$ and the result follows since $vK = G$. □

It was noted by Abhyankar [Abh56] that generalised power series with coefficients in $\mathbb{F}_p$ and exponents in $\frac{1}{p^\infty}\mathbb{Z}$ arise naturally as root to the Artin-Schreier polynomial

$$f(X) = X^p - X - 1/t \in \mathbb{F}_p(t).$$

Indeed, by linearity of the Frobenius, we have that

$$x = \sum_{n \geq 1} t^{-1/p^n}$$

is a root of f. We get all roots of f by adding to x elements of $\mathbb{F}_p$. It is tempting to see x as some kind of limit to the sequence

$$\left\{ \sum_{i=1}^{n} t^{-1/p^i} \right\}$$

in $\mathbb{F}_p((t))^{1/p^\infty}$, the perfect hull of $\mathbb{F}_p((t))$. In this sense, $\mathbb{F}_p((t^{1/p^\infty}))$ could be seen as a completion to $\mathbb{F}_p((t))^{1/p^\infty}$. However, uniqueness fails since the sequence is not convergent and any element $x + y$ with $v(y) \geq 0$ could be seen as a limit. For this to make sense, we need a weaker notion of convergence, that of a pseudo-convergence, which will be made more precise in Section 1.3.5.

As we will see, the question of decidability for $\mathbb{F}_p((t^{1/p^\infty}))$ and similar fields reduces to the question of finding a decision procedure for the existence of roots of one variable polynomials over $\mathbb{F}_p(t)$. Such a procedure already exists for $\mathbb{F}_p((t))^{1/p^\infty}$ by standard valuation theory. More precisely, any root to a polynomial $f \in \mathbb{F}_p(t)[X]$ in $\mathbb{F}_p((t))^{1/p^\infty}$ is in $\mathbb{F}_p((t^{1/p^n}))$, where $p^n \geq \deg(f)$. Determining if $\mathbb{F}_p((t^{1/p^n}))$ has a root of f can be done for example by the recursion procedure defined in Section 2.1 and using Krasner's Lemma. Since $\mathbb{F}_p((t^{1/p^\infty}))$ is a maximal immediate extension of $\mathbb{F}_p((t))^{1/p^\infty}$, finding a decision procedure for $\mathbb{F}_p((t^{1/p^\infty}))$ amounts to determining which immediate extensions of $\mathbb{F}_p((t))^{1/p^\infty}$ lie inside $\mathbb{F}_p((t^{1/p^\infty}))$, given the reduction to one variable polynomials over $\mathbb{F}_p[t]$.

The following result, appearing as Corollary 5.10 in [Kuh16], shows that passing from $\mathbb{F}_p((t))^{1/p^\infty}$ to its completion does not give more information about immediate extensions inside $\mathbb{F}_p((t^{1/p^\infty}))$.

Theorem 1.3.14. *Let (K, v) be a henselian valued field (K, v) and let $\widehat{K}$ be its completion, as described in Section 1.3.1. Then (K, v) is existentially closed in its completion $(\widehat{K}, v)$ if and only if the extension $\widehat{K}/K$ is separable.*

1.3.4 Additive polynomials

Definition 1.3.15. *Let K be a field and let $P(X) \in K[X]$. Then P is called **additive** if $P(X + Y) = P(X) + P(Y)$ as polynomials in X and Y.*

Our use of additive polynomials relies completely on the following important result. It appears for example as Lemma 12.2.3 in [AS03].

Lemma 1.3.16 (Ore's lemma)**.** *Let K be a field of characteristic p and let $f(X) \in K[X]$. Then there is a non-zero additive polynomial $P(X) \in K[X]$ of degree $p^{\deg(f)}$ such that f divides P.*

Proof. Consider $\{X^{p^i} \mod f(X) \mid 0 \leq i \leq \deg(f)\}$ as a set of vectors in the K-vector space $K[X]/(f)$. By cardinality, these are linearly dependent over K. Thus, there are $a_i \in K$ such that

$$\sum_{i=0}^{\deg(f)} a_i X^{p^i} \equiv 0 \mod f(X). \qquad \square$$

Remark 1.3.17. In the case of Ore's lemma when $K = \mathbb{F}_p(t)$, there is an algorithm that takes as input f and returns the additive polynomial P. We denote this algorithm by ADDITIVE_MULTIPLE. To see that this algorithm indeed exists, we note that we can use Euclid's algorithm to obtain $b_{k,i} \in \mathbb{F}_p(t)$ for $k < \deg(f)$ and $i \leq \deg(f)$ such that

$$X^{p^i} \equiv \sum_{k=0}^{\deg(f)-1} b_{k,i} X^k.$$

We then let $(a_i)_{0 \leq i \leq \deg(f)}$ be a non-trivial solution to the system of linear equations over $\mathbb{F}_p$ given by

$$\sum_{i=0}^{\deg(f)} a_i \sum_{k=0}^{\deg(f)-1} b_{k,i} X^k \equiv 0 \mod f.$$

On input $f(X)$, the algorithm ADDITIVE_MULTIPLE thus returns $\sum_{i=0}^{\deg(f)} a_i X^{p^i}$.

1.3.5 Kaplansky fields

While $\mathbb{F}_p((t^{1/p^\infty}))$ can be seen as a sort of completion of $\mathbb{F}_p((t))^{1/p^\infty}$, in the sense that for example the sequence

$$\left(\sum_{i \leq n} t^{-1/p^i} \right)_{n \geq 1}$$

is completed by the element $\sum_{n \geq 1} t^{-1/p^n} \in \mathbb{F}_p((t^{1/p^\infty}))$, this completion is not unique. In the current section, we will describe this notion of completion by overviewing the work by Kaplansky in [Kap42]. We will see that this will also give a deeper understanding of immediate extensions of valued fields. All results without proofs in this section are due to Kaplansky.

Definition 1.3.18. *Let (K, v) be a valued field and let $\{a_\rho\}_{\rho \in I}$ be a set of elements of K where the index set I is well-ordered without a last element. Then $\{a_\rho\}$ is said to be* ***pseudo-convergent*** *if for all $\rho < \sigma < \tau$, we have $v(a_\sigma - a_\rho) < v(a_\tau - a_\sigma)$.*

Lemma 1.3.19 ([Kap42, Lemma 1])**.** *Let $\{a_\rho\}$ be a pseudo-convergent sequence. Then one of the following holds.*

1. *$v(a_\rho) = v(a_\sigma)$ for all large enough σ and ρ;*
2. *$v(a_\rho) < v(a_\sigma)$ for all $\rho < \sigma$.*

Lemma 1.3.20 ([Kap42, Lemma 2])**.** *Let $\{a_\rho\}$ be a pseudo-convergent sequence. Then*

$$v(a_\sigma - a_\rho) = v(a_{\rho+1} - a_\rho)$$

for all $\sigma > \rho$.

By Lemma 1.3.20, we can write $\gamma_\rho := v(a_\sigma - a_\rho)$ for any $\sigma > \rho$. This gives us the following definition.

Definition 1.3.21. *We say that ξ is a limit of a pseudo-convergent sequence $\{a_\rho\}$ if $v(\xi - a_\rho) = \gamma_\rho$ for all ρ.*

The following important result establishes the first connection between pseudo-convergent sequences and immediate extensions.

Theorem 1.3.22 ([Kap42, Theorem 1])**.** *Let (L, v) be an extension of (K, v). If $(L, v)/(K, v)$ is an immediate extension, then any element in $L \setminus K$ is a limit of a pseudo-convergent sequence of elements in K, without a limit in K.*

Lemma 1.3.23 ([Kap42, Lemma 5])**.** *Let $\{a_\rho\}$ be a pseudo-convergent sequence in (K, v) and let $f(X) \in K[X]$ be a non-constant polynomial. Then for some sufficiently large λ, we have that $\{f(a_\rho)\}_{\rho > \lambda}$ is a pseudo-convergent sequence. In particular, one of the following holds.*

1. *$vf(a_\rho) = vf(a_\sigma)$ for all sufficiently large ρ and σ;*
2. *$vf(a_\rho) < vf(a_\sigma)$ for all sufficiently large ρ and σ, with $\rho < \sigma$.*

Definition 1.3.24. *A pseudo-convergent sequence $\{a_\rho\}$ is said to be of* ***algebraic type*** *if there is a polynomial $f(X) \in K[X]$ such that (2) in Lemma 1.3.23 holds for f. If $\{a_\rho\}$ is not of algebraic type, it is said to be of* ***transcendental type****.*

We can associate a kind of minimal polynomial $q(X) \in K[X]$ to a pseudo-convergent sequence of algebraic type by letting q be of minimal degree such that (2) in Lemma 1.3.23 holds for q.

Theorem 1.3.25 ([Kap42, Theorem 2 and Theorem 3])**.** *Let $\{a_\rho\}$ be a pseudo-convergent sequence without a limit in K. Then the following hold.*

1. *If $\{a_\rho\}$ is of transcendental type, then there is an immediate transcendental extension $K(z)$ of K such that z is a limit of $\{a_\rho\}$. Furthermore, if $K(u)$ is an immediate extension of K such that u is a limit of $\{a_\rho\}$, then $K(u)$ is isomorphic to $K(z)$ over K.*

2. *If $\{a_\rho\}$ is of algebraic type and $q(x)$ is a minimal polynomial of $\{a_\rho\}$, in the sense described above, then there is an immediate algebraic extension $K(z)$ of K such that z is a limit of $\{a_\rho\}$ and $q(z) = 0$. Furthermore, if $K(u)$ is an immediate extension of K such that u is a limit of $\{a_\rho\}$ and $q(u) = 0$, then $K(u)$ is isomorphic to $K(z)$ over K.*

Remark 1.3.26. Note that Theorem 1.3.25 does not say that the limit of a pseudo-convergent sequence of algebraic type necessarily defines an algebraic extension. Indeed, consider the sequence $\sum_{i=1}^{n} t^{-1/p^i}$ over $\mathbb{F}_p((t))^{1/p^\infty}$. This is a pseudo-convergent sequence with the limit $x = \sum_{n\geq 1} t^{-1/p^n} \in \mathbb{F}_p((t^{1/p^\infty}))$. Then, for any transcendental element $y \in \mathbb{F}_p((t^{1/p^\infty}))_{\geq 0}$, we have that $x + y$ is a transcendental pseudo-limit of the given sequence.

For a valued field (K, v) of equal characteristic p, the following two conditions are what Kaplansky calls **Hypothesis A** [Kap42], which provides a criterion for understanding all the immediate extensions of K.

1. Any non-zero additive polynomial $f \in Kv[X]$ is surjective on Kv.

2. The value group vK is p-divisible.

A valued field satisfying Hypothesis A is also called a **Kaplansky field**. An immediate but important fact is that any immediate extension of a Kaplansky field is also a Kaplansky field. Furthermore, note that the conditions of Hypothesis A can be expressed as first order statements in $\mathcal{L}_{\text{ring}}$ and $\mathcal{L}_{\text{og}}$ respectively. Therefore, if (L, v) is a Kaplansky field and (F, w) is a valued field such that $Lv \equiv Fw$ and $vL \equiv wF$, we have that (F, w) is also a Kaplansky field. The importance of Hypothesis A is captured in the following Theorem.

Theorem 1.3.27 ([Kap42, Theorem 5])**.** *Let (K, v) be a valued field of equal characteristic p satisfying Hypothesis A. Then, (K, v) admits a maximal immediate extension (L, v) which is unique up to valuation preserving isomorphism over K.*

We will mainly be interested in uniqueness of immediate algebraic algebraically maximal extensions. For a Kaplansky field, this situation is implicitly covered in the proof of Theorem 1.3.27. The following result shows however that we do not need to assume hypothesis A, as long as the maximal immediate extension is unique.

Lemma 1.3.28. *Let (E, v) be a valued field admitting a maximal immediate extension (L, v) which is unique up to valuation preserving isomorphism over E. Then, the relative algebraic closure (K, v) of (E, v) in (L, v) is the unique, up to valuation preserving isomorphism over E, algebraic extension of (E, v) which is immediate and algebraically maximal.*

Proof. Let K' be an immediate algebraic algebraically maximal extensions of E. It is enough to show that K is isomorphic to K' as a valued field over E, since this implies that K is also algebraically maximal. Let L' be a maximal immediate extension of K'. Then K' is the relative algebraic closure of E in L', since any extension of K' inside L' is immediate and since K' is algebraically maximal. Furthermore, we have that L and L' are isomorphic as valued fields over E, by assumption on E. Denote this isomorphism by Φ. For any polynomial $f \in E[X]$, we have that $a \in L$ is a root of f if and only if $\Phi(a) \in L'$ is a root of f. Therefore $\Phi(K) = K'$ and we are done. □

Both conditions of Hypothesis A are necessary, as illustrated by the following two examples.

Example 1.3.29. Consider the polynomial $f(X) = X^p - X - 1/t$. It defines an immediate extension K_1 of $\mathbb{F}_p((t))^{1/p^\infty}$ inside $\mathbb{F}_p((t^{1/p^\infty}))$, since $\alpha = \sum_{n\in\mathbb{N}} t^{-1/p^n}$ is a root of f. On the other hand, the polynomial $g(X) = X^p - X - 1/t - 1$ defines an immediate extension K_2 of $\mathbb{F}_p((t))^{1/p^\infty}$ which is not a subfield $\mathbb{F}_p((t^{1/p^\infty}))$. Indeed, if g had a root β in $\mathbb{F}_p((t^{1/p^\infty}))$, then $\eta = \alpha - \beta$ would be a root of $X^p - X - 1$ in $\mathbb{F}_p((t^{1/p^\infty}))$. But then $v(\eta^p - \eta) = 0$, so $v(\eta) = 0$ and $\bar{\eta}$ is a root of $X^p - X - 1$ in $\mathbb{F}_p$. This is a contradiction. Since a unique maximal immediate extension of $\mathbb{F}_p((t))^{1/p^\infty}$ would contain both K_1 and K_2, we conclude that there is no such extension.

Example 1.3.30. Let $\mathbb{F}$ be a field of characteristic p. Then, by Hensel's lemma, $\mathbb{F}_p((t))$ has a root to the polynomial $f(X) = X^p - X + t$. This can also be seen

directly as $x = \sum_{n\in\mathbb{N}} t^{p^n}$ is a root. On the other hand, letting $s = t+1$ and considering the $t-adic$ valuation on $\mathbb{F}((s))$, we get that $\mathbb{F}(t) = \mathbb{F}(s)$ has a maximal immediate extension $\mathbb{F}((s))$, which admits a root to the polynomial $g(X) = X^p - X + s$. Like in the previous example, no immediate extension of $\mathbb{F}(t)$ can contain roots of both f and g, so $\mathbb{F}(t)$ does not admit a unique maximal immediate extension.

The following result by Whaples gives an alternative useful characterisation of Kaplansky fields. Note that the original statement in [Wha57, Theorem 1] refers to the residue field as a Kaplansky field, rather than the valued field itself.

Theorem 1.3.31. *A valued field (K, v) is a Kaplansky field if and only if it satisfies the following.*

1'. Kv has no algebraic extension of degree divisible by p.

2. The value group vK is p-divisible.

We will need the following results, which appear in Theorem 1.1 and Proposition 1.2 in [Kuh22].

Theorem 1.3.32. *Let (L, v) be an algebraically maximal Kaplansky field. Then for any subfield K of L, we have that L contains an algebraically maximal immediate extension of K. Furthermore, if K is a relatively algebraically closed subfield of L, then (K, v) is also an algebraically maximal Kaplansky field.*

1.3.6 Tame fields

When $\mathbb{F}$ is a perfect field and Γ is a p-divisible ordered abelian group, then $\mathbb{F}((t^\Gamma))$ falls in a class of fields called tame fields. This class was studied extensively by Kuhlman in [Kuh16] and we follow this approach.

Definition 1.3.33. *An algebraic extension $(L|K, v)$ of a henselian valued field (K, v) is called **tame** if every finite subextension $E|K$ of $L|K$ satisfies the following conditions:*

1. $(vE : vK)$ is prime to p

2. $Ev|Kv$ is separable

3. $E|K$ is defectless.

*A **tame field** is a henselian valued field for which all algebraic extensions are tame.*

That Hahn fields with perfect residue field and p-divisible value group are canonical examples of tame fields is, if not apparent from the definition, clear from the following alternative characterisations [Kuh16, Theorem 3.2, Corollary 3.3].

Theorem 1.3.34. *A valued field (K, v) is tame if and only if (K, v) is algebraically maximal, Kv is perfect, and vK is p-divisible. If (K, v) has characteristic (p, p), then (K, v) is tame if and only if it is algebraically maximal and perfect.*

Given Theorem 1.3.34 and Kaplansky's characterisation of immediate extensions, the following result is clear for tame Hahn fields of equal characteristic. For the general situation, see [Kuh16, Lemma 3.7]

Lemma 1.3.35. *Let (L, v) be a tame field and let $(K, v) \subset (L, v)$ be a relatively algebraically closed subfield. Suppose that $Lv|Kv$ is an algebraic extension. Then (K, v) is a tame field, vL/vK is torsion free, and $Kv = Lv$.*

Using Lemma 1.3.13, the condition in Lemma 1.3.35 that Lv/Kv is an algebraic extension can be omitted when considering Hahn fields.

Lemma 1.3.36. *Let $\mathbb{F}$ be a perfect field of characteristic p and let Γ be a p-divisible value group. Let (K, v) be the relative algebraic closure of $\mathbb{F}_p(t)$ in $\mathbb{F}((t^\Gamma))$. Then (K, v) is a tame field and Γ/vK is torsion free.*

Proof. Since vK is the relative divisible hull of $v(t)$ in Γ, we have that Γ/vK is torsion free. By Lemma 1.3.13, we have that K is relatively algebraically closed in $L = Kv((t^{vK}))$. By assumption on F and Γ, we have that Kv is perfect and vK is p-divisible, so L is tame. Since $Lv = Kv$, we are in the situation of Lemma 1.3.35 and (K, v) is a tame field. □

The following example, inspired by Example 3.9 in [Kuh04] shows that the two previous lemmas are not trivial.

Example 1.3.37. Let $p > 2$. Let s and t be two algebraically independent transcendental elements over $\mathbb{F}_p$. In particular, $\alpha = st$ is transcendental over $\mathbb{F}_p(s)$. Let $\Gamma = \frac{1}{2p^\infty}\mathbb{Z}$ and consider the Hahn field

$$L = \mathbb{F}_p(s)^{1/p^\infty}((\alpha^\Gamma)).$$

This can be considered as a subfield of

$$\mathcal{M} = \mathbb{F}_p(s^{1/2})^{1/p^\infty}((t^\Gamma)).$$

Indeed, let

$$x = \sum_{\gamma \in S_x} a_\gamma \alpha^\gamma \in L.$$

Then, for any $\gamma \in S_x$, we can write $\gamma = \frac{m}{2p^n}$, with $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. But then $s^\gamma \in \mathbb{F}_p(s^{1/2})^{1/p^\infty}$, so it makes sense to write

$$x = \sum_{\gamma \in S_x} a_\gamma (st)^\gamma = \sum_{\gamma \in S_x} a_\gamma s^\gamma t^\gamma \in \mathcal{M}.$$

Let v be the t-adic valuation on $\mathcal{M}$. The equality above also shows that the α-adic valuation on L coincides with the restriction of v to L. So $vL = \Gamma$ and, by construction, Lv is perfect. Since (L, v) is also maximal, it is therefore a tame field.

Now consider the relative algebraic closure K of $\mathbb{F}_p(t)$ in L. We claim that K is contained in the Hahn field

$$E = \mathbb{F}_p((t^{1/p^\infty})).$$

To see this, we first note that E is contained in L. Indeed, any term at^{m/p^n} appearing in an element in E can be written as $as^{-m/p^n}(\alpha)^{m/p^n}$. Now consider the relative algebraic closure of $\mathbb{F}_p(t)$ in $\mathcal{M}$. This is contained in $F = \mathbb{F}_p((t^\Gamma))$, which implies that K is contained in $L \cap F$. Suppose now that K contains an element $x \in F \setminus E$. Write this element as $x = y + z$, where $y \in E$ and $v(z) \notin vE$. Since both K and E are contained in L, we must have that $z \in L$. Let $at^{\frac{m}{2p^n}}$ be the initial term of z. Since $\frac{m}{2p^n} \notin vE$, we have that m is odd. We then have that $a^{-1}t^{-\frac{m+1}{2}} \in L$, and the initial term of $w = a^{-1}t^{-\frac{m+1}{2}}y^{p^n}$ is $t^{-1/2}$. Since w is in L, we also have that $w\alpha^{1/2}$ is in L. But $w\alpha^{1/2}$ has valuation 0, and its residue class is a square root of s. This contradicts L having residue field $\mathbb{F}_p(s)^{1/p^\infty}$, so K is contained in E. Since K contains $\mathbb{F}_p(t)^{1/p^\infty}$, we have that $vK = \frac{1}{p^\infty}\mathbb{Z}$. But $vL = \Gamma$, so vL/vK has torsion.

Similarly, tameness of the relative algebraic closure of $\mathbb{F}_p(t)$ can fail, as seen in this example.

Example 1.3.38. Again, let s be transcendental over $\mathbb{F}_p(t)$. We will consider all fields in this example as subfields of the Hahn field

$$\mathcal{M} = \overline{\mathbb{F}}_p((s^{\mathbb{Q}}))((t^{1/p^\infty}))$$

with the t-adic valuation v. To clarify the notation, we have that $\mathcal{M}v = \overline{\mathbb{F}}_p((s^{\mathbb{Q}}))$. Note that $\mathcal{M}$ is a Kaplansky field.

Let $\alpha = \sum_{n \geq 1} s^{-1/p^n}$ and let E be the field given by adjoining

$$\beta = \alpha + \sum_{n \geq 1} t^{-1/p^n}$$

to $\mathbb{F}_p((s))^{1/p^\infty}((t))$. Note that $\alpha \notin \mathbb{F}_p((s))^{1/p^\infty}$. Since β is a root of $X^p - X - s^{-1} - t^{-1}$, we have that $E/\mathbb{F}_p((s))^{1/p^\infty}((t))$ is an extension of degree p. Since $v(\beta) = -1/p$, adjoining β does not extend the residue field of $\mathbb{F}_p((s))^{1/p^\infty}((t))$, i.e. $Ev = \mathbb{F}_p((s))^{1/p^\infty}$.

By Theorem 1.3.32, we can let L be a maximal immediate extension of E inside $\mathcal{M}$. Let K be the relative algebraic closure of $\mathbb{F}_p(t)$ in L. Since $\mathbb{F}_p$ is relatively algebraically closed in $\mathbb{F}_p((s^{1/p^\infty}))$, we have that $Kv = \mathbb{F}_p$. By Lemma 1.3.13, we get that K is contained in $\mathbb{F}_p((t^{1/p^\infty}))$. Furthermore, since $vK = \frac{1}{p^\infty}\mathbb{Z}$, adding $\sum_{n\geq 1} t^{-1/p^n}$ gives an immediate algebraic extension of K. This is a proper extension, since if $\sum_{n\geq 1} t^{-1/p^n} \in L$, then $\alpha \in L$. Hence, K is not algebraically maximal.

One of the main results in [Kuh16] is that tame fields admit an Ax-Kochen Ershov principle in the language $\mathcal{L}_{\text{val}}$. In particular, this implies the following.

Theorem 1.3.39 ([Kuh16, Theorem 1.6])**.** *Let q be a power of a prime p and let Γ be an ordered abelian group which is divisible or elementarily equivalent to $\frac{1}{p^\infty}\mathbb{Z}$. Then $\mathbb{F}_q((t^\Gamma))$ equipped with the t-adic valuation is decidable in the language $\mathcal{L}_{val}$.*

To mimic this result for $\mathcal{L}_t$, we need the following.

Definition 1.3.40. *Let $\mathcal{C}$ be an elementary class of tame fields in the language $\mathcal{L}_{val}$. If for every two fields $(L, v), (F, w) \in \mathcal{C}$ and every common defectless subfield (K, v) of (L, v) and (F, w) such that vL/vK is torsion free and $Lv|Kv$ is separable, the conditions $vL \equiv_{vK} wF$ and $Lv \equiv_{Kv} Fw$ imply that $(L, v) \equiv_{(K,v)} (F, w)$, then we will call $\mathcal{C}$ **relatively subcomplete** (in the language $\mathcal{L}_{val}$).*

Theorem 1.3.41 (Theorem 7.1 in [Kuh16])**.** *The class of tame fields is relatively subcomplete in the language $\mathcal{L}_{\text{val}}$.*

1.3.7 Finite automata

In this section, we include some standard results on finite automata, as presented in [AS03]. We also present key results in [Ked06]. The main findings of this thesis rely on the existence of algorithms which outputs certain automata. The results are thus stated in this manner, i.e. by saying that there exists an algorithm that outputs an automaton with certain properties. While the referenced results are not stated explicitly like this, it follows from the proofs in the references that such algorithms do exist. When necessary, additional details are provided to emphasise this.

We will need the following three kinds of finite automata.

Definition 1.3.42. *A **deterministic finite automaton**, or a **DFA**, is a tuple $M = (Q, \Sigma, \delta, q_0, F)$ where*

- *Q is a finite set (the **states**);*
- *Σ is a finite set (the **input alphabet**);*
- *δ is a function from $Q \times \Sigma$ to Q (the **transition function**);*
- *$q_0 \in Q$ (the **initial state**);*
- *F is a subset of Q (the **accepting states**).*

Definition 1.3.43. *A **deterministic finite automaton with output**, or a **DFAO**, is a tuple $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ where*

- *Q is a finite set (the **states**);*
- *Σ is a finite set (the **input alphabet**);*
- *δ is a function from $Q \times \Sigma$ to Q (the **transition function**);*
- *$q_0 \in Q$ (the **initial state**);*
- *Δ is a finite set (the **output alphabet**);*
- *τ is a function from Q to Δ (the **output function**).*

Definition 1.3.44. *A **nondeterministic finite automaton**, or an **NFA**, is a tuple $M = (Q, \Sigma, \delta, q_0, F)$ where*

- *Q is a finite set (the **states**);*
- *Σ is a finite set (the **input alphabet**);*
- *δ is a function from $Q \times \Sigma$ to the power set of Q (the **transition function**);*
- *$q_0 \in Q$ (the **initial state**);*
- *F is a subset of Q (the **accepting states**).*

If $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ is a DFAO and $0 \in \Delta$, we say that a state $q \in Q$ an **accepting state of** M if $\tau(q) \neq 0$. Thus, a DFA can be seen as a DFAO with output alphabet $\{0, 1\}$.

We will consider families of DFAOs where the input alphabet Σ and the output alphabet Δ are fixed. Denote the collection of such DFAOs by $\mathcal{D}(\Sigma, \Delta)$. For any DFAO, we will identify its set of states Q with the set $\{1, \ldots, |Q|\}$ if not specified otherwise. With this identification, we can view $\mathcal{D}(\Sigma, \Delta)$ as a set. Furthermore, with the identifications

$$\begin{aligned} s_1 &= \ (\\ s_2 &= \ \{ \\ s_3 &= \ , \\ s_4 &= \ \} \\ s_5 &= \ ) \end{aligned}$$

$\mathcal{D}(\Sigma, \Delta)$ can be seen as a formal language over the alphabet

$$\Xi = \{s_1, s_2, s_3, s_4, s_5\} \cup \{*\} \cup \Sigma \cup \Delta,$$

where $\{*\}$ again is used to generate $\mathbb{N}$.

For simplicity, we enforce any string in $\mathcal{D}(\Sigma, \Delta)$ to be without repetitions of the elements in the sets, and with elements of Q in increasing order, i.e. on the form

$$\big(\{1, \ldots, i\}, \{\Sigma_1, \ldots, \Sigma_j\}, \{\delta_1, \ldots, \delta_k\}, q_0, \{\Delta_1, \ldots, \Delta_\ell\}, \{\tau_1, \ldots, \tau_m\}\big)$$

where $|\{\{\Sigma_1, \ldots, \Sigma_j\}| = j$, $|\{\delta_1, \ldots, \delta_k\}| = k$, $\{\Delta_1, \ldots, \Delta_\ell\}| = \ell$, and $|\{\tau_1, \ldots, \tau_m\}| = m$. It follows that $\mathcal{D}(\Sigma, \Delta)$ is recursively enumerable, since it is straight forward to verify if a string in Ξ^* is on the prescribed form or not. Denote by ENUMERATE_DFAO the algorithm which enumerates $\mathcal{D}(\Sigma, \Delta)$.

If M is a DFAO with input alphabet Σ and transition function δ, we extend δ to the function

$$\delta^* : Q \times \Sigma^* \to Q$$

defined recursively by

$$\begin{aligned} \delta^*(q, \emptyset) &= q \\ \delta^*(q, wa) &= \delta(\delta^*(q, w), a) \end{aligned}$$

where $q \in Q$, $w \in \Sigma^*$ and $a \in \Sigma$. Furthermore, we let

$$f_M : \Sigma^* \to \Delta$$

be the function defined by

$$f_M(w) = \tau(\delta^*(q_0, w)).$$

Note that any DFA is both a DFAO and an NFA, and that the following two definitions indeed agree on DFAs.

Definition 1.3.45. *Let $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ be a DFAO. For a string $w \in \Sigma^*$, we say that M **accepts** w if $f_M(w) \neq 0$. The set of strings in Σ^* accepted by M is called the **language accepted by** M. A language accepted by some DFA is called **regular**.*

Definition 1.3.46. *Let $N = (Q, \Sigma, \delta, q_0, F)$ be an NFA and let $w = s_1 \cdots s_n \in \Sigma^*$. An **accepting path** for w is a sequence of states $q_1, \ldots, q_n \in Q$ such that $q_i \in \delta(q_{i-1}, s_i)$ for $i \in \{1, \ldots, n\}$ and $q_n \in F$. We say that N **accepts** w if there exists an accepting path for w in N. The set of strings in Σ^* accepted by N is called the **language accepted by** N.*

As models of computation, an NFA is equivalent to a DFA in the following sense (see for example Theorem 4.1.3 in [AS03]).

Theorem 1.3.47. *There is an algorithm* EQUIVALENT_DFA *which takes as input an NFA M and outputs a DFA M' such that M and M' accept the same language.*

We denote by $\text{rev} : \Sigma^* \to \Sigma^*$ the function sending $s_1 \cdots s_n$ to $s_n \cdots s_1$. The following appears as Theorem 4.3.3 in [AS03].

Theorem 1.3.48. *There is an algorithm* REV *which takes as input a DFAO M and returns a DFAO M' such that $f_{M'} = f_M \circ \text{rev}$.*

We fix some notation for the following lemma. Let n be a positive integer. Given an NFA $M = (Q, \Sigma, \delta, q_0, F)$ and a string $w \in \Sigma^*$, denote by $a_M(w)$ the number of accepting paths for w in M. Let

$$\begin{aligned} g_M : \Sigma^* &\to \mathbb{Z}/n\mathbb{Z} \\ w &\mapsto [a_M(w)]. \end{aligned}$$

Lemma 1.3.49 ([Ked06, Lemma 2.2.2])**.** *There is an algorithm* ACCEPTING_PATHS *which takes as input an NFA M and outputs a DFAO M' such that $g_M = f_{M'}$, with g_M being as defined above.*

We will mainly consider finite automata with input alphabet

$$\Sigma_p = \{0, 1, \ldots, p-1, .\}.$$

Definition 1.3.50. *A string $s = s_1 \cdots s_n \in \Sigma_p^*$ is said to be a **valid base p-expansion** if $s_1 \neq 0$, $s_n \neq 0$, and s_k is equal to the radix point for exactly one $k \in \{1, \ldots, n\}$. If s is a valid base p-expansion and s_k is the radix point, then we define the **value** of s to be*

$$v(s) = \sum_{i=1}^{k-1} s_i p^{k-1-i} + \sum_{i=k+1}^{n} s_i p^{k-i} \in \frac{1}{p^\infty}\mathbb{N}.$$

Conversely, for an element $v \in \frac{1}{p^\infty}\mathbb{N}$, we denote by $s(v)$ the valid base p-expansion of v.

Definition 1.3.51. *Let Δ be a finite set. A function*

$$f : \frac{1}{p^\infty}\mathbb{N} \to \Delta$$

*is called **p-automatic** if there is a DFAO $M = (Q, \Sigma, q_0, \Delta, \tau)$ such that for any $v \in \frac{1}{p^\infty}\mathbb{Z}$, we have that $f(v) = f_M(s(v))$.*

The connection between finite automata and generalised power series is captured in the following result, which is a particular instance of the more general Theorem 4.1.3. in [Ked06].

Theorem 1.3.52. *Let q be a power of a prime p and let $f : \frac{1}{p^\infty}\mathbb{N} \to \mathbb{F}_q$ be a function with well-ordered support. Then the generalised power series*

$$\sum_{\gamma \in \frac{1}{p^\infty}\mathbb{N}} f(\gamma) t^\gamma \in \mathbb{F}_q[[t^{1/p^\infty}]]$$

is algebraic over $\mathbb{F}_q(t)$ if and only if f is p-automatic.

It is often convenient to consider finite automata as edge-labeled directed graphs, i.e. as directed graph (V, E) together with a labelling function ℓ from E to some set S. In particular, this will be useful to verify effectiveness of results in this section.

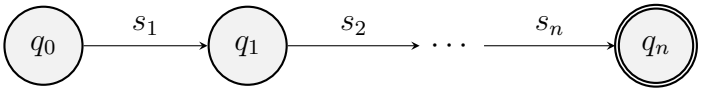
Remark 1.3.53. There is an algorithm SUBGRAPH which takes as input a finite edge-labeled directed graph $G = (V, E, \ell)$ and a subset $U \subset V$ and returns the edge set E_U of the induced subgraph $G[U]$ together with the labelling function of G restricted to E_U. It is defined as follows.

SUBGRAPH$(G = (V, E, \ell), U \subset V)$

$E_U \leftarrow \emptyset$
$\ell_U \leftarrow \emptyset$
for $(u, v) \in U^2$ **do**
    if $(u, v) \in E$ **then**
        $E_U \leftarrow E_U \cup \{(u, v)\}$
        for $s \in \ell(E)$ **do**
            if $\ell(u, v) = s$ **then**
                $\ell_U \leftarrow \ell_U \cup \{((u, v), s)\}$
return (E_U, ℓ_U)

Definition 1.3.54. *Let $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ be a DFAO or an NFA. The **transition graph** of M is the edge-labeled directed graph on the vertex set Q, with an edge from $q \in Q$ to $q' \in Q$ labeled by $s \in \Sigma$ if $\delta(q, s) = q'$.*

When illustrating transition graphs, we will use double circles around a state to illustrate that it is an accepting state. Furthermore, we will omit all edges that do not lead to accepting paths, and all states only reached by such paths. For example, the following is an illustration of a DFA which only accepts the string $s_1 \cdots s_n$.



Remark 1.3.55. The following defines an algorithm which takes as input a DFAO or an NFA $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ and returns the edges E and the labelling ℓ of the transition graph of M.

TRANSITION_GRAPH$(M = (Q, \Sigma, \delta, q_0, \Delta, \tau))$

$E \leftarrow \emptyset$
$\ell \leftarrow \emptyset$
for $(q, q', s) \in Q^2 \times \Sigma$ **do**
    if $\delta(q, s) = q'$ **then**
        $E \leftarrow E \cup \{(q, q')\}$
        $\ell \leftarrow \ell \cup \{((q, q'), s)\}$
return (E, ℓ)

Definition 1.3.56. *Let $M = (Q, \Sigma_p, \delta, q_0, \Delta, \tau)$ be a DFAO. We say that M is **well-formed** (resp. **well-ordered**) if there is an arbitrary (resp. a well-ordered) subset $S \subset \frac{1}{p^\infty}\mathbb{N}$ such that the language accepted by M consists of the valid base p expansions of the elements of S.*

Remark 1.3.57. To verify that $M = (Q, \Sigma_p, \delta, q_0, \Delta, \tau)$ is well-formed, it is enough to consider strings of length at most $m = (3p+1)|Q|+2$. Indeed, suppose that $n > m$ and that M accepts a string $w = s_1 \cdots s_n$ which is not the valid base p-expansion of any $a \in \frac{1}{p^\infty}\mathbb{N}$. By definition, this means that w satisfies one of the following items.

1. $s_1 = 0$;
2. $s_n = 0$;
3. no s_i is equal to the radix point;
4. s_i and s_j are both equal to the radix point with $i \neq j$.

Suppose that the first or third item holds. Since $n > |Q| + 1$, we have that the sequence $\delta^*(q_0, s_1s_2)$, $\delta^*(q_0, s_1s_2s_3)$, ..., $\delta^*(q_0, s_1 \cdots s_n)$ contains two identical states. Let $i, j \in \{2, \ldots, n\}$ be distinct such that $\delta^*(q_0, s_1 \cdots s_i) = \delta^*(q_0, s_1 \cdots s_j)$. Without loss of generality, assume that $i < j$. Then $\delta^*(q_0, s_1 \cdots s_i s_{j+1} \cdots s_n) = \delta^*(q_0, w)$. In particular, M accepts the string $s_1 \cdots s_i s_{j+1} \cdots s_n$ which is of length strictly less than n beginning with s_1. By induction, we get that M accepts a string w' of length m, with elements being a subset of $\{s_1, \ldots, s_n\}$, which also begins with s_1. By construction, if w satisfies the first item then so does w', and if w satisfies the third item then so does w'. Hence w' is not a valid base p expansion. By the same argument, fixing $s_n = 0$ instead of s_1, we get that M accepts a string of length m which is not a valid base p expansion if the second item hold.

Suppose now that the fourth item holds. Let $e_1, \ldots, e_n$ be the sequence of edges corresponding to the sequence of connected vertices

$$q_0, \delta(q_0, s_1), \delta^*(q_0, s_1s_2), \ldots, \delta^*(q_0, s_1 \cdots s_n).$$

Let i and j be such that s_i is the first radix point of w and s_{i+j} is the second radix point of w. We can assume that the subsequences $(e_k)_{1 \leq k < i}$, $(e_k)_{i < k < i+j}$ and $(e_k)_{i+j < k \leq n}$ all separately only contain distinct edges. Indeed, if $e_k = e_\ell$ for some $k < \ell$ with

$$(k, \ell) \in \{1, \ldots, i-1\}^2 \cup \{i+1, \ldots, i+j-1\}^2 \cup \{i+1+1, \ldots, n\}^2$$

then we repeatedly replace w with the string $s_1 \cdots s_k s_{\ell+1} \cdots s_n$, which by construction also contains two radix points and is accepted by M. We will see that this string must have length less than or equal to m, thus showing that M accepts a string of length less than or equal to m which is not a valid base p expansion.

Since Σ_p contains $p+1$ elements, the total number of edges of the transition graph of M is $(p+1)|Q|$, and the total number of edges that are not labeled by the radix point is $p|Q|$. Since $(e_k)_{1\leq k<i}$ only contains distinct vertices, none labeled by the radix point, we have that $i \leq p|Q|+1$. Similarly, we get that $j \leq p|Q|+1$. By the assumption that $(e_k)_{i+j<k\leq n}$ only contains distinct edges, the length of this sequence must be bounded above by the total number of edges in the transition graph. Hence, $n-i-j \leq (p+1)|Q|$. Combining the obtained inequalities gives

$$n \leq (3p+1)|Q|+2,$$

and we are done.

Remark 1.3.58. By the bound obtained in Remark 1.3.57, we conclude that there is an algorithm which takes as input a DFAO $M = (Q, \Sigma_p, \delta, q_0, \Delta, \tau)$ and returns TRUE if M is well-formed, and FALSE otherwise. We denote this algorithm by WELL_FORMED. It is defined as follows.

WELL_FORMED$(Q, \Sigma_p, \delta, q_0, \Delta, \tau)$

```
for s = s_1 ··· s_n ∈ Σ_p^* with n ≤ (3p+1)|Q|+2 do
    ▷ Verify that no string starting or ending with 0 is accepted.
    if s_1 = 0 or s_n = 0 then
        if f_M(s) ≠ 0 then
            return FALSE
    ▷ Verify that every accepted string has exactly one radix point.
    if s_i ≠ . for all i ∈ {1,...,n} or s_i = s_j = . for some i ≠ j then
        if f_M(s) ≠ 0 then
            return FALSE
return TRUE
```

To verify that a DFAO is well-ordered, we need a bit more.

Definition 1.3.59. *Let $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA. We say that M is **minimal** if there is no DFA with fewer states than M accepting the same language as M.*

Remark 1.3.60. There is an algorithm which takes as input a DFA M and outputs a minimal DFA M' which accepts the same language as M and which is unique up to renaming the states. For details, see Section 4.4.3 in [HU79]. We will denote this algorithm by MIN_DFA.

The Myhill-Nerode theorem, appearing for example as Theorem 4.1.8 in [AS03], provides a way verify if a given language is regular not.

Definition 1.3.61. *Let $\mathcal{L}$ be a language over an alphabet Σ. We say that an equivalence relation $\sim$ on Σ is **right-invariant** if $w \sim w'$ implies $wz \sim w'z$ for all $z \in \Sigma^*$.*

Theorem 1.3.62 (Myhill-Nerode theorem)**.** *Let $\mathcal{L}$ be a language over a finite alphabet Σ. Then $\mathcal{L}$ is regular if and only if there exists a right-invariant equivalence relation $\sim$ of finite index on Σ^* such that $\mathcal{L}$ is the union of some of the equivalence classes of $\sim$.*

The notion of minimality for DFAs does not extend directly to DFAOs, since all the properties of a DFAO are not captured by the language it accepts. We will instead use this less restrictive notion of minimality.

Definition 1.3.63. *Let $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$ be a DFAO. We say that a state $q \in Q$ is **reachable** from a state q_1 if there is some string $s \in \Sigma^*$ such that $\delta^*(q_1, s) = q$. If q is reachable from q_0, we say that q is reachable. If q is not reachable, we say that it is **unreachable**. If M has no unreachable states, we say that M is **minimal**.*

If M is a minimal DFA, then it is also minimal as a DFAO, since removing unreachable states does not change the accepted language.

Remark 1.3.64. If $M = (Q, \Sigma, \delta, q_0, \tau, \Delta)$ is a DFAO with set of states Q and if $q' \in Q$ is reachable from $q \in Q$ by a string $w = s_1 \dots s_n$, then we can assume that $n \leq |Q|$. Indeed, if $\delta^*(q, s_1 \dots s_i) = \delta^*(q, s_1 \dots s_j)$ for some $i \neq j$, then we can replace w with $w' = s_1 \dots s_i s_{j+1} \dots s_n$, which still gives a path from q to q'. Consequently, there is an algorithm REACHABLE_STATES which on input M returns all states of M reachable states of M, by returning all states of M reachable by strings of length at most $|Q|$.

Definition 1.3.65. *A state $q \in Q$ is **relevant** if there exists an accepting state reachable from q. If q is not relevant, we say that it is **irrelevant**.*

Remark 1.3.66. There is an algorithm which takes as input a DFAO M together with a state q of M and returns the relevant states reachable from q. We denote it by RELEVANT_STATES. It is defined as follows. As in Remark 1.3.64, we only need to consider strings of length less than or equal to $|Q|$.

RELEVANT_STATES$(M = (Q, \Sigma, \delta, q_0, \Delta, \tau), q)$

$Q_q \leftarrow \emptyset$
for $s = s_1 \cdots s_n \in \Sigma^*$ with $n \leq |Q|$ **do**
  if $\tau(\delta^*(q, s)) \neq 0$ **then**
    $Q_q \leftarrow Q_q \cup \{\delta^*(q, s_1 \cdots s_i) \mid \text{for } 0 \leq i \leq n\}$
return Q_q

We write RELEVANT_STATES(M) in place of RELEVANT_STATES(M, q_0). Note that if M is minimal, then all states are reachable from q_0, so all relevant states of M are in this case given by RELEVANT_STATES(M).

Definition 1.3.67. *Let M be a DFAO with input alphabet Σ_p. We say a state $q \in Q$ is **preradix** (resp. **postradix**) if there exists a valid base p expansion $s = s_1 \cdots s_n$ accepted by M with s_k equal to the radix point such that $q = \delta^*(q_0, s_1 \cdots s_i)$ for some $i < k$ (resp. for some $i \geq k$).*

Remark 1.3.68. If M has input alphabet Σ_p and is well-formed, then no accepted state can be both preradix and postradix. Indeed, suppose that there is an accepted state q which is both preradix and postradix. Then, there are valid base p expansions $s_1 \cdots s_m$ and $s'_1 \cdots s'_n$ accepted by M with radix points s_k and s'_ℓ respectively such that

$$q = \delta^*(q_0, s_1 \cdots s_i) = \delta^*(q_0, s'_1 \cdots s'_j),$$

with $i < k$ and $j \geq \ell$. We then have that

$$\delta^*(q_0, s_1 \cdots s_m) = \delta^*(q_0, s'_1 \cdots s'_j s_{i+1} \cdots s_m)$$

is an accepted state reached by a string with two radix points, which is a contradiction.

Remark 1.3.69. By definition, any postradix state q is relevant. Furthermore, any relevant state is postradix if and only if there is a string $w = s_1 \cdots s_n$ not containing any radix point such that $\delta^*(q, w)$ is an accepting state. This, combined with Remark 1.3.64 shows that the following defines an algorithm which takes as input a well-formed DFAO M and outputs the postradix states of M. A similar algorithm exists for preradix states, though we will not need it.

POSTRADIX($M = (Q, \Sigma_p, \delta, q_0, \Delta, \tau)$)

```
PostradixStates ← ∅
RelevantStates ← RELEVANT_STATES(M)
for q ∈ RelevantStates do
    for w = s_1 ··· s_n ∈ {0, ..., p − 1}* with n ≤ |Q| do
        if τ(δ*(q, w)) ≠ 0 then
            PostradixStates ← PostradixStates ∪ {q}
return PostradixStates
```

We will now consider a characterisation of transition graphs which will allow us to tell if a DFAO is well-ordered.

Definition 1.3.70. *Let $G = (V, E)$ be a directed graph and let $v \in V$. We say that G is a **rooted saguaro**, and that v is a **root** of G, if the following hold.*

1. *Each vertex of G lies on at most one cycle, up to permutation of the vertices by rotation.*[3]

2. *There exists directed paths from v to each vertex of G.*

*An edge of a rooted saguaro is **cyclic** if it lies on a cycle and **acyclic** otherwise.*

Remark 1.3.71. There is an algorithm which takes as input a finite directed graph $G = (V, E)$ and an element $v \in V$ and outputs TRUE if G is a rooted saguaro with root v, and FALSE otherwise. We denote this algorithm by ROOTED_SAGUARO. To see that such an algorithm indeed exists, we first let CYCLES be an algorithm which takes as input a directed graph and return the set of finitely many cycles of G (for example by going through all possible paths of length at most $|V| + 1$). From this, we can check that each vertex only appears in one such cycle, up to rotation of the vertices. For the second item, it is enough to go through directed paths of length at most $|V| - 1$ to verify that each vertex of G is in such a path. Indeed, if there is a path $(v_1, v_2),\ (v_2, v_3), \ldots,\ (v_n, v_{n+1})$ from $v = v_1$ to $w = v_{n+1}$ with $n \geq |V|$, then $v_i = v_j$ for some $i \neq j$. This gives a path $(v_1, v2), \ldots,\ (v_i, v_{j+1}), \ldots\ (v_n, v_{n+1})$ of length strictly less than n.

Definition 1.3.72. *Let $G = (V, E)$ be a directed graph. A **proper p-labelling** of G is a function $\ell : E \to \{0, \ldots, p-1\}$ with the following properties hold for all $v, w, x \in V$.*

1. *If $w \neq x$ and $(vw, vx) \in E^2$, then $\ell(vw) \neq \ell(vx)$.*

2. *If $vw \in E$ lies on a cycle and $vx \in E$ does not lie on a cycle, then $\ell(vw) > \ell(vx)$*

Remark 1.3.73. There is an algorithm p_LABELLING which takes as input a directed graph $G = (V, E)$ together with a function $\ell : E \to \{0, \ldots, p-1\}$ and returns TRUE if ℓ is a proper p-labelling of E and FALSE otherwise. It is defined as follows.

[3]With cycle, we mean a closed directed path with no repeated vertices apart from the first and last. In [Ked06], the term *minimal cycle* is used for what we call a cycle.

p_LABELLING(V, E, ℓ)

```
Cycles ← CYCLES(V, E)
for (v, w, x) ∈ V^3 do
    if w ≠ x and vw ∈ E and vx ∈ E then
        if ℓ(v, w) = ℓ(v, x) then
            return FALSE
    if vw ∈ Cycles and vx ∈ E \ Cycles then
        if ℓ(vw) ≤ ℓ(vx) then
            return FALSE
return TRUE
```

Theorem 1.3.74 ([Ked06, Theorem 7.1.6])**.** *Let M be a DFA with input alphabet Σ_p and suppose that M is minimal and well-formed. For any state q of M, let G_q be the subgraph of the transition graph consisting of relevant states reachable from q. Then M is well-ordered if and only if for each relevant postradix state q, we have that G_q is a rooted saguaro with root q, equipped with a proper p-labelling.*

We will now fix some notation to allow us to go between elements in $\mathbb{F}_q[[t^{1/p^\infty}]]$ and their corresponding automata. For a well-ordered DFAO with input alphabet Σ_p and output set $\mathbb{F}_q$, we denote by $\mathrm{Pow}(M)$ the element

$$\sum_{\gamma \in \frac{1}{p^\infty}\mathbb{N}} f_M(s(\gamma))t^\gamma \in \mathbb{F}_q[[t^{1/p^\infty}]].$$

If $a \in \mathbb{F}_q$, we denote by aM the DFAO given from M by replacing the output function τ with $a\tau$. By definition, this implies that $\mathrm{Pow}(aM) = a\mathrm{Pow}(M)$. We write $-M$ instead of $-1M$. Note that $\mathrm{Pow}(M) = 0$ if and only if M has no reachable accepting states. When M is minimal, this is equivalent to RELEVANT_STATES$(M) = \emptyset$.

To define a DFA corresponing to $1 \in \mathbb{F}_q[[t^{1/p^\infty}]]$, we need a DFA

$$\mathbb{1} = (Q, \Sigma_p, \delta, q_0, \{0, 1\}, \tau\})$$

which accepts only the string $s(0)$, i.e. the string only consisting of a single radix point. More precisely, this is defined as follows.

- $Q = \{q_0, q_1, q_2\}$, where $q_i = i$.
- $\delta(q_0, s) = q_1$ for all $s \in \{0, \ldots, p-1\}$.
- $\delta(q_0, s(0)) = q_2$.
- $\delta(q_i, s) = q_1$ for $i \in \{1, 2\}$ and for all $s \in \Sigma_p$.

- $\tau(q_i) = 0$ for $i \in \{0, 1\}$ and $\tau(q_2) = 1$.

With this definition, $\mathbb{1}$ is minimal and well-ordered, and $\mathrm{Pow}(\mathbb{1}) = 1$.

Remark 1.3.75. We can write any $x \in \mathbb{F}_q[[t^{1/p^\infty}]]$ as a linear combination over $\mathbb{F}_q$. In particular, if M is a well-ordered DFAO M, we get

$$\mathrm{Pow}(M) = \sum_{i=1}^{q-1} a_i \sum_{r \in S_i} t^r \in \mathbb{F}_q[[t^{1/p^\infty}]]$$

where $a_i \in \mathbb{F}_q^*$ and $a_i \neq a_j$ for $i \neq j$, and where S_i is a well-ordered, possibly empty, subset of $\frac{1}{p^\infty}\mathbb{Z}$. With this in mind, there is an algorithm LINEAR_COMBINATION which takes as input a DFAO M with output alphabet $\mathbb{F}_q$ and returns a set of tuples $\{(a_i, M_i) \mid i \in \{1, \ldots, q-1\}\}$ where the $a_i \in \mathbb{F}_q$ are all distinct and the M_i are minimal DFAs with input alphabet Σ_p such that, if M is well-ordered, we have

$$\mathrm{Pow}(M) = \sum_{i=1}^{q-1} a_i \mathrm{Pow}(M_i). \tag{1.1}$$

If $M = (Q, \Sigma_p, \delta, q_0, \mathbb{F}_q, \tau)$, let M_i' be the DFA given by $(Q, \Sigma_p, \delta, q_0, \mathbb{F}_q, \tau_i)$, where $\tau_i(q) = 1$ if $\tau(q) = a_i$ and $\tau_i(q) = 0$ otherwise. Then $(M_i')_{1 \leq i \leq n}$ satisfies (1.1). Taking M_i to be MIN_DFA(M_i') gives the desired result. By construction, we also have that M is well-ordered if and only if all of the M_i are well-ordered. Indeed, if M_i is not well-ordered, then there is an infinite descending sequence $(v_j)_{j \in \mathbb{N}}$ of elements in $\frac{1}{p^\infty}\mathbb{N}$ such that M_i accepts the valid base p-expansion of each v_j. By definition of τ_i, this implies that M also accepts the valid base p-expansions of each s_j, so M is not well-ordered. Conversely, suppose that M is not well-ordered, accepting the valid base p expansions of an infinite descending sequence $(v_j)_{j \in \mathbb{N}}$. By definition, this means that $f_M(s(v_j)) \neq 0$ for all j. By the pigeonhole principle, there is an $i \in \{1, \ldots, q-1\}$ and an infinite subsequence $(v_j')_{j \in \mathbb{N}}$ such that $f_M(s(v_j')) = a_i$. By definition of τ_i, this implies that M_i accepts the valid base p expansions of $(v_j')_{j \in \mathbb{N}}$ as well, so M_i is not well-ordered.

Remark 1.3.76. Using LINEAR_COMBINATION, we see that there is an algorithm EQUALS which takes as input two well-ordered DFAOs M and N with output alphabet $\mathbb{F}_q$, returning TRUE if $\mathrm{Pow}(M) = \mathrm{Pow}(N)$ and FALSE otherwise. Since MIN_DFA gives a unique minimal DFA, up to renaming the state, the algorithm EQUALS amounts to checking that, for every $a \in \mathbb{F}_q$, if (a, M') and (a, N') are tuples in LINEAR_COMBINATION(M) and LINEAR_COMBINATION(N), then M' and N' are equal, up to renaming the states.

Remark 1.3.77. From Theorem 1.3.74 and Remark 1.3.75, we conclude that there is an algorithm which takes as input a DFAO M with input alphabet Σ_p and returns TRUE if M is well-ordered, and FALSE otherwise. We denote this algorithm by WELL_ORDERED. It is defined as follows.

WELL_ORDERED($M = (Q, \Sigma_p, \delta, q_0, \Delta, \tau)$)

```
for (a, N) ∈ LINEAR_COMBINATION(M) do
    ▷ Verify that N satisfies the properties of Theorem 1.3.74.
    if not WELL_FORMED(N) then
        return FALSE
    (E, ℓ) ← TRANSITION_GRAPH(N)
    RelevantStates ← RELEVANT_STATES(N, q_0)
    PostradixStates ← POSTRADIX(N)
    for q ∈ RelevantStates ∩ PostradixStates do
        Q_q ← RELEVANT_STATES(N, q)
        (E_q, ℓ_q) ← SUBGRAPH((Q, E, ℓ), Q_q)
        if not ROOTED_SAGUARO((Q_q, E_q) then
            return FALSE
        if not p_LABELLING(Q_q, E_q, ℓ_q) then
            return FALSE
return TRUE
```

Remark 1.3.78. Given a prime number p and a prime power $q = p^n$, the set of there is an algorithm ENUMERATE_WELL_ORDERED_$\mathbb{F}_q$ which enumerates well-ordered DFAOs with output alphabet $\mathbb{F}_q$. On input n, this algorithm returns the n:th well-formed DFAO in $\mathcal{D}(\Sigma_p, \mathbb{F}_q)$, which is verified using WELL_ORDERED.

In Section 3.2, we will use Theorem 1.3.52 to determine which monic one variable polynomials over $\mathbb{F}_p[t]$ have roots in certain Hahn fields. To this end, we will need the following two lemmas describing an effective procedure for arithmetic of DFAOs representing elements in $\mathbb{F}_q[[t^{1/p^\infty}]]$. They appear implicitly in [Ked06] as Lemma 7.2.1 and Lemma 7.2.2 respectively. Again, the proofs are entirely due to Kedlaya and are included to emphasise effectiveness.

Lemma 1.3.79. *There is an algorithm* ADD *which takes as input two well-ordered DFAOs M and M', both having input alphabet Σ_p and output set $\mathbb{F}_q$, and outputs a well-ordered DFAO N with the same input alphabet and output set such that* $\mathrm{Pow}(N) = \mathrm{Pow}(M) + \mathrm{Pow}(M')$.

Proof. Let $M = (Q, \Sigma_p, \delta, q_0, \mathbb{F}_q, \tau)$ and $M' = (Q', \Sigma_p, \delta', q_0', \mathbb{F}_q, \tau')$. Define

$$N = (Q \times Q', \Sigma_p, \tilde{\delta}, (q_0, q_0'), \mathbb{F}_q, \tilde{\tau})$$

where $\tilde{\delta}((q,q'),s) = \delta(q,s) \times \delta'(q',s)$ and $\tilde{\tau}(q,q') = \tau(q) + \tau'(q')$. By construction, N is a DFAO. Let $w \in \Sigma^*$ be a valid base p expansion. We have that

$$\begin{aligned} f_N(w) &= \tilde{\tau}(\tilde{\delta^*}((q_0,q_0'),w)) \\ &= \tilde{\tau}(\delta^*(q_0,w),\delta'^*(q_0',w)) \\ &= \tau(\delta^*(q_0,w)) + \tau'(\delta^*(q_0',w)) \\ &= f_M(w) + f_{M'}(w). \end{aligned}$$

Hence, $f_N = f_M + f_{M'}$ and so $\mathrm{Pow}(N) = \mathrm{Pow}(M) + \mathrm{Pow}(M')$. We define ADD to return N on input M. □

In the following result, we will consider reversed base p expansions. This will not just be a matter of reversing valid base p-expansions, but we will also allow for leading and trailing zeroes. This is to make sense of base p addition with carries. More precisely, if $w_1 = s_1 \cdots s_m$ and $w_2 = t_1 \cdots t_m$, where $s_m = t_m = 0$, w_1 and w_2 both contain exactly one radix point in the same position k, we make the make the following definitions for $i \in \{1,\ldots,k-1\} \cup \{k+1,\ldots,m\}$.

$$\begin{aligned} c_0 &= 0 \\ u_i &= s_i + t_i + c_{i-1} \mod p \\ c_i &= 1 \text{ if } s_i + t_i + c_{i-1} \geq p \\ c_i &= 0 \text{ if } s_i + t_i + c_{i-1} < p \\ c_k &= c_{k-1} \end{aligned}$$

We say that $u_1 \cdots u_{k-1}.u_{k+1} \cdots u_m$ is the base p addition with carries of w_1 and w_2.

Lemma 1.3.80. *There is an algorithm* MULTIPLY *which takes as input two well-ordered DFAOs $\mathbb{X}$ and $\mathbb{Y}$ both having input alphabet Σ_p and output set $\mathbb{F}_q$, and outputs a well-ordered DFAO $\mathbb{W}$ with the same input alphabet and output set such that* $\mathrm{Pow}(\mathbb{W}) = \mathrm{Pow}(\mathbb{X})\mathrm{Pow}(\mathbb{Y})$.

Proof. Suppose that MULTIPLY is defined on minimal well-ordered DFAs. Denote this restriction of MULTIPLY by MULTIPLY_DFA. Let

$$\text{LINEAR_COMBINATION}(\mathbb{X}) = \{(a_i, \mathbb{X}_i) \mid i \in \{1,\ldots,1-q\}\}$$

and let

$$\text{LINEAR_COMBINATION}(\mathbb{Y}) = \{(a_i, \mathbb{Y}_i) \mid i \in \{1,\ldots,1-q\}\}.$$

Then

$$\mathrm{Pow}(\mathbb{X})\mathrm{Pow}(\mathbb{Y}) = \sum_{i=1}^{q-1}\sum_{j=1}^{q-1} a_i a_j \mathrm{Pow}(\mathbb{X}_i)\mathrm{Pow}(\mathbb{Y}_j).$$

Thus, MULTIPLY can be defined in the following way.

MULTIPLY$(\mathbb{X}, \mathbb{Y})$

1: $\{(a_i, \mathbb{X}_i) \mid i \in \{1, \ldots, 1-q\} \leftarrow$ LINEAR_COMBINATION$(\mathbb{X})$
2: $\{(a_i, \mathbb{Y}_i) \mid i \in \{1, \ldots, 1-q\} \leftarrow$ LINEAR_COMBINATION$(\mathbb{Y})$
3: $\mathbb{W} \leftarrow a_1 a_1$MULTIPLY_DFA$(\mathbb{X}_1, \mathbb{Y}_1)$
4: **for** $i \in \{2, \ldots, q-1\}$ **do**
5: **for** $j \in \{2, \ldots, q-1\}$ **do**
6: $\mathbb{W} \leftarrow$ ADD$(\mathbb{W}, a_i a_j$MULTIPLY_DFA$(\mathbb{X}_i, \mathbb{Y}_j))$
7: **return** $\mathbb{W}$

We will now define MULTIPLY_DFA. Suppose that $\mathbb{X}$ and $\mathbb{Y}$ are minimal well-ordered DFAs. Let $x = \mathrm{Pow}(\mathbb{X})$ and let $y = \mathrm{Pow}(\mathbb{Y})$. By definition of multiplication in Hahn fields, the coefficient of a term with value γ in xy is equal to the number of ways to write $r_1 + r_2 = \gamma$ with $r_1 \in \mathrm{supp}(x)$ and $r_2 \in \mathrm{supp}(y)$. Since these coefficients are in characteristic p, we can take this number modulo p. We will see that this amounts to counting the number of accepting paths modulo p in a certain NFA and then use Lemma 1.3.49 to conclude the result. To this end, let $M_x = \mathrm{REV}(\mathbb{X})$ and let $M_y = \mathrm{REV}(\mathbb{Y})$. Write $M_x = (Q_x, \Sigma_p, \delta_x, q_{0,x}, \mathbb{F}_q, \tau_x)$ and $M_y = (Q_x, \Sigma_p, \delta_x, q_{0,x}, \mathbb{F}_q, \tau_x)$. Let S be the subset of $\Sigma_p^* \times \Sigma_p^*$ consisting of pairs (w_1, w_2) with the following properties.

(1) w_1 and w_2 have the same length.

(2) w_1 and w_2 each end with 0.

(3) w_1 and w_2 each have a single radix point, and both are in the same position.

(4) After removing leading and trailing zeroes, w_1 and w_2 become the reversed valid base p expansions of some $i \in \mathrm{supp}(x)$ and $j \in \mathrm{supp}(y)$ respectively.

We will use Theorem 1.3.62 to show that S is a regular language over $\Sigma = \Sigma_p \times \Sigma_p$, under the identification of Σ^* with the subset of $\Sigma_p^* \times \Sigma_p^*$ where the coordinates have equal length.

To start, we will define an equivalence relation $\sim_x$ on Σ^* as follows. Let $q \in Q_x$ and denote by $E_q^{(1,x)}$ the set of strings $w = us_1 \cdots s_k v \in \Sigma^*$ for which the following hold.

(i) u and v are strings of only zeroes;

(ii) $0 \notin \{s_1, s_k\}$;

(iii) $\delta^*(q_{0,x}, s_1 \cdots s_k v) = q$;

(iv) $s_1 \cdots s_k$ is accepted by M_x.

Let $E_q^{(2,x)}$ be the set of strings defined as $E_q^{(1)}$, but with the fourth item replaced with

(iv') $s_1 \cdots s_k$ is not accepted by M_x.

We have that the set $\{E_q^{(i,x)} \mid i \in \{1,2\},\ q \in Q_x\}$ partitions Σ^*. Denote the equivalence relation given by this partitioning by $\sim_x$. By (iii), we have that $\sim_x$ is right-invariant. Since Q_x is finite, we have that $\sim_x$ is of finite index. We define $\sim_y$ in exactly the same way, replacing all instances of x with y.

Using $\sim_x$ and $\sim_y$, we now define an equivalence relation $\sim$ on Σ^* as follows. Let $w = (w_1, w_2) \in \Sigma^*$. If w_1 and w_2 both contain exactly one radix point in the same position, we say that w is of type A. If neither w_1 nor w_2 contains a radix point, say that w is of type B. If w is neither of type A nor of type B, we say that w is of type C. Let $w' = (w_1', w_2') \in \Sigma^*$. We define $w \sim w'$ to hold if w and w' are both of type C, or if the following hold.

(a) w is of the same type as w';

(b) $w_1 \sim_x w_1'$;

(c) $w_2 \sim_y w_2'$.

Since $\sim_x$ and $\sim_y$ are right-invariant and of finite index, so is $\sim$. It is immediate that S is the union of equivalence classes of $\Sigma^*/\sim$, namely the equivalence classes of elements $w = (w_1, w_2)$ of type A with $w_1 \in E_q^{(1,x)}$ and $w_2 \in E_{q'}^{(1,y)}$ for some $q \in Q_x$ and some $q' \in Q_y$. We conclude that S is regular.

We will now construct an explicit DFA $M = (Q, \Sigma, \delta, q_0, F)$ which accepts S. This is essentially an application of Corollary 4.1.9 in [AS03]. Let Q be a set of representatives of $\Sigma^*/\sim$. Such a set can be obtained by considering strings of bounded length, as in the definition of RELEVANT_STATES. For $w \in Q$ and $s \in \Sigma$, let $\delta(w, s) = w'$, where $ws \sim w'$. Let q_0 be the element in Q which is equivalent to the empty string under $\sim$. Let $F = Q \cap S$. By construction, we have that M accepts S.

Informally, the DFA M can be seen to accept the pairs of reversed base p expansions of the exponents in $\mathrm{supp}(x) \times \mathrm{supp}(y)$ which are well set up for adding

these pairs together under base p addition with carries. We will now construct an NFA $M' = (Q', \Sigma_p, \delta', q_0', F')$ which captures this addition. Let $Q' = Q \times \{0, 1\}$, let $q_0' = (q_0, 0)$ and let $F' = F \times \{0\}$, where F is the set of accepting states of M. To define δ', let $(q, i) \in Q'$ and consider the following cases.

1. If $s \in \{0, \ldots, p-1\}$, we include $(q', 0)$ (resp. $(q', 1)$) in $\delta'((q, i), s)$ if there exists a pair $(t, u) \in \{0, \ldots, p-1\}^2$ with $t + u + i < p$ (resp. $t + u + i \geq p$) and $t + u + i \equiv s \mod p$ such that $\delta(q, (t, u)) = q'$.

2. If s is equal to the radix point, we include (q', i) in $\delta((q, i), s)$ if $\delta(q, (s, s)) = q'$, and we never include $(q', 1 - i)$.

It is shown in the proof of [Ked06, Lemma 2.2.2] that the number of accepting paths of $w \in \Sigma_p^*$ in M' is equal to the number of pairs $(w_1, w_2) \in S$ which sum to w with its leading and trailing zeroes under ordinary base p addition with carries. Let $N = \text{ACCEPTING_PATHS}(M')$, as in Lemma 1.3.49. So the function $f_N(w)$ equals the number of accepting paths of w in M' modulo p.

A priori, there might be $(w_1, w_2) \in S$ which sum to a reversed base p expansion of γ even though (w_1, w_2) does not sum to w, since we need to take into account leading and trailing zeroes. Appending leading zeroes to w will account for more possible $(w_1, w_2) \in S$. From [Ked06], we get a bound to how many zeroes we need to append. To make this more precise, let m be greater than the number of states of M and suppose that w begins with m leading zeroes. In the proof of [Ked06, Lemma 2.2.2] it is shown that $0w$ then has the same number of accepting paths as w.

We conclude that the function that, given the reversed valid base p expansion of a number $\gamma \in \frac{1}{p^\infty}\mathbb{N}$, computes the mod p reduction of the number of ways to write $\gamma = i + j$ with $(i, j) \in \text{supp}(x) \times \text{supp}(y)$ is given by a DFAO $N' = (\tilde{Q}', \Sigma_p, \tilde{\delta}', \tilde{q}_0', \mathbb{F}_p, \tilde{\tau}')$ which is constructed using $N = (\tilde{Q}, \Sigma_p, \tilde{\delta}, \tilde{q}_0, \mathbb{F}_p, \tilde{\tau})$ in the following way. Let $G = (V, E)$ be the transition graph of N. We set the initial state of N' to be $\tilde{q}_0' = \tilde{\delta}^*(\tilde{q}_0, m \cdot 0)$, where $m \cdot 0$ denotes the string with m zeroes. We let the transition graph of N' be $G_{\tilde{q}_0'}$. For any state q of N', we set $\tilde{\tau}'(q) = \tilde{\tau}(\tilde{\delta}(q, 0))$. In other words, N' amounts to appending m leading zeroes and one trailing zero to a string and then running the result through N. Finally, having MULTIPLY_DFA returning $\mathbb{W} = \text{REV}(N')$ on input $(\mathbb{X}, \mathbb{Y})$ gives the desired result. □

Remark 1.3.81. For any $i \in \mathbb{N}$, let M_i be the DFAO illustrated after Definition 1.3.54, such that the accepted string $s_1 \cdots s_n$ is a valid base p expansion of i. By construction, we then have that $\text{Pow}(M_i) = t^i$. By Lemma 1.3.80, this implies that

for a DFAO M, we have $\mathrm{Pow}(\textsc{multiply}(M_i, M)) = t^i \mathrm{Pow}(M)$. We can thus extend the notation aM for $a \in \mathbb{F}_p$ to allow for $a = \sum_{j=0}^{s} a_j t^j \in \mathbb{F}_p[t]$, by letting aM be the DFAO defined by adding together the DFAOs $a_j M_j$ using the algorithm ADD.

Remark 1.3.82. There is an algorithm $\textsc{power}^i$ for any $i \in \mathbb{N}$ which takes as input a well-ordered DFAO M and returns a DFAO N such that $\mathrm{Pow}(N) = \mathrm{Pow}(M)^i$. The sequence of such algorithms $(\textsc{power}^i)_{i\in\mathbb{N}}$ is defined recursively by letting $\textsc{power}^0(M) = \mathbb{1}$ and

$$\textsc{power}^{i+1}(M) = \textsc{multiply}(M, \textsc{power}^i(M)).$$

Remark 1.3.83. There is an algorithm IS_ROOT which takes as input a polynomial $f(X) \in \mathbb{F}_p[t][X]$ and a DFAO $\mathbb{X}$ and returns TRUE if $f(\mathrm{Pow}(\mathbb{X})) = 0$ and FALSE otherwise. It is defined as follows.

IS_ROOT$(f = \sum_{i=0}^{n} a_i X^i, \mathbb{X})$

$\mathbb{W} \leftarrow a_0 \mathbb{1}$
for $i \in \{1, \dots, n\}$ **do**
  $\mathbb{X}^i \leftarrow \textsc{power}^i(\mathbb{X})$
  $\mathbb{W} \leftarrow \textsc{add}(\mathbb{W}, a_i \mathbb{X}^i)$
if RELEVANT_STATES$(\mathbb{W}) = \emptyset$ **then**
  return TRUE
return FALSE

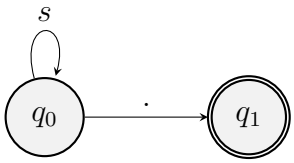
1.3.8 Arithmetic of finite automata through an example

The effectiveness of the arithmetic on DFAOs, as obtained by Lemma 1.3.79 and Lemma 1.3.80, is crucial for our coming decidability results. We will therefore illustrate this procedure, in particular multiplication, in a simplified example using the transition graphs.

Let $p > 2$ and consider the element $x = \sum_{n\geq 0} t^{1-1/p^n} \in \mathbb{F}_p((t^{1/p^\infty}))$. We will compute the DFAO corresponding to

$$x^2 = \sum_{\gamma} \sum_{\substack{\gamma_1,\gamma_2 \in \mathrm{supp}(x) \\ \gamma_1+\gamma_2=\gamma}} t^\gamma.$$

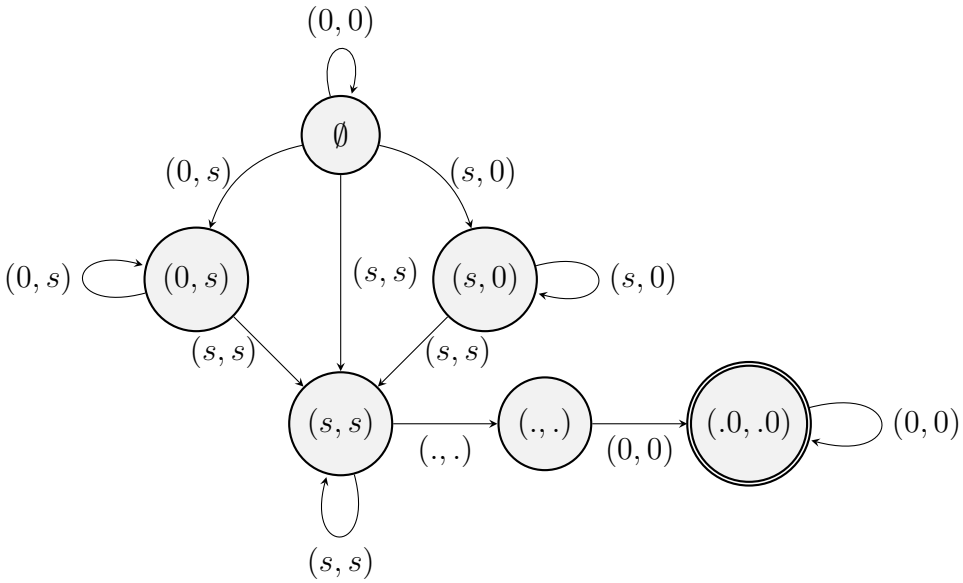
We start with the DFA accepting the reversed base p expansions of the support of x. As above, we will omit all edges that do not lead to accepting paths, and all states only reached by such paths. Let $s = p - 1$. The DFA for x is then as follows.



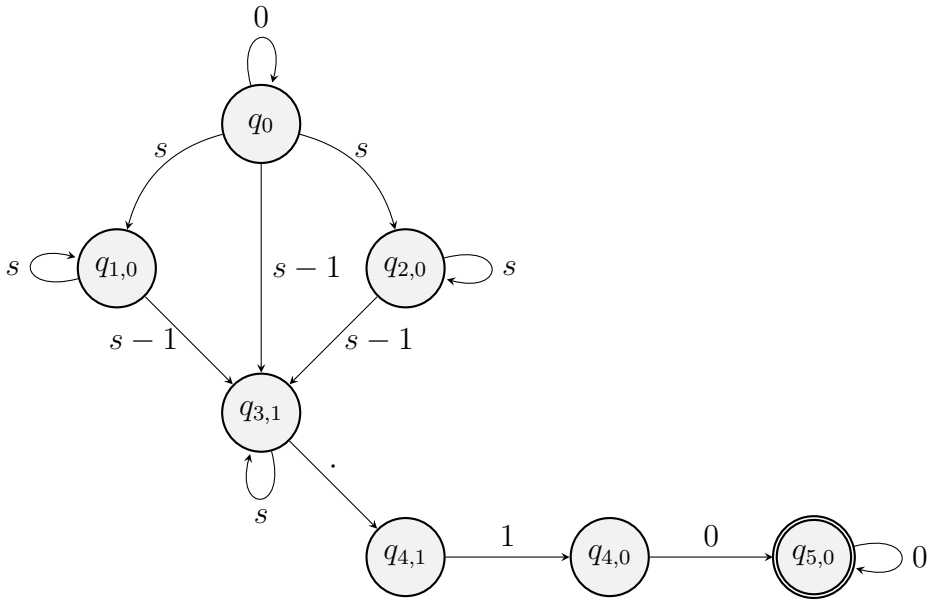
We get that

$$\{\emptyset, (0,s), (s,0), (s,s), (.,.), (.0,.0), (.0,0.)\}$$

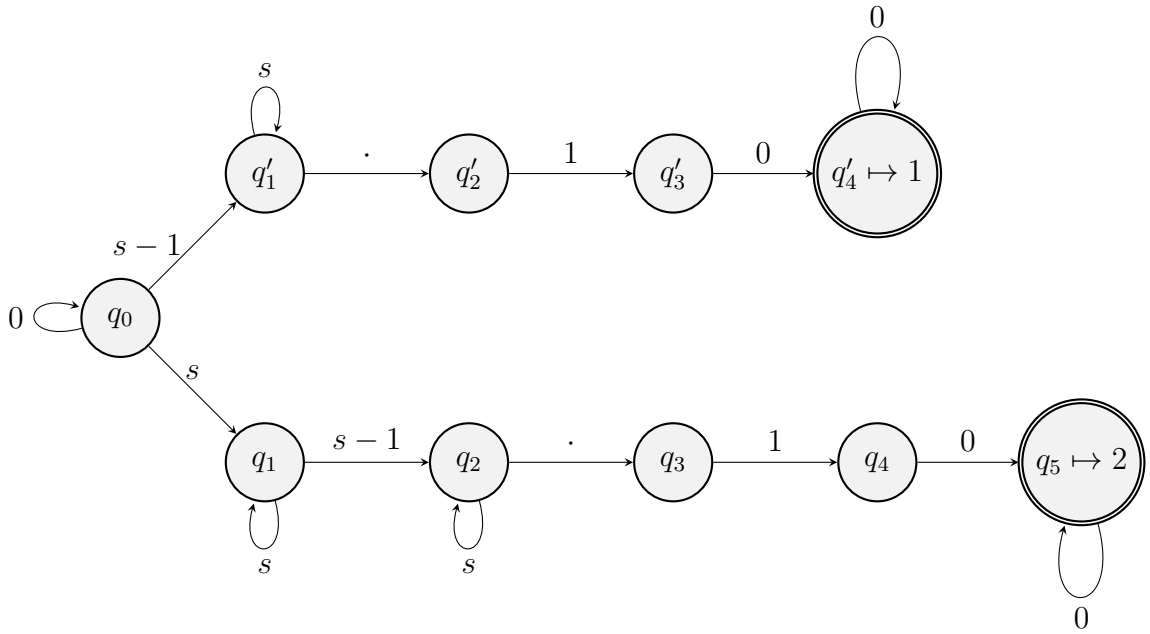
is a set of representatives of the equivalence classes of $\Sigma^*/\sim$, with the notation from the proof of Lemma 1.3.80. From this, we obtain the DFA where accepting paths correspond to possible expansions in the support of (x,x), omitting the state $(.0,0.)$ which is not relevant.



The following NFA now captures addition base p with carries of elements in the support as an NFA.



Finally, counting the number of accepted paths in the previous NFA is captured in the following DFAO.



Given an element $\gamma \in \frac{1}{p^\infty}\mathbb{N}$, the coefficient of t^γ in x^2 is now given by tracing the base p expansion of γ in the last DFAO. If q is the final state under this procedure, the coefficient is then 1 respectively 2 if q is equal to q'_4 or q_5 respectively, and it is equal to 0 otherwise.

Chapter 2

Algebraicity of generalised power series

2.1 On the support of algebraic elements

It was shown by Puiseux, and implicitly apparent in work by Newton, that when $\mathbb{F}$ has characteristic 0 the algebraic closure of $\overline{\mathbb{F}}((t))$ is the direct limit of $(\overline{\mathbb{F}}((t^{1/n})))_{n\in\mathbb{N}}$ [Eis95, p. 295]. Another way to formulate this fact is by the following two properties about the relative algebraic closure K of $\overline{\mathbb{F}}((t))$ in $\overline{\mathbb{F}}((t^{\mathbb{Q}}))$:

1. The support of elements in K have order type at most ω.
2. Elements in K cannot have infinite ramification in the support, in the sense made more precise in Definition 2.1.16.

Note that the first property implies that no element in K can have bounded support, since this would give an element with support of order type $\omega + 1$ by adding a suitable power of t. Both these properties are contradicted in characteristic p, for example by the element $1 + \sum_{n\in\mathbb{N}} t^{-1/p^n}$. However, in this section we use a transfinite approximation method to obtain the following modified properties in positive characteristic:

1. The support of elements in K have order type strictly smaller than ω^ω.
2. Elements in K cannot have infinite ramification away from p in the support.

The second item is due to Rayner and we will provide an alternative proof, originally appearing in [Lis21]. The first item seems to not have been treated in the literature, though the order type of the support of elements in Hahn fields of characteristic zero is studied in [KL19].

2.1.1 Approximating roots

We start this section by describing a method introduced in [Lam86] for constructing roots in Hahn fields to polynomials over the underlying field of formal Laurent series. For this, we need a version of Taylor expansions in positive characteristic.

Definition 2.1.1. *Let K be a field and let*

$$f(X) = \sum_{i=0}^{n} a_i X^i \in K[X].$$

Then the k-th Hasse derivative of f is defined as

$$D^{(k)} f(X) := \sum_{i=k}^{n} \binom{i}{k} a_i X^{i-k} \in K[X].$$

Remark 2.1.2. We will not consider derivatives of formal power series. Thus, with K being a field of power series, $f \in K[X]$ and $x \in K$, we will write $D^{(k)} f(x)$ in place of $(D^{(k)} f)(x)$. We will also omit parenthesis in expressions of the form $(D^{(k)} f(x))g(X)$, since we will never consider expressions of the form $D^{(k)}(f(x)g(X))$.

Theorem 2.1.3 (Taylor expansion)**.** *Let K be a field and let $f(X) \in K[X]$ be of degree n and let $\lambda \in K$. Then*

$$f(X) = \sum_{k=0}^{n} D^{(k)} f(\lambda)(X - \lambda)^k.$$

Proof. By linearity of the Hasse derivative, it is enough to show the statement for $f(X) = X^n$. We have

$$\begin{aligned} \sum_{k=0}^{n} D^{(k)} f(\lambda)(X - \lambda)^k &= \sum_{k=0}^{n} \binom{n}{k} \lambda^{n-k} (X - \lambda)^k \\ &= ((X - \lambda) + \lambda)^n \\ &= X^n, \end{aligned}$$

and we are done. □

To fix some notation, let $\mathbb{F}$ be an algebraically closed field of characteristic p, let Γ be a divisible ordered abelian group, and let

$$f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{F}((t^\Gamma))[X].$$

With $x \in \mathbb{F}((t^\Gamma))$ and $i \in \{1, \ldots, n\}$, we define

$$g_{i,x}(X) := D^{(i)}f(x)X^i.$$

Let $b_{i,x}t^{\rho_{i,x}}$, with $b_{i,x} \in \mathbb{F}$, denote the initial term of $D^{(i)}f(x)$. To clarify the relationship between $g_{i,x}$ and $b_{i,x}t^{\rho_{i,x}}$, we have that $g_{i,x}(X) = (b_{i,x}t^{\rho_{i,x}} + z)X^i$, where $z \in \mathbb{F}((t^\Gamma))$ is of valuation strictly greater than $\rho_{i,x}$.

We now define the function $\gamma_{i,x} : \Gamma \cup \{\infty\} \to \Gamma \cup \{\infty\}$ by letting $\gamma_{i,x}(r) = \rho_{i,x} + ir$ for $r \in \Gamma$ and $\gamma_{i,x}(\infty) = \infty$. In particular, we get that $vg_{i,x}(y) = \gamma_{i,x}(r)$ for any $y \in \mathbb{F}((t^\Gamma))$ of valuation r. Let

$$\gamma_x(r) := \min_{i \in \{1,\ldots,n\}} \left\{\gamma_{i,x}(r)\right\}$$

and let

$$J_x(r) := \left\{i \in \{1, \ldots, n\} \mid \gamma_{i,x}(r) = \gamma_x(r)\right\}.$$

By construction, we have that $vg_{i,x}(y) > \gamma_x(r)$ for any $i \notin J_x(r)$. This implies that

$$v\left(\sum_{i=1}^{n} g_{i,x}(\zeta t^r)\right) \geq \gamma_x(r), \tag{2.1}$$

with equality if and only if $\sum_{i \in J_x(r)} b_{i,x} \neq 0$.

Suppose now that x is a root of f and consider an approximation $w = x_{<\lambda}$ of x. We want to find $r \in \Gamma$ and $\zeta \in \mathbb{F}$ such that $w + \zeta t^r$ is a better approximation of some root $\alpha \in \mathbb{F}((t^\Gamma))$ of f such that $\alpha_{<\lambda} = w$. To do this, we will find ζ and r such that $vf(w) < vf(w + \zeta t^r)$, and then proceed by transfinite recursion. Let r be such that $\gamma_w(r) = vf(w)$. For any $\zeta \in \mathbb{F}$, we have the equality

$$f(w + \zeta t^r) = f(w) + \sum_{i=1}^{n} g_{i,w}(\zeta t^r).$$

If $bt^{\gamma_w(r)}$ is the initial term of $f(w)$, we let ζ be such that

$$\sum_{i \in J_w(r)} b_{i,w}\zeta^i = -b \tag{2.2}$$

to get that $vf(w + \zeta t^r) > \gamma_w(r)$, as we wanted. We capture this procedure in the following definition, using the same notation as above.

Definition 2.1.4. *Let $f(X) \in \mathbb{F}((t^\Gamma))[X]$ and let $w \in \mathbb{F}((t^\Gamma))$ be an approximation of a root of f. We say that ζt^r is an **approximation term** for w with respect to f if $w_{<r} = w$, if $\gamma_w(r) = vf(w)$, and if $\zeta \in \mathbb{F}$ satisfies the equality* (2.2).

As mentioned, successively adding approximation terms eventually gives a root to f. More precisely, we define a transfinite recursion procedure as follows. Let $w_0 := w$. For any ordinal $\sigma > 0$ such that $f(w_\lambda) \neq 0$ for all $\lambda < \sigma$, let

$$w_\sigma = w + \sum_{\lambda<\sigma} \zeta_\lambda t^{r_\lambda}$$

where $\zeta_\lambda t^{r_\lambda}$ is a fixed approximation term for w_λ with respect to f. We then get the following.

Lemma 2.1.5. *There is an ordinal σ such that $f(w_\sigma) = 0$.*

Proof. It is enough to show that $vf(w_\sigma) > vf(w_\tau)$ for all ordinals σ and τ such that $\sigma > \tau$. Indeed, if this inequality holds but no w_σ is a root of f, then by taking σ to be an ordinal of cardinality strictly greater than $|\Gamma|$, we get that $\big(vf(w_\lambda)\big)_{\lambda\leq\sigma}$ is a strictly increasing sequence of cardinality strictly greater than $|\Gamma|$ in Γ.

Let $\sigma > \tau$. We note that

$$w_\sigma - w_\tau = w + \sum_{\lambda<\sigma} \zeta_\lambda t^{r_\lambda} - \left(w + \sum_{\lambda<\tau} \zeta_\lambda t^{r_\lambda} \right) = \sum_{\tau\leq\lambda<\sigma} \zeta_\lambda t^{r_\lambda}.$$

Therefore, we get

$$f(w_\sigma) = f\left(w_\tau + \sum_{\tau\leq\lambda<\sigma} \zeta_\lambda t^{r_\lambda} \right) = f(w_{\tau+1}) + \sum_{i=1}^{n} g_{i,w_{\tau+1}} \left(\sum_{\tau<\lambda<\sigma} \zeta_\lambda t^{r_\lambda} \right).$$

Since $vf(w_{\tau+1}) > vf(w_\tau)$ by construction, and since

$$v\left(\sum_{i=1}^{n} g_{i,w_{\tau+1}} \left(\sum_{\tau<\lambda<\sigma} \zeta_\lambda t^{r_\lambda} \right) \right) \geq \gamma_{w_{\tau+1}}(r_{\tau+1}) = vf(w_{\tau+1}),$$

we conclude that $vf(w_\sigma) > vf(w_\tau)$. □

Remark 2.1.6. Even if w is not the approximation of a root of f, we can still use the transfinite recursion procedure to find a root to the polynomial $f(w+X)$. Hence, we obtain a sequence $(\zeta_\lambda t^{r_\lambda})_{\lambda<\sigma}$ with r_λ strictly increasing such that $w + \sum_{\lambda<\sigma} \zeta_\lambda t^{r_\lambda}$ is a root of f. In particular, we find the possible initial terms of roots of f as the possible approximation terms for 0 with respect to f, i.e. by finding ζt^r such that the initial term of $\sum_{k=1}^{n} D^{(k)} f(0)(\zeta t^r)^k$ cancels the initial term of $f(0)$.

While successively adding approximation terms gives a root of f, we will see that it is not a sufficient procedure to recover all the roots. Using the same notation as above, and with x being a root of f, suppose now that $r \in \Gamma$ is such that $x_{\leq r}$ is a better approximation of x than w, as defined in the beginning of Section 1.3.3. In particular, if $\zeta \in \mathbb{F}$ is such that $x_{\leq r} = w + \zeta t^r$, then $\zeta \neq 0$. In this situation, we can write $x = w + \zeta t^r + y$, with $v(y) > r$. We have the equality

$$f(w + \zeta t^r + y) = f(w) + \sum_{i=1}^{n} g_{i,w}(\zeta t^r + y)^i.$$

Since $v(y) > r$, we have that $b_{i,w}\zeta^i t^{\rho_{i,w}+ir}$ is the initial term of both $g_{i,w}(\zeta t^r)^i$ and $g_{i,w}(\zeta t^r + y)^i$. In particular, we have $vg_{i,w}(\zeta t^r) = vg_{i,w}(\zeta t^r + y) = \gamma_{i,w}(r)$.

Since x is assumed to be a root of f, we have

$$vf(w) = v\left(\sum_{i=1}^{n} g_{i,w}(\zeta t^r + y)\right). \tag{2.3}$$

Using inequality (2.1), this implies that

$$vf(w) \geq \gamma_w(r). \tag{2.4}$$

If inequality (2.4) is strict, then equality (2.3) gives

$$v\left(\sum_{j \in J_w(r)} g_{j,w}(\zeta t^r + y)\right) > \gamma_w(r).$$

In particular, this holds if $f(w) = 0$. For any $j \in J_w(r)$, the term of valuation $\gamma_w(r)$ in $g_{j,w}(\zeta t^r + y)$ is simply the initial term, i.e. $b_{j,w}\zeta^j t^{\gamma_{j,w}(r)}$. Furthermore, by deinifion of $J_w(r)$, we have that this term in fact is equal to $b_{j,w}\zeta^j t^{\gamma_w(r)}$. Hence, we conclude that ζ satisfies

$$\sum_{j \in J_w(r)} b_{j,w}\zeta^j = 0. \tag{2.5}$$

Consequently, $|J_w(r)| > 1$, since we otherwise would have $\zeta = 0$.

Assume now that (2.4) is an equality. Then, we are exactly in the situation preciding Definition 2.1.4, and ζt^r is an approximation term for w with respect to f, i.e. ζ satisfies 2.2.

We summarise the discussion in the following lemma.

Lemma 2.1.7. *Let $f(X) \in \mathbb{F}((t^\Gamma))$. If $w + \zeta t^r$ is a better approximation than w of some root x of f, then*

(a) ζ satisfies (2.5) and $|J_w(r)| > 1$ or

(b) ζt^r is an approximation term for w with respect to f.

In some non-trivial cases, we can use approximation terms to directly determine if a polynomial has a root in a particular field or not, as illustrated by the following example.

Example 2.1.8. Let

$$f(X) = X^3 - X^2 - \frac{1}{t} \in \mathbb{F}_3(t)[X].$$

We will show by induction that there is a root

$$x \in \overline{\mathbb{F}}_3((t^{\mathbb{Q}}))$$

such that each term of x is of the form at^γ with $a \in \mathbb{F}_3$ and $\gamma \in \frac{1}{3^\infty}\mathbb{Z}$, i.e. such that $x \in \mathbb{F}_3((t^{1/3^\infty}))$. For any such root, we have by Remark 2.1.6 that the initial term is equal to $t^{-1/3}$. Assume that we have an approximation $w = x_{<\lambda} \in \mathbb{F}_3((t^{1/p^\infty}))$ for some ordinal λ. If $f(w) = 0$ we are done, so assume $f(w) \neq 0$. Let ζt^r be an approximation term for w with respect to f. Then, we have that $vf(w) = \min\{r - 1/3,\ 2r,\ 3r\}$. By definition of approximation term, we also have that $r > v(w)$. So $2r > r - 1/3$ and $vf(w) \neq 2r$. Suppose that $r - 1/3 = 3r$. Then $r = -1/6$, so $vf(w) = -1/2$. This is a contradiction, since $w \in \mathbb{F}_3((t^{1/3^\infty}))$. Hence, we have that $vf(w)$ is equal to either $r - 1/3$ or to $3r$, but not both.

Let $\xi t^{vf(w)}$, with $\xi \in \mathbb{F}_3$. If $vf(w) = r - 1/3$, we let $\zeta = \xi/2$. If $vf(w) = 3r$, we set $\zeta^3 = -\xi$, i.e. $\zeta = -\xi$. In both cases, $\zeta t^r \in \mathbb{F}_3(t)^{1/3^\infty}$. This shows that each approximation in the recursion procedure preceding Lemma 2.1.5 lies in $\mathbb{F}_3((t^{1/3^\infty}))$, so we conclude that the root w_σ in the lemma also lies in $\mathbb{F}_3((t^{1/3^\infty}))$.

In this example, we can also use Lemma 2.1.7 to determine the minimal Hahn field containing all roots of f. Consider the following functions, as in the discussion preceding Defintion 2.1.4 recalling that $v(w) = -1/3$ for any non-zero approximation w of a root x of f.

$$\begin{aligned}\gamma_{1,w}(r) &= -1/3r;\\ \gamma_{2,w}(r) &= 2r;\\ \gamma_{3,w}(r) &= 3r.\end{aligned}$$

Since these function do not depend on w, we will just write γ_1, γ_2 and γ_3. Let ζt^r be such that $w = \zeta t^r$ is a better approximation than w of some root x of f. Assuming

that ζt^r is not an approximation term for w with respect to f, we get by Lemma 2.1.7 that $|J_w(r)| > 1$. Pairs of the lines defined by the γ_i intersect at $r = -1/6$, $r = -1/3$ and $r = 0$. For $r = -1/3$ and $r = 0$, we have that $|J_w(r)| = 1$. For $r = -1/6$ however, we have that $J_w(r) = \{1, 3\}$. Since ζ satisfies

$$-2\zeta + \zeta^3 = 0,$$

we have that $\zeta \in \{\sqrt{2}, \sqrt{2}\}$. Therefore, $w + \zeta t^r \in K := \mathbb{F}_3(\sqrt{2})((t^{\frac{1}{2\cdot 3^\infty}}))$. Repeating the argument above for the existence of a root in $\mathbb{F}_3((t^{1/3^\infty}))$ with $w' = w + \zeta t^r$ in place of w shows that f has a root $w'_\sigma \in K$.

Since the choice of approximation term for valuation r for w is unique when $|J_w(r)| = 1$, and since we showed that there was no approximation term with valuation $r = -1/6$, we get that w_σ and w'_σ are the unique roots x and y such that $x_{\leq -1/6} = w$ and $y_{\leq -1/6} = w + \zeta t^r$. Since any root of f in $\overline{\mathbb{F}}_3((t^{\mathbb{Q}}))$ must have w as an initial sum, we get that the third root α of f in $\overline{\mathbb{F}}_3((t^{\mathbb{Q}}))$ must satisfy $\alpha_{\leq r} = w - \zeta t^r$. Hence, α is obtained by repeating the recursion procedure for $w - \zeta t^r$, which shows that $\alpha \in K$. Conversely, any Hahn field containing w'_σ and α will contain K as a subfield.

Remark 2.1.9. The reason why the recursion procedure cannot be used immediately for arbitrary polynomials is that it can be difficult to compute $D^{(n)}f(x_{<\lambda})$. More precisely, since the truncations of $x_{<\lambda}$ give a pseudo convergent sequence of algebraic type, we might have that $vD^{(n)}f(x_{<\tau}) < vD^{(n)}f(x_{<\lambda})$ for any $\tau < \lambda$, so $D^{(n)}f(x_{<\lambda})$ is not computable by finite approximation. Note that Krasner's Lemma does not work in this situation, since the value of $D^{(n)}f(x_{<\tau})$ might be bounded. However, if the Hasse derivatives are constant, the situation becomes easier, as we will see in the special case of additive polynomials.

2.1.2 Order type of the support of algebraic elements

When K has characteristic p, then $P \in K[X]$ is additive if and only if it is of the form

$$\sum_{i=0}^{n} a_i X^{p^i}.$$

In this case, the $D^{(p^k)}P(X) = a_k X^{p^k}$ and $D^{(\ell)}P(X) = 0$ for ℓ not a power of p. Since these Hasse derivatives are constant, we get in particular that the functions $\gamma_{i,w}$ and the set $J_w(r)$ in Section 2.1.1 do not depend on w. When P is given, we will thus only write γ_i and $J(r)$. Furthermore, if w is the approximation of a root of P, using

the Taylor approximation of P to find an approximation term ζt^r for w with respect P just amounts to writing

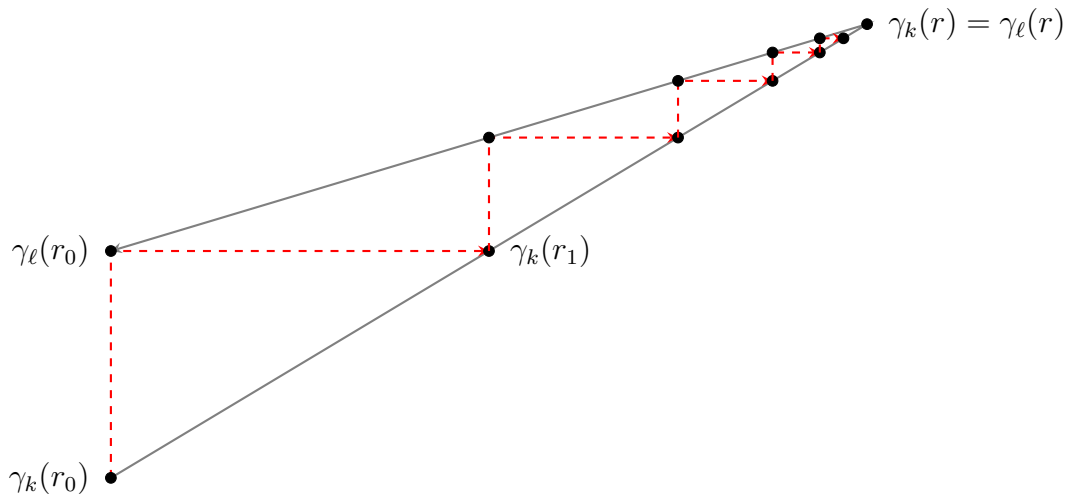
$$P(w + \zeta t^r) = P(w) + P(\zeta t^r).$$

As we will see, this implies that the material in Section 2.1.1 has an elementary geometric interpretation which simplifies computation. This is made possible with the following definition.

Definition 2.1.10. *Let $\mathbb{F}$ be a field of characteristic p and let Γ be an ordered abelian group. Let $P(X) \in \mathbb{F}((t^\Gamma))[X]$ be an additive polynomial. We say that $r \in \mathbb{R} \cup \{\infty\}$ is a* ***point of intersection of*** *P if $|J(r)| > 1$.*

Remark 2.1.11. The number of points of intersection of P is bounded by the maximal number of intersection points of $n+1$ lines, including the point at infinity, i.e. by $n(n+1)/2+1$. Furthermore, there is an algorithm which takes as input an additive polynomial $P(X) \in \mathbb{F}_p[t][X]$ and outputs the points of intersection of P. This can be seen simply by noting that the γ_i in this case are lines with integer slopes.

Let P be an additive polynomial, let x be a root of P with value r_0, and let r be the minimal point of intersection P larger than r_0. With Definition 2.1.10 in mind, the recursion procedure of approximating a root of P via approximation terms can be illustrated as follows.



The illustration suggests the procedure converges to r, so that the minimal element in the support of x larger than or equal to r would be r_ω. This is an instance of a more general fact which is captured in the following lemma.

Lemma 2.1.12. *Let*

$$P(X) = \sum_{i=0}^{m} a_i X^{p^i} \in \mathbb{F}_p((t))[X]$$

be an additive polynomial and let

$$x = \sum_{\tau<\sigma} b_\tau t^{r_\tau} \in \overline{\mathbb{F}}_p((t^{\mathbb{Q}}))$$

be a root of P with support $\{a_\tau \mid \tau < \sigma\}$. Let $\lambda < \sigma$ be such that $\sigma \geq \lambda \cdot \omega$. Then, $\lim_{i\to\infty} r_{\lambda\cdot i}$ is a point of intersection of P.

Proof. Let $r = \sup_{i\in\mathbb{N}}\{r_{\lambda\cdot i}\} \in \mathbb{R}\cup\{\infty\}$ and let $w = x_{<r}$. While r might not be in $\mathbb{Q}$, it makes sense to talk about the set $J(r)$, by extending the functions γ_i to $\mathbb{R}\cup\{\infty\}$ in the natural way. Let $(s_i)_{i\in\mathbb{N}}$ be a subsequence of $(r_{\lambda\cdot i})_{i\in\mathbb{N}}$ such that $x_{\leq s_i} - x_{<s_i}$ is an approximation term for $x_{<s_i}$ with respect to P, for every i. Such a subsequence exists, since $|J(r_\tau)| > 1$ except when r_τ is a point of intersection of P. In particular, we have that $\lim_{i\to\infty} s_i = r$. Let b_i' be such that $x_{\leq s_i} - x_{<s_i} = b_i' t^{s_i}$. By definition, we then have that $vP(b_i' t^{s_i}) = vP(x_{<s_i})$. Let ℓ_i and k_i be such $vP(b_i' t^{s_i}) = \gamma_{\ell_i}(s_i)$ and $\gamma_{k_i} = vP(x_{<s_i})$. In particular, $\ell_i \neq k_i$. We can assume that neither ℓ_i nor k_i depend on i, possibly by replacing (s_i) with a subsequence. Write $\ell = \ell_i$ and $k = k_i$. Since s_i converges to r, we can let $M \in \mathbb{N}$ be such that $\gamma_j(s) > \gamma_\ell(r)$ for all $j \notin J(r)$ and all $s > s_M$. Similarly, we can let $N \in \mathbb{N}$ be such that $\gamma_\ell(s_n) > \gamma_j(s_M)$ for all $n > N$ and all $j \notin J(r)$. Now, let $n > N$ and let $s < r$ be such that $\gamma_k(s) = \gamma_\ell(s_n)$. If $k \notin J(r)$, then $\gamma_\ell(s_n) > \gamma_k(s_M)$. So $s > s_M$, but then $\gamma_k(s) > r$, which contradicts $\gamma_k(s) = \gamma_\ell(s_n)$. Hence, $k \in J(r)$ and r is a point of intersection of P. □

Remark 2.1.13. Note that Lemma 2.1.12 only uses that the Hasse derivatives of P are constant. One could thus formulate a similar statement for more general polynomials where this holds.

We can now determine a bound for the order type of elements in $\overline{\mathbb{F}}_p((t^{\mathbb{Q}}))$ that are algebraic over $\mathbb{F}_p((t))$.

Theorem 2.1.14. *Let $x \in \overline{\mathbb{F}}_p((t^{\mathbb{Q}}))$ be algebraic over $\mathbb{F}_p((t))$. Then x has order type at most ω^m, where $m = n(n+1)/2 + 1$ and n is the degree of x over $\mathbb{F}_p((t))$.*

Proof. Let f be the minimal polynomial of x over $\mathbb{F}_p((t))$ and let $P(X) = \sum_{k=0}^{n} a_k X^{p^k}$ be an additive polynomial divisible by f, as in Lemma 1.3.16. By induction and Lemma 2.1.12, the order type of x is at most ω^m, where m is the number of points of intersection of P. As noted in Remark 2.1.11, m is bounded above by $n(n+1)/2+1$, which proves the theorem. □

Remark 2.1.15. The idea with Theorem 2.1.14 is give a general bound to algebraic elements. Given f, we can obtain a sharper bound by considering the actual points of intersection of the corresponding additive polynomial.

2.1.3 A result by Rayner

Definition 2.1.16. *Let $x \in \mathbb{F}((t^\Gamma))$. Let $r \in \Gamma$ be in the support of x. Let S be the support of $x_{<r}$. We say that a prime q **ramifies** at r in x if there exists a positive integer K such that $r = \frac{a}{bq^K}$ and, for any $k \geq K$ there is no element $s = \frac{a'}{b'q^k} \in S$, where a, a', b and b' are all coprime to q. When x is clear from context, we will just say that q ramifies at r.*

Definition 2.1.17. *Let $x \in \mathbb{F}((t^\Gamma))$. Let $r \in \Gamma$ and suppose that $x_{\leq r} - x_{<r} = \zeta t^r$ is non-zero. Let K be the minimal subfield of $\mathbb{F}$ such that $x_{<r} \in K((t^\Gamma))$. We say that ζ **expands** x at r if $\zeta \notin K$.*

As mentioned, there are elements in the relative algebraic closure of $\mathbb{F}_p(t)$ in $\mathbb{F}_p((t^{1/p^\infty}))$ that require infinite ramification for p. It was established by Rayner that this is not the case for primes different than p [Ray68]. We will give a new proof of this result using additive polynomials. This method will also give an effective bound for the ramification away from p, which will be necessary in Chapter 3. Similarly, we will show that expanding away from p:th roots is bounded, in a sense made more precise below.

Let $P(X) = \sum_{i=0}^n a_i X^{p^i} \in \mathbb{F}_p(t)[X]$ be an additive polynomial and write

$$I_P := \{i \in \{0, \dots, n\} \mid a_i \neq 0\}.$$

As above, we denote by γ_i the function on $\mathbb{Q} \cup \{\infty\}$ sending r to $p^i r + v(a_i)$ for $i \in I_P$.

Theorem 2.1.18. *Let $\mathbb{F}$ be a field of characteristic p and let $P(X) \in \mathbb{F}_p(t)[X]$ be an additive polynomial. Let q be a prime different from p. If $x \in \mathbb{F}((t^\mathbb{Q}))$ is a root of P and $r \in \mathbb{Q}$ is such that q ramifies at r in x, then r is a point of intersection of P.*

Proof. Write $P = \sum_{i=0}^n a_i X^{p^i}$. Let $r \in \Gamma$ be in the support of x and suppose that $q \neq p$ is a prime which ramifies in x at r. Let $\zeta t^r = x_{\leq r} - x_{<r}$. Let $c_1 t^{\gamma_1}$ be the initial term of $P(x_{<r})$ and let $c_2 t^{\gamma_2}$ be the initial term of $P(\zeta t^r)$. If ζt^r is an approximation term for $x_{<r}$, we have that $\gamma_\ell(r) = \gamma_2$ for some $\ell \in J(r)$. This implies that

$$r = \frac{\gamma_2 - v(a_\ell)}{p^\ell}.$$

By the assumption on q, this is only possible if

$$\gamma_2 - v(a_\ell) = \frac{a}{bq^k}$$

for some $a, b \in \mathbb{Z}$ coprime to q and some positive integer k. On the other hand, since P is additive, there is some $j \in I_P$ and some r_τ in the support of $x_{<r}$ such that

$$\gamma_2 = \gamma_j(r_\tau).$$

This gives the equality

$$r_\tau = \frac{a + bq^k(v(a_i) - v(a_j))}{bq^{k+j}}.$$

Since a is coprime to q, we get that $a + bq^k(v(a_i) - v(a_j))$ is coprime to q as well. This contradicts the assumption on q. Hence, ζt^r is not an approximation term for $x_{<r}$ with respect to P and $|J(r)| > 1$ by Lemma 2.1.7. □

Given $m \in \mathbb{N}$, we define $\Gamma_m := \frac{1}{mp^\infty}\mathbb{Z}$.

Corollary 2.1.19. *Let F be a field of characteristic p. There is an algorithm* MAXIMAL_RAMIFICATION *which takes as input a polynomial $f(X) \in \mathbb{F}_p(t)[X]$ and outputs a natural number m not divisible by p such that any root of f in $\mathbb{F}((t^{\mathbb{Q}}))$ is already in $\mathbb{F}((t^{\Gamma_m}))$.*

Proof. Let $\deg(f) = n$. Let $P(X) =$ ADDITIVE_MULTIPLE(f) as in Remark 1.3.17. Suppose that $x \in \mathbb{F}((t^{\mathbb{Q}}))$ is a root of $f(X)$, so in particular a root of $P(X)$. Let S be the points of intersection of P. Let $q_1^{e_1}, \ldots, q_\ell^{e_\ell}$ be the prime powers coprime to p occurring as factors in the denominators of the reduced fractions of elements in S. By Theorem 2.1.18 and by definition of a prime ramifying in x, any $r = a/b$ on reduced form in the support of x is such that the prime power factors of b coprime to p divides $m = \prod_{i=1}^{\ell} q_i^{e_i}$. In other words, the support of x is contained in Γ_m. The result thus follows from having MAXIMAL_RAMIFICATION returning m on input f. □

Remark 2.1.20. Rayner shows the existence of the bound in Corollary 2.1.19 by showing that $\bigcup_{m=1}^{\infty} \overline{\mathbb{F}}((t^{\Gamma_m}))$ is closed under Artin-Schreier extensions. An alternative proof was given by Poonen in [Poo93, Corollary 7], which uses the following argument. Let S be the set of automorphisms on $\mathbb{F}((t^{\mathbb{Q}}))$ given by sending $\sum_\gamma a_\gamma t^\gamma$ to $\sum_\gamma \zeta(\gamma) a_\gamma t^\gamma$, where ζ is a homomorphism from $\mathbb{Q}/\mathbb{Z}$ to the roots of unity in $\mathbb{F}$. Then $\bigcup_{m=1}^{\infty} \overline{\mathbb{F}}((t^{\Gamma_m}))$ is the subfield of $\mathbb{F}((t^{\mathbb{Q}}))$ consisting of elements with finite orbits under the action of S. This is an algebraically closed field by [Poo93, Lemma 5]. It was noted by Konstantinos Kartas that effectiveness also follows from the proof by

Poonen, since high ramification away from p gives too many roots of f. While this approach would be enough for our main decidability results, using Theorem 2.1.18 gives knowledge of where in the support ramification can occur, which might be of computaional interest for further research.

We have the following analogue of Rayner's result for the residue field.

Theorem 2.1.21. *Let $\mathbb{F}$ be a perfect field of characteristic p and let $P(X) \in \mathbb{F}_p(t)[X]$ be an additive polynomial. Let $\zeta \in \overline{\mathbb{F}}$. If $x \in \mathbb{F}((t^{\mathbb{Q}}))$ is a root of P and $r \in \mathbb{Q}$ is such that ζ expands x at r, then r is a point of intersection of P.*

Proof. Write $w = x_{<r}$. If $|J(r)| = 1$, then ζt^r is an approximation term for $x_{<r}$ and ζ satisfies an equation of the form $\zeta^{p^i} = b$, where $b \in K^*$. Since K is an algebraic extension of $\mathbb{F}$, it is perfect and so $\zeta \in K$ This contradicts the assumption that ζ expands x at r. Hence, $|J(r)| > 1$, and r is a point of intersection of P. □

Corollary 2.1.22. *There is an algorithm* MAXIMAL_EXPANSION *which takes as input a polynomial $f(X) \in \mathbb{F}_p(t)[X]$ and outputs a natural number m such that any root of f in $\overline{\mathbb{F}}((t^{\mathbb{Q}}))$ is already in $\mathbb{F}_{p^m}((t^{\mathbb{Q}}))$.*

Proof. Let $\deg(f) = n$ and let $P(X) =$ ADDITIVE_MULTIPLE(f). Write $P(X) = \sum_{i=0}^{n} a_i X^{p^i}$. Suppose that $x \in \overline{\mathbb{F}}((t^{\mathbb{Q}}))$ is a root of $f(X)$, so in particular a root of $P(X)$. Let r be in the support of x and let $w = x_{<r}$. Suppose that $w \in \mathbb{F}_{p^u}((t^{\mathbb{Q}}))$ for some $u \in \mathbb{N}$. Let ζt^r be the initial term of $x - w$. Suppose that $|J(r)| = 1$. Then ζ satisfies an equation of the form

$$\zeta^{p^\ell} = a$$

where $a \in \mathbb{F}_{p^u}$. Since $\mathbb{F}_{p^u}$ is perfect, we get that $\zeta \in \mathbb{F}_{p^u}$. If $|J(r)| > 1$, then r is a point of intersection of P and ζ satisfies an equation of the form

$$\sum_{j \in J(r)} a_j \zeta^{p^j} = a$$

with $a \in \mathbb{F}_{p^u}$. This shows that a has degree at most p^k over $\mathbb{F}_{p^u}$, with k being maximal such that $\gamma_k \in J(r)$. In other words, a is contained in $\mathbb{F}_{p^{mk!}}$.

Since the initial term $\zeta_0 t^{v(x)}$ of x is a better approximation of x than 0 and since $P(0) \in \mathbb{F}_p$, we get in particular that the ζ_0 has degree at most p^{k_0} over $\mathbb{F}_p$, with k_0 being maximal such that $\gamma_{k_0} \in J(v(x))$. This serves as the base case for concluding by transfinite induction that $x \in \mathbb{F}_{p^{u!}}((t^{\mathbb{Q}}))$, where $u = \prod_{i=1}^{n} p^i$ over $\mathbb{F}_p$. Having MAXIMAL_EXPANSION returning $u!$ on input f thus gives the desired result. □

Remark 2.1.23. Note that the bound obtained in the proof of Corollary 2.1.22 cannot be sharp. It assumes that for every $k \in \{1, \ldots, n\}$, there is a point of intersection of P such that k is maximal among the i such that $\gamma_i \in J(r)$. This is impossible since there cannot be n points of intersection of P. It is possible to have MAXIMAL_RAMIFICATION return a sharper bound, taking into account the points of intersection of P, but this is not necessary for our purposes.

2.2 A note on Diophantine approximation in Hahn fields

A monumental result in transcendental number theory is Liouville's theorem on Diophantine approximation, and its use to construct explicit transcendental numbers [Lio51]. It states that for any real algebraic number x of degree $n \geq 2$, there exists a constant $c > 0$ such that

$$\left| x - \frac{a}{b} \right| \geq \frac{c}{|b|^n}$$

for every integers a and $b \neq 0$.

The following direct analogue of Liouville's theorem for function fields was proven by Mahler [Mah49].

Theorem 2.2.1. *Let K be a field and suppose that $x \in K((t))$ is algebraic over $K(t)$ of degree $n \geq 2$. Then, with $|\cdot|_t$ being the t-adic norm, there exists a constant $c \in \mathbb{R}_{>0}$ such that*

$$\left| x - \frac{a}{b} \right|_t \geq \frac{c}{|b|_t^n}$$

for any $a \in K[t^{-1}]$ and nonzero $b \in K[t^{-1}]$.

It follows from the proof of Theorem 2.2.1 that the statement also holds if one replaces $K((t))$ with any field containing $K(t)$, as long as its valuation extends the t-adic and the approximation is done with elements in $K(t)$. For a Hahn field $K((t^\Gamma))$ with $\mathbb{Z} \subset \Gamma$, this is immediate, and we actually get a stronger result. Indeed, let $x \in K((t^\Gamma))$ be algebraic over $K(t)$ and let $\gamma \in \Gamma$ be minimal in the support of x such that

$$\operatorname{supp}(x) \cap \Gamma_{\leq \gamma} \subset \mathbb{Z}.$$

The statement of Theorem 2.2.1 now holds with $c = |t^\gamma|_t$.

Example 2.2.2. Just as Liouville's original theorem is used to show that $\sum_{n\geq 1} 10^{-n!}$ is a transcendental number[1], Theorem 2.2.1 implies that $x = \sum_{n\geq 1} t^{n!}$ is transcendental over $\mathbb{F}_p(t)$. To recall the argument, suppose that x is algebraic over $\mathbb{F}_p(t)$, let $a_k = t^{-k!}\sum_{i=1}^{k} t^{i!}$ and let $b_k = t^{-k!}$. Note that $|b_k|_t$ is unbounded. We have

$$\left| x - \frac{a_k}{b_k} \right|_t = e^{-(k+1)!}.$$

Thus, $\left| x - \frac{a_k}{b_k} \right|_t < e^{-k!k} = |b_k|_t^{-k}$. Assume x is algebraic of degree n over $\mathbb{F}_p(t)$ and let c be as in Theorem 2.2.1. Let $r \in \mathbb{N}$ be large enough so that $|b_{r+n}|_t^{-r} < c$. Then we have

$$\left| x - \frac{a_{r+n}}{b_{r+n}} \right|_t < |b_{r+n}|_t^{-(r+n)} < \frac{c}{|b_{r+n}|_t^{n}},$$

contradicting Theorem 2.2.1.

Theorem 2.2.1 generalises to approximating algebraic elements in $\mathbb{F}_p((t^{1/n}))$ with elements in $\mathbb{F}_p(t^{1/n})$, by replacing t with $t^{1/n}$. It is therefore tempting to look for a similar statement for approximating elements in say $\mathbb{F}_p((t^{1/p^\infty}))$ by elements in $\mathbb{F}_p(t)^{1/p^\infty}$. While it is not clear how to obtain such a result, it can be noted that in a sense, it would not give us additional information about elements in $\mathbb{F}_p((t^{1/p^\infty}))$ that are transcendental over $\mathbb{F}_p(t)$. By Theorem 1.3.14, we know that $\mathbb{F}_p((t^{1/p^\infty}))$ is relatively algebraically closed in its completion. Hence, any element in $\mathbb{F}_p((t^{1/p^\infty})) \setminus \mathbb{F}_p((t))^{1/p^\infty}$ which is algebraic over $\mathbb{F}_p(t)$ must have a finite accumulation point in the support. Say that we have an element

$$x = \sum_{i\in\mathbb{N}} a_i t^{\gamma_i} \in \mathbb{F}_p((t^{1/p^\infty}))$$

and suppose that γ_ω is a finite accumulation point of $(\gamma_i)_{i\in\mathbb{N}}$. Suppose that we want to use an approximation argument to determine if x is transcendental. To use the argument in Example 2.2.2, a naive approach would be to set $a_k = t^{-\gamma_k}\sum_{i=1}^{k} t^{\gamma_i}$ and $b_k = t^{-\gamma_k}$. The problem here is that the valuation of b_k does not get arbitrarily big, so we cannot conclude a contradiction as in Example 2.2.2.

[1]Liouville originally presented this number as transcendental without a proof in 1844, but the theorem on Diophantine approximation appeared for the first time in [Lio51]. For a detailed account of the history, see [Lüt90].

Chapter 3

The $\mathcal{L}_t$-theories of tame Hahn fields

3.1 An AKE-principle for tame fields in $\mathcal{L}_t$

Throughout this section, let (E, v) be a fixed valued field of residue characteristic p such that Ev is an algebraic extension of its prime field. Let $\Pi \subset E$ be such that $v\Pi$ generates vE. Let (L, v) be a tame field containing E and denote by (K, v) the relative algebraic closure of E in L. We will assume that (K, v) is algebraically maximal and that vL/vK is torsion free. In particular, if $E = \mathbb{F}_p(t)$ with the t-adic valuation, then L can be an equal charactersitic tame Hahn field, since the conditions on K are then satisfied by Lemma 1.3.36.

We will use Theorem 1.3.41 to obtain an AKE-principle for the theory of (L, v) in the language $\mathcal{L}_{\text{val}}(v\Pi)$, following closely the proof of Lemma 6.1 in [Kuh16].[1]

Lemma 3.1.1. *Let (F, w) be a tame field containing (E, v) and suppose that $vL \equiv_{v\Pi} wF$ and $Lv \equiv_{Ev} Fw$. Suppose furthermore that (K, v) is isomorphic over (E, v) to a valued subfield of (F, w). Then $(L, v) \equiv (F, w)$ in the language $\mathcal{L}_{val}(K)$.*

Proof. By assumption, (K, v) is algebraically maximal. Since L is perfect, we also have that K is perfect. Furthermore, since vL is p-divisible and vL/vK is torsion free, we have that vK is p-divisible. Hence, by Theorem 1.3.34, we have that (K, v) is tame. In particular, it is defectless. Since $Lv|Kv$ is separable we are in the situation of Definition 1.3.40 and it is enough to show that $vL \equiv_{vK} wF$ and $Lv \equiv_{Kv} Fw$.

Let $\psi(\bar{a})$ be a sentence in $\mathcal{L}_{\text{og}}(vK)$. Since K is an algebraic extension of E, we have that vK is a subgroup of the divisible hull of vE. With $\bar{a} = (a_1, \ldots, a_m)$, we

[1] This AKE-principle was originally formulated for $E = \mathbb{F}_p(t)$ and $\Pi = \{t\}$. The general result was prompted by Konstantinos Kartas asking if it also holds in characteristic zero. I would also like to thank him for suggesting to consider E as an arbitrary subfield, as an earlier version (see [Lis21]) only treated $E = \mathbb{F}_p(t)$ and $E = \mathbb{Q}$.

can therefore write

$$a_i = \sum_{j=1}^{n} \frac{b_{i,j}}{c_{i,j}} v(\pi_{i,j}),$$

where $\frac{b_{i,j}}{c_{i,j}} \in \mathbb{Q}$ and $\pi_{i,j} \in \Pi$. Each a_i is the unique element in vK satisfying the $\mathcal{L}_{\mathrm{og}}(v\Pi)$-formula $\phi_i(X)$ defined as

$$\prod_{j=1}^{n} c_{i,j} X = \sum_{j=1}^{n} b_{i,j} \prod_{k \neq j} c_{i,k} v(\pi_{i,j}).$$

Hence, $\psi(\bar{(}a))$ is equivalent to the $\mathcal{L}_{\mathrm{og}}(v\Pi)$-sentence

$$\exists X_1 \cdots \exists X_m \left(\psi(X_1, \ldots, X_m) \bigwedge_{i=1}^{m} \phi_i(X_i) \right).$$

Since vL and wF are elementary equivalent in the language $\mathcal{L}_{\mathrm{og}}(v\Pi)$, they are therefore elementary equivalent in the language $\mathcal{L}_{\mathrm{og}}(vK)$.

Since Kv is contained in $\mathrm{acl}(E)$, we have by Lemma 1.3.11 that $Lv \equiv_{Kv} Fw$. We conclude that we are in the situation of Definition 1.3.40. By Theorem 1.3.41, we get that $(L, v) \equiv_{(K,v)} (F, w)$ in the language $\mathcal{L}_{\mathrm{val}}$, and we are done. □

We will now show that Lemma 3.1.1 implies an AKE-principle in $\mathcal{L}_{\mathrm{val}}(K)$ relative to the algebraic part. For a set $A \subset L$, denote by $\mathcal{M}_A$ the set of monic polynomials over A. For each $f \in \mathcal{M}_A$, let ϕ_f be the $\mathcal{L}_{\mathrm{val}}(A)$-sentence defined as

$$\exists X \left(f(X) = 0 \wedge v(X) \geq 0 \right).$$

Define

$$S_{L,A} = \{\phi_f \mid f \in \mathcal{M}_A,\ (L, v) \models \phi_f\}.$$

We then have the following.

Theorem 3.1.2. *Suppose that (E, v) has rank one. Let $A \subset E_{\geq 0}$ be dense in the completion of $E_{\geq 0}$, with respect to v. Let (F, w) be a tame field containing (E, v) such that $(F, w) \models S_{L,A}$ and such that $vL \equiv_{v\Pi} wF$ and $Lv \equiv Fw$. Then, (K, v) is isomorphic over E to a subfield of F and, identifying K with its image under this isomorphism, we have that $(L, v) \equiv (F, w)$ in the language $\mathcal{L}_{val}(K)$.*

Proof. Let (F, w) be as described. We want to show that (K, v) is isomorphic as a valued field over E to a valued subfield of F. Since (L, v) and (F, w) are henselian, the isomorphism of (E, v) and (E, w) can be extended to an isomorphism of valued

fields Φ over E of the henselisations E^h of E in L and F respectively. Consider the set $\mathcal{U}$ of finite separable extensions of E^h inside L. We claim that any element in $\mathcal{U}$ is imomorphic over E^h to a subfield of F. Indeed, let $U \in \mathcal{U}$. Then $U = E^h(c_0)$, where c_0 is integral over $E^h_{\geq 0}$. Let

$$u = a_0 + \cdots + a_{n-1}X^{n-1} + X^n \in E^h_{\geq 0}[X]$$

be the minimal polynomial of c_0 and let $\{c_0, \ldots, c_{n-1}\} \subset \bar{E}$ be the conjugates of c_0. Let $\alpha_i = \max_{i \neq j}\{v(c_i - c_j)\}$ and let $\alpha = \max_i\{\alpha_i\}$. Since any valuation ring is integrally closed in its field of fraction we have that $v(c_i) \geq 0$ for each i, so $\alpha \geq 0$. By Theorem 1.3.4, there is $\gamma \in v\bar{E}$ such that for any polynomial

$$\tilde{u} = \prod_{i=1}^{n}(X - \tilde{c}_i) = \tilde{a}_0 + \cdots + \tilde{a}_{n-1}X^{n-1} + X^n \in \bar{E}[X]$$

with $\min_{0 \leq i < n}\{v(a_i - \tilde{a}_i)\} > \gamma$ and for any $i \in \{1, \ldots, n\}$, there is exactly one $j_i \in \{1, \ldots, n\}$ such that $v(c_i - \tilde{c}_{j_i}) > \alpha$. In particular, any such $\tilde{u}$ is separable and $v(\tilde{c}_{j_0}) \geq 0$. Since (E, v) has rank one, we have that E^h is contained in the completion of E with respect to v. Hence, by assumption on A, we can let $\tilde{u} = \tilde{a}_0 + \cdots + \tilde{a}_{n-1}X^{n-1} + X^n \in A[X]$ be such that $\min_{0 \leq i < n}\{v(a_i - \tilde{a}_i)\} > \gamma$. By Krasner's Lemma, we get that $E^h(c_0) \subset E^h(\tilde{c_{j_0}})$. By the degree of c_0, this implies that $\tilde{u}$ is irreducible over E^h. Conversely, we can take $\tilde{u}$ to be close enough to u so that $v(c_0 - \tilde{c}_0) > \max_{i \neq 0}\{v(\tilde{c_0} - \tilde{c}_i)\}$. This implies that $E^h(\tilde{c}_{j_0}) \subset E^h(c_0)$, so $E^h(\tilde{c}_{j_0}) = E^h(c_0)$. In particular, $\tilde{c}_{j_0} \in L$ and $\phi_{\tilde{u}} \in S$, so $\tilde{u}$ has a root $c \in F$ and the map $\tilde{c}_{j_0} \mapsto c$ embeds $E^h(c_0)$ over E^h into F.

We can now conclude that relative separable closure of E^h in L embeds over E^h into F, following the argument in [Wof21]. The set $\mathcal{U}$ together with inclusions forms a directed system. The corresponding direct limit E' is the relative separable closure of E^h in L. By the universal property of direct limit, it is enough to show that there is a set of embeddings $\{\iota_U : U \hookrightarrow_{E^h} F \mid U \in \mathcal{U}\}$ which is compatible with inclusions. For this, we consider the following inverse system. For each $U \in \mathcal{U}$, let V_U be the set of embeddings over E^h of U into F. As shown above, this is a finite nonempty set for each U. Define a partial order $\leq$ on $\mathcal{V}$ by letting $V_U \leq V_{U'}$ if $U \subset U'$. Under this ordering and together with retriction maps, $\mathcal{V}$ forms an inverse system. Since it is an inverse system of finite nonempty sets, we have that the corresponding inverse limit is nonempty. By construction, an element of this inverse limit is a compatible system of embeddings over E^h, as wanted.

Since the valuation on a henselian field extends uniquely to algebraic extensions, the valuation on the image of E' in F induced by v coincides with w. Hence, Φ extends to E'. Finally, since L and F are perfect, we can extend Φ to the perfect hull of E', which is equal to K. We conclude that there is a valued field isomorphism of (K, v) to a subfield of F which preserves E. Hence, we are in the situation of Lemma 3.1.1, and we can conclude the statement.

□

Remark 3.1.3. Note that by Theorem 3.1.2, the copy of K in F will indeed be the relative algebraic closure of E. One could get this immediately by imposing that $F \models \neg\phi_f$ for all monic $f \in E_{\geq 0}[X]$ such that $L \models \neg\phi_f$. The reason why we don't need to do this is because of relative subcompleteness; the fact that (K, v) is a valued subfield of (F, w) is enough to guarantee that it cannot have any proper algebraic extensions in F.

We now obtain Theorem 1.2.2 and Theorem 1.2.3 as corollaries to Theorem 3.1.2.

Proof of Theorem 1.2.2 and Theorem 1.2.3. Let $E = \mathbb{F}_p(t)$, $A = \mathbb{F}_p[t]$, and $\pi = t$ if L has characteristic p. Let $E = \mathbb{Q}$, $A = \mathbb{Z}$, and $\pi = p$ if L has characteristic zero. In both cases, we have that $S = S_{L,A}$. When L has characteristic p, $v(\pi) > 0$ by assumption. Otherwise, $v(\pi) > 0$ since Lv has characteristic p. We get that v is the π-adic valuation on E, up to scaling. In particular, (E, v) has rank one and A is dense in the completion of $E_{\geq 0}$ with respect to v. Since the relative algebraic closure (K, v) of (E, v) in L satisfies the conditions in beginning of Section 3.1 and since F satisfies the conditions of Theorem 3.1.2 with $\Pi = \{\pi\}$, we have that $(L, v) \equiv (F, w)$ in the language $\mathcal{L}_{\text{val}}(K)$. In particular, since $\pi \in K$, we get that $(L, v) \equiv_\pi (F, w)$. When $\pi = p$, this just says that $(L, v) \equiv (F, w)$ □

The field L in Example 1.3.37 can also be used to show that the assumption of vL/vK being torsion free is necessary.

Example 3.1.4. With the notation of Example 1.3.37 and $p > 3$, let F be an algebraically maximal immediate extension of $\mathbb{F}_p(t, (st)^{1/2}, s^{1/3})^{1/p^\infty}$, so F is a tame field with value group equal to vL. Since $Lv = \mathbb{F}_p(s)^{1/p^\infty}$ is isomorphic to $Fv = \mathbb{F}_p(s^{1/3})^{1/p^\infty}$, we have that $Lv \equiv Fv$. By construction, the relative algebraic closure of $\mathbb{F}_p(t)$ in L is equal to the relative algebraic closure of $\mathbb{F}_p(t)$ in F. However, (F, v) satisfy the $\mathcal{L}_t$-sentence

$$\exists X \exists Y \exists Z (X^2 = Yt \wedge v(Y) = 0 \wedge Z^3 = Y)$$

which is not satisfied in L.

In certain cases, it is not necessary to specify the set S in Theorem 3.1.2. For this, we fix E to be $\mathbb{F}_p(t)$.

Theorem 3.1.5. *Let $\mathbb{F}$ be a field of characteristic p without any proper finite extension of degree divisible by p and let (L, v) be $\mathbb{F}((t^{1/p^\infty}))$ with the t-adic valuation. Let (F, w) be a tame field containing $\mathbb{F}_p(t)$ such that $vL \equiv_{v(t)} wF$ and $Lv \equiv Fw$. Then $(L, v) \equiv (F, w)$ in the language $\mathcal{L}_t$.*

Proof. The valuation preserving isomorphism between the copies of $\mathbb{F}_p(t)$ in (L, v) and (F, w) respectively can be extended to the perfect hull $\mathbb{F}_p(t)^{1/p^\infty}$ of $\mathbb{F}_p(t)$. Again, we can extend this to a valued fields isomorphism Φ of the henselisations $D = (\mathbb{F}_p(t)^{1/p^\infty})^h$ of $\mathbb{F}_p(t)^{1/p^\infty}$ in L and F respectively. We can then extend Φ to an isomorphism of valued fields with residue fields equal to Kv as follows.

For an element $c \in K_{\geq 0}$, denote by $f_c(X)$ its minimal polynomial over D. Let $I = \{c \in K_{\geq 0} \mid f_c(X) \in \mathbb{F}_p[X]\}$ and let $\mathcal{U} = \{D(c) \mid c \in I\}$. We have that $\mathcal{U}$ together with inclusions is a directed system. Indeed, for two extensions U and U' in $\mathcal{U}$, their compositum is equal to $D(c, c')$, with c and c' being elements in I. Since f_c and $f_{c'}$ are irreducible over $\mathbb{F}_p$, we have that $[\mathbb{F}_p(\bar{c}) : \mathbb{F}_p] = [U : D]$ and $[\mathbb{F}_p(\bar{c'}) : \mathbb{F}_p] = [U' : D]$. Let $\alpha \in Kv$ be such that $\mathbb{F}_p(\bar{c}, \bar{c'}) = \mathbb{F}_p(\alpha)$ and let $u(X) \in \mathbb{F}_p[X]$ be the minimal polynomial of α. Since u is separable, there is $d \in K_{\geq 0}$ such that d is a lift of α with $u(d) = 0$, as in Theorem 1.3.6. Let $V = D(d)$. Since $[V : D] \geq [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$, we have that u remains irreducible over D and is the minimal polynomial of d over D. This shows that $V \in \mathcal{U}$ and that $UU' = V$.

Let $D' = \varinjlim \mathcal{U}$. For each $c \in I$, let ϕ_c be the $\mathcal{L}_{\text{val}}$-sentence $\exists X(f_c(X) = 0)$. By definition of I, we have that $(L, v) \models \phi_c$ for each $c \in I$. Since $(L, v) \equiv (F, w)$ in the language $\mathcal{L}_{\text{val}}$, this implies that $(F, w) \models \phi_c$ for each $c \in I$. As in the proof of Theorem 3.1.2, we get that D' embeds over $(\mathbb{F}_p(t)^{1/p^\infty})^h$ into F. Thus, we can extend Φ to a valued field isomorphism of the copies of D' in L and F respectively. Note that any witness of a sentence ϕ_f must have valuation 0. Indeed, let $f = \sum_{i=0}^n a_i X^i$ with $a_i \in \mathbb{F}_p$ and suppose $v(x) \neq 0$. Then $v(a_i x^i) = iv(x)$ for all non-zero a_i. This implies that

$$vf(x) = \min_{i:\ a_i \neq 0} \{iv(x)\} \neq \infty,$$

so $f(x) \neq 0$.

Let $\alpha \in Kv$ and let f_α be the minimal polynomial of α over $\mathbb{F}_p$. In particular, f_α is separable. Let $a \in K_{\geq 0}$ be a lift of α such that $f_\alpha(a) = 0$. As noted above, f_α remains irreducible over D. This implies that $a \in D'$, by definition of I. Hence, $\alpha \in D'v$, so $Kv \subset D'v$. For the converse inclusion, we just note that $D'v$ is an algebraic extension

of $\mathbb{F}_p$. To summarise, we now have an injective field homomorphism from an algebraic subextension (D', v) of $(L, v)/(\mathbb{F}_p(t), v)$ into (F, w), preserving $\mathbb{F}_p(t)$, where $D'v = Kv$ and $vD' = \frac{1}{p^\infty}\mathbb{Z}$. We identify the image of (D', v) in (F, w) with (D', v) itself.

By elementary equivalence in $\mathcal{L}_{\text{val}}$, both (L, v) and (F, w) are algebraically maximal Kaplansky fields. By Theorem 1.3.32, the relative algebraic closure of $\mathbb{F}_p(t)$ in L and F are therefore algebraically maximal Kaplansky fields. Hence, (D', v) is also a Kaplansky field and (K, v) is the unique algebraically maximal immediate algebraic extension of D', as in Lemma 1.3.28. Thus, the isomorphism of the copies of D' in L and F extends to an isomorphism of valued fields between K and a subfield of F and we are in the situation of Lemma 3.1.1, noting that our particular choice of L satisfies the general assumptions of this section. □

Corollary 3.1.6. *Let $\mathbb{F}$ be a field of characteristic p without any proper finite extension of degree divisible by p. Suppose that $\mathbb{F}$ is decidable in the language $\mathcal{L}_{ring}$. Then $\mathbb{F}((t^{1/p^\infty}))$ is decidable in the language $\mathcal{L}_t$. In particular, if $\mathbb{F}$ is algebraically closed, then $\mathbb{F}((t^{1/p^\infty}))$ is decidable.*

Proof. By Theorem 3.1.2, the $\mathcal{L}_t$-theory of $\mathbb{F}((t^{1/p^\infty}))$ is axiomatised by the $\mathcal{L}_{\text{val}}$-theory of tame fields, the $\mathcal{L}_{\text{og}}(1)$-theory of $\frac{1}{p^\infty}\mathbb{Z}$ and the $\mathcal{L}_{\text{ring}}$-theory of $\mathbb{F}$, which are all decidable. □

Remark 3.1.7. When $\mathbb{F}$ is an algebraically closed field of characteristic p, then $\mathbb{F}$ is decidable. In particular, by Corollary 3.1.6, there is an algorithm COUNT_ROOTS_$\mathbb{F}$, which takes as input a polynomial $f(X) \in \mathbb{F}_p[t]$ and returns $m \in \mathbb{N}$, where m is the number of roots of f in $\mathbb{F}[[t^{1/p^\infty}]]$.

3.2 Decidability of $\mathbb{F}((t^{1/p^\infty}))$

We now turn to the question of decidability in $\mathcal{L}_t$ for Hahn fields $\mathbb{F}((t^{1/p^\infty}))$ of characteristic p. In this case, we can use the theory of finite automata established in Section 1.3.7 to show that there is a recursive procedure to determine the set $S_{\mathbb{F}((t^{1/p^\infty})),\mathbb{F}_p[t]}$ in Theorem 3.1.2. This approach was suggested by Ehud Hrushovski. We will later see how decidability of general tame Hahn fields of characteristic p can be reduced to this case. To start, we need the following lemma.

Lemma 3.2.1. *Let $q = p^n$ be a prime power. Let $\mathbb{F}$ be a decidable field of characteristic p. Then, there is an algorithm* IS_IN_$\mathbb{F}$ *which on input a well-ordered DFAO $M = (Q, \Sigma_p, \delta, q_0, \mathbb{F}_q, \tau)$ with reachable states F outputs* TRUE *if $\tau(F) \subset \mathbb{F}$ and* FALSE *otherwise.*

Proof. Let $M = (Q, \Sigma_p, \delta, q_0, \mathbb{F}_q, \tau)$ be a well-ordered DFAO. Let F be its reachable states, which are given by REACHABLE_STATES(M). To start, we want to determine the minimal positive integer k such that $\tau(F) \subset \mathbb{F}_{p^k}$. We do this by using the fact that $\tau(F) \subset \mathbb{F}_{p^k}$ if and only if all elements in $\tau(F)$ are roots of the polynomial $X^{p^k} - X$. As described in Section 1.3.7, elements in $\tau(F)$ are polynomials over $\mathbb{F}_p[X]$ of degree at most $n-1$. Hence, with $g(X) \in \mathbb{F}_p[X]$ being the irreducible polynomial of degree n used to define $\mathbb{F}_q$ as an alphabet, determining if $\tau(F)$ is a subset of $\mathbb{F}_{p^k}$ amounts to checking if the sentence ψ_k defined by

$$\exists X \left(g(X) \bigwedge_{h \in \tau(F)} (h(X)^{p^k} - h(X) = 0) \right)$$

holds in $\mathbb{F}_q$. Since any $\alpha \in \overline{\mathbb{F}}_p$ witnessing ψ_k will be in $\mathbb{F}_q$ by definition of g, it is enough to check if ψ_k holds in $\overline{\mathbb{F}}_p$, which we can do by decidability of $\overline{\mathbb{F}}_p$. Hence, starting from $k = 1$ and increasing k until $\overline{\mathbb{F}}_p \models \psi_k$ gives us the minimal positive integer k such that $\tau(F) \subset \mathbb{F}_{p^k}$.

Now, it only remains to verify if $\mathbb{F}_{p^k} \subset \mathbb{F}$ or not. This is done using decidability of $\mathbb{F}$, since $\mathbb{F}_{p^k} \subset \mathbb{F}$ if and only if $\mathbb{F}$ has p^k distinct roots to the polynomial $X^{p^k} - X$. □

Theorem 3.2.2. *Let $\mathbb{F}$ be a decidable perfect field of characteristic p. Then the Hahn field $\mathbb{F}((t^{1/p^\infty}))$ is decidable in the language $\mathcal{L}_t$.*

Proof. By Theorem 3.1.2, with $E = \mathbb{F}_p(t)$, the $\mathcal{L}_t$-theory of $\mathbb{F}((t^{1/p^\infty}))$ is axiomatised by the $\mathcal{L}_{\text{val}}$-axioms for tame fields of characteristic p, the $\mathcal{L}_{\text{og}}(v(t))$-theory of $\frac{1}{p^\infty}\mathbb{Z}$, the $\mathcal{L}_{\text{ring}}$-theory of $\mathbb{F}$, and the set $S = S_{\mathbb{F}((t^{1/p^\infty})),\mathbb{F}_p[t]}$. The $\mathcal{L}_{\text{og}}(v(t))$-theory of $\frac{1}{p^\infty}\mathbb{Z}$ is decidable by Lemma 1.3.12, and the $\mathcal{L}_{\text{ring}}$-theory of $\mathbb{F}$ is decidable by assumption. In particular, they are both recursively enumerable. Hence, it is enough to show that there is an algorithm ENUMERATE_S which enumerates S to conclude that the $\mathcal{L}_t$-theory of $\mathbb{F}((t^{1/p^\infty}))$ is recursively enumerable. We will show something slightly stronger, namely that S is decidable. For this, we create an algorithm DECIDE_S which takes as input a sentence ϕ_f with $f \in \mathbb{F}_p[t]$ monic, and outputs TRUE if $\phi_f \in S$ and FALSE otherwise. This algorithm is outlined as follows.

1. Let $m =$ COUNT_ROOTS_$\overline{\mathbb{F}}(f)$, i.e. the number of unique roots of f in $\overline{\mathbb{F}}[[t^{1/p^\infty}]]$, and let $n =$ MAXIMAL_EXPANSION(f). By Lemma 1.3.13, any root of f in $\overline{\mathbb{F}}[[t^{1/p^\infty}]]$ is contained in $\overline{\mathbb{F}}_p((t^{1/p^\infty}))$. So by Corollary 2.1.22, all such roots lie in $\mathbb{F}_q[[t^{1/p^\infty}]]$, where $q = p^n$.

2. Find DFAOs $M_1, \ldots, M_m$ such that $\{\mathrm{Pow}(M_i) \mid 1 \leq i \leq m\}$ is the set of all roots of f in $\mathbb{F}_q[[t^{1/p^\infty}]]$ by going through well-ordered DFAOs with output alphabet $\mathbb{F}_q$ and check if they represent roots to f using IS_ROOT. When finding a DFAO M such that IS_ROOT(f, M) returns TRUE, we verify that $\mathrm{Pow}(M)$ is not equal to any of the previous found roots using EQUALS.

3. Check if any of these roots are in $\mathbb{F}[[t^{1/p^\infty}]]$, using the algorithm IS_IN_$\mathbb{F}$ from Lemma 3.2.1.

In pseudocode, the algorithm is given as follows.

DECIDE_$S(\phi_f)$

```
m ← COUNT_ROOTS_F̄(f)
n ← MAXIMAL_EXPANSION(f)
q ← p^n
R ← ∅
k ← 0
while |R| < m do
    M ← ENUMERATE_WELL_ORDERED_F_q(k)
    if IS_ROOT(f, M) then
        IsRoot ← TRUE
        for N ∈ R do
            if EQUALS(M, N) then
                IsRoot ← FALSE
    if IsRoot then
        R ← R ∪ {M}
    n ← n + 1
for M ∈ R do
    if IS_IN_F(M) then
        return TRUE
return FALSE
```

We conclude that the set S is decidable, so $\mathbb{F}((t^{1/p^\infty}))$ is decidable in the language $\mathcal{L}_t$. □

Remark 3.2.3. An algorithm which enumerates S can be constructed by listing the j first polynomials $f_1, \ldots, f_j$ over $\mathbb{F}_p[t]$ and the j first well-ordered DFAs $M_1, \ldots, M_j$ with output alphabet $\mathbb{F}_{q_j}$, where $q_j = p^{m_j}$ is a subfield of $\mathbb{F}$ such that any root of $f_1, \ldots, f_j$ in $\mathbb{F}((t^{1/p^\infty}))$ is already in $\mathbb{F}_q((t^{1/p^\infty}))$, and such that $\mathbb{F}_{q_j} \subset \mathbb{F}_{q_{j+1}}$. If $f_k(\mathrm{Pow}(M_\ell))$ for some k and some ℓ less than or equal to j, and if f_k is not already equal to ENUMERATE_$S(i)$ for some $i < n$, then ENUMERATE_S returns f_k. If this

is not the case, we increase j and repeat. The condition that $\mathbb{F}_{q_j} \subset \mathbb{F}_{q_{j+1}}$ is met using MAXIMAL_EXPANSION and it ensures that we will list all DFAOs that represent a root in $\mathbb{F}((t^{1/p^\infty}))$ of some polynomial $f \in \mathbb{F}_p[t][X]$. The reason why why instead show that S is decidable is to avoid the technicalities of comparing automata with different output alphabets.

3.3 Decidability of general positive characteristic tame Hahn fields

We now turn to the question of decidability when there is ramification at primes different from the characteristic. As in Section 2.1.3, given $m \in \mathbb{N}$ we write

$$\Gamma_m = \frac{1}{mp^\infty}\mathbb{Z}.$$

We start with the following observation.

Corollary 3.3.1. *Let $\mathbb{F}$ be a decidable perfect field of characteristic p. Then, for any $m \in \mathbb{N}$, we have that $\mathbb{F}((t^{\Gamma_m}))$ is decidable in $\mathcal{L}_t$.*

Proof. This follows from Theorem 3.2.2, with $t^{1/m}$ in place of t. □

Theorem 3.3.2. *Let (L, v) be a tame field containing $\mathbb{F}_p(t)$. Suppose that Lv and vL are decidable in $\mathcal{L}_{ring}$ and $\mathcal{L}_{og}(v(t)$ respectively. Let $\mathbb{F}$ be a perfect decidable subfield of Lv containing the relative algebraic closure of $\mathbb{F}_p$ in Lv and let Γ be the relative divisible hull of $\langle v(t)\rangle$ in vL. Suppose that $(\mathbb{F}((t^\Gamma)), v_t)$ is a valued subfield of (L, v). Then, (L, v) is decidable in $\mathcal{L}_t$*

Proof. We will use Theorem 3.1.2. For this, we first note that the relative algebraic closure K of $\mathbb{F}_p(t)$ in L is contained in $\mathbb{F}((t^\Gamma))$. Indeed, let K' be the relative algebraic closure of $\mathbb{F}_p(t)$ in $\mathbb{F}((t^\Gamma))$. Then (K', v) is tame by Lemma 1.3.36. In particular, K' is algebraically maximal. Since Kv is contained in $\mathbb{F}$, we have that $K'v = Kv$. Since Γ is the relative divisible hull of $\langle v(t)\rangle$, which is equal to vK, we also have that $vK' = vK$. Hence, K/K' is an immediate algebraic extension, so $K = K'$. Since $vK = \Gamma$, we have that vL/vK is torsion free. We are therefore in the situation of Theorem 3.1.2, and it is again enough to show that there is a decision procedure for the set S defined before Theorem 3.1.2.

Now, let $f(X) \in \mathbb{F}_p[t][X]$ be monic. Let $m = \text{MAXIMAL_RAMIFICATION}(f)$, as in Corollary 2.1.19. Then any root of f in $\mathbb{F}[[t^{\mathbb{Q}}]]$ is already in $\mathbb{F}[[t^{\Gamma_m}]]$, where $\Gamma_m = \frac{1}{mp^\infty}\mathbb{Z}$ as above. Let U be the set of factors of m. Let V be the set of natural numbers n

such that n is not divisible by p and such that $\frac{u}{n} \in \Gamma$ for some $u \in \mathbb{Z}$, where $\langle v(t) \rangle$ is identified with $\mathbb{Z}$ in Γ. Note that $\frac{u}{n} \in \Gamma$ if and only if $\frac{u}{np^e} \in \Gamma$ for any $e \in \mathbb{N}$, since Γ is p-divisible. Furthermore, we have that $\frac{u}{n} \in V$ if and only if $\frac{u'}{n} + v \in \Gamma$ for some $u' \in \{1, \ldots, n-1\}$ and $v \in \mathbb{Z}$. Since $\mathbb{Z}$ is a subgroup of Γ, this holds if and only if $\frac{u'}{n} \in \Gamma$. Using decidability of vL, we get that there is an algorithm which on input f outputs the set

$$U \cap V = \{n_1, \ldots, n_\ell\}.$$

Indeed, since m is not divisible by p, this algorithm outputs exactly the elements $n \in U$ for which $vL \models \bigvee_{0<u<n} \exists X(nX = u)$.

Define

$$m' := \prod_{i=1}^{\ell} n_i.$$

Since $\mathbb{F}[[t^\Gamma]] \subset \mathbb{F}[[t^\mathbb{Q}]]$, any root of f in $\mathbb{F}[[t^\Gamma]]$ is already in $\mathbb{F}[[t^{\Gamma_m}]]$.

Let $x \in \mathbb{F}[[t^{\Gamma_m}]] \cap \mathbb{F}[[t^\Gamma]]$. Then, since the support of x is in Γ_m, we can write

$$x = \sum_{i \in I} a_i t^{\frac{m_i}{n_i p^i}}$$

where $I \subset \mathbb{N}$, $m_i \in \mathbb{N}$, and $n_i \in U$. On the other hand, since the support of x is in Γ and since no n_i is divisible by p, we have that each n_i is in V. Hence, $x \in \mathbb{F}[[t^{\Gamma_{m'}}]]$. Conversely, if $x \in \mathbb{F}[[t^{\Gamma_{m'}}]]$, we write

$$x = \sum_{i \in I} a_i t^{\frac{m_i}{n_i p^i}}$$

where each $n_i \in U \cap V$. Since each n_i divides m, we get that $x \in \mathbb{F}[[t^{\Gamma_m}]]$ and since $n_i \in V$, we get that $x \in \mathbb{F}[[t^\Gamma]]$. We conclude that $\mathbb{F}[[t^{\Gamma_m}]] \cap \mathbb{F}[[t^\Gamma]] = \mathbb{F}[[t^{\Gamma_{m'}}]]$. We can thus use the decision procedure from Corollary 3.3.1 for $\mathbb{F}((t^{\Gamma_{m'}}))$ to determine if f has a root in $\mathbb{F}[[t^\Gamma]]$ or not. Since any root $x \in L$ of f is already in $\mathbb{F}((t^\Gamma))$ as noted above, we can now use this same decision procedure to determine if f has a root in K or not, and we are done. □

We now get Theorem 1.2.1 as an immediate consequence of Theorem 3.3.2, since $\mathbb{F}((t^G))$ is a subfield of $\mathbb{F}((t^\Gamma))$, with G being the relative divisible hull of $\langle v(t) \rangle$ in Γ.

Bibliography

[Abh56] Shreeram Abhyankar. Two notes on formal power series. *Proc. Amer. Math. Soc.*, 7:903–905, 1956.

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

[AK65a] James Ax and Simon Kochen. Diophantine problems over local fields I. *Amer. J. Math.*, 87:605–630, 1965.

[AK65b] James Ax and Simon Kochen. Diophantine problems over local fields II. A complete set of axioms for p-adic number theory. *Am. J. Math.*, 87:631–648, 1965.

[AS03] Jean-Paul Allouche and Jeffrey Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[Dit18] Philip Dittmann. *A model-theoretic approach to the arithmetic of global fields*. PhD thesis, University of Oxford, 2018.

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

[DS03] Jan Denef and Hans Schoutens. On the decidability of the existential theory of $\mathbb{F}_p[\![t]\!]$. In *Valuation Theory and its Applications, Vol. II (Saskatoon, SK, 1999)*, volume 33 of *Fields Institute Communications*, pages 43–60. American Mathematical Society, Providence, RI, 2003.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[Ers65] Yuri L. Ershov. On elementary theories of local fields. *Algebra i Logika Sem.*, 4:5–30, 1965.

[Hah07] Hans Hahn. Über die nichtarchimedischen größensysteme. *Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Wien, Mathematisch - Naturwissenschaftliche Klasse*, 1907.

[Hil00] David Hilbert. Mathematische probleme. *Nachrichten von der Königl. Gesellschaft der Wissenschaften zu Göttingen*, 3:253–297, 1900.

[HU79] John E. Hopcroft and Jeff D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley Publishing Company, 1979.

[Kap42] Irving Kaplansky. Maximal fields with valuations. *Duke Math. J.*, 9:303–321, 06 1942.

[Kar20] Konstantinos Kartas. Decidability via the tilting correspondence. Preprint, arXiv:2001.04424, 2020.

[Ked06] Kiran S. Kedlaya. Finite automata and algebraic extensions of function fields. *J. de Theor. des Nr. de Bordeaux*, 18:379–420, 2006.

[KL19] Julia F. Knight and Karen Lange. Lengths of developments in $K((G))$. *Selecta Math. (N.S.)*, 25(1):Paper No. 14, 36, 2019.

[Koe14] Jochen Koenigsmann. Undecidability in number theory. In *Model Theory in Algebra, Analysis and Arithmetic*, pages 159–195. Springer, Heidelberg, 2014.

[Kuh04] Franz-Viktor Kuhlmann. Value groups, residue fields, and bad places of rational function fields. *Trans. Amer. Math. Soc.*, 356(11):4559–4600, 2004.

[Kuh16] Franz-Viktor Kuhlmann. The algebra and model theory of tame valued fields. *J. Reine Angew. Math.*, 719:1–43, 2016.

[Kuh22] Franz-Viktor Kuhlmann. Subfields of algebraically maximal Kaplansky fields. *Commun Algebra*, DOI: 10.1080/00927872.2022.2032118, 2022.

[Lam86] David Lampert. Algebraic p-adic expansions. *J. Number Theory*, 23:279–284, 1986.

[Lio51] Joseph Liouville. Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques. *Journal de Mathématiques Pures et Appliquées*, pages 133–142, 1851.

[Lis21] Victor Lisinski. Decidability of positive characteristic tame Hahn fields in $\mathcal{L}_t$. Preprint, arXiv:2108.04132, 2021.

[Lüt90] Jesper Lützen. *Joseph Liouville 1809–1882: master of pure and applied mathematics*, volume 15 of *Studies in the History of Mathematics and Physical Sciences*. Springer-Verlag, New York, 1990.

[Mac39] Saunders MacLane. The universality of formal power series fields. *Bulletin of the American Mathematical Society*, 45:888–890, 1939.

[Mah49] Kurt Mahler. On a theorem of Liouville in fields of positive characteristic. *Canad. J. Math.*, 1:397–400, 1949.

[Mat70] Yuri V. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[Poo93] Bjorn Poonen. Maximally complete fields. *Enseign. Math. (2)*, 39(1-2):87–106, 1993.

[Ray68] Francis J. Rayner. An algebraically closed field. *Glasgow Math. J.*, 9:146–151, 1968.

[RZ60] Abraham Robinson and Elias Zakon. Elementary properties of ordered abelian groups. *Trans. Amer. Math. Soc.*, 96:222–236, 1960.

[Ser79] Jean-Pierre Serre. *Local Fields*. Springer, New York; Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Sip13] Michael Sipser. *Introduction to the Theory of Computation*. Course Technology, Boston, MA, third edition, 2013.

[TZ12] Katrin Tent and Martin Ziegler. *A course in model theory*, volume 40 of *Lecture Notes in Logic*. Association for Symbolic Logic, La Jolla, CA; Cambridge University Press, Cambridge, 2012.

[War89] Seth Warner. *Topological Fields*. ISSN. Elsevier Science, 1989.

[Wha57] George Whaples. Galois cohomology of additive polynomial and n-th power mappings of fields. *Duke Math. J.*, 24(2):143–150, 06 1957.

[Wof21] Eric Wofsey. When can we embed field extensions into one another? Mathematics Stack Exchange, 2021. URL: https://math.stackexchange.com/q/4052915 (version: 2021-03-07).