Undecidability in some Field Theories

Brian Tyrrell

Balliol College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

March 2023

Dedicated

to

Sunny

for

everything

"My Theorem will tell the story. Each graph with a beginning and a middle and an end."
"There's no romance in geometry," Lindsey answered.
"Just you wait."

– John Green, *An Abundance of Katherines.*

Age cannot wither her, nor custom stale
Her infinite variety.

– William Shakespeare, *Antony and Cleopatra.*

One and one and one and one doesn't equal four. Each one remains unique, there is no way of joining them together. They cannot be exchanged, one for the other. They cannot replace each other.

– Margaret Atwood, *The Handmaid's Tale.*

Sitting at his side Stephen solved out the problem. He proves by algebra that Shakespeare's ghost is Hamlet's grandfather . . .
. . . Across the page the symbols moved in grave morrice, in the mummery of their letters, wearing quaint caps of squares and cubes.

– James Joyce, *Ulysses.*

Freedom is the freedom to say that two plus two make four. If that is granted, all else follows.

– George Orwell, *1984.*

DPhil in Mathematics

DECLARATION OF AUTHORSHIP

Name: BRIAN TYRRELL **Candidate number: 1020982**

College: BALLIOL **Supervisor(s): PROF. JOCHEN KOENIGSMANN**

Title of dissertation:

Undecidability in some Field Theories

I have read and understood the University's disciplinary regulations concerning conduct in examinations and, in particular, the regulations on plagiarism (*The University Student Handbook* Section 8.7; available at https://www.ox.ac.uk/students/academic/student-handbook).

I have read and understood the Education Committee's information and guidance on academic good practice and plagiarism at https://www.ox.ac.uk/students/academic/guidance/skills.

The dissertation I am submitting is entirely my own work except where otherwise indicated.

It has not been submitted, either partially or in full, either for this Honour School or qualification or for another Honour School or qualification of this University (except where the Special Regulations for the subject permit this), or for a qualification at any other institution.

I have clearly indicated the presence of all material I have quoted from other sources, including any diagrams, charts, tables or graphs.

I have clearly indicated the presence of all paraphrased material with appropriate references.

I have acknowledged appropriately any assistance I have received in addition to that provided by my supervisor(s).

I have not copied from the work of any other candidate.

I have not used the services of any agency providing specimen, model or ghostwritten work in the preparation of this dissertation.

The dissertation I am submitting is identical in content with the electronic copy of the dissertation submitted for screening.

Candidate's signature: ..... Date: .....

Brian Tyrrell

Acknowledgements

Most of my DPhil experience would not have been possible without Professors Jochen Koenigsmann & Ehud Hrushovski. To Jochen I am greatly indebted for years of supervision and guidance, and to Udi I am indebted for additional mathematical advice and direction. I am grateful to Professor Jonathan Pila and Dr. Jamshid Derakhshan for helpful comments and conversations, to Professors Arno Fehm and Boris Zilber, and to Professors Andreea Nicoara and Maryanthe Malliaris for years of advice, counsel, and education. My DPhil has also benefited enormously from extensive conversations with Dr. Vicky Neale and Sandy Patel over the years. I have been very fortunate in my academic career, and especially fortunate I had Ger Keogan in 2009 begin it.

I am grateful to Mikhail Blinov for his translation of [Erš80, Chapter 5, §1.4] (any errors in presentation are, of course, my own). Thanks also to Robert Baumann for helpful conversations on topics around *Chapter 2*. I acknowledge the generous financial support of the Clarendon Fund, the Foley-Béjar Scholarship Fund, and the Covid-19 Scholarship Extension Fund, crucial to the production of this work.

I have also been very fortunate in my friendships. My thanks to all the Junior Logicians at Oxford through the years, especially Alex, Arturo, Atticus, Benedikt, Cassani, Emma, Francesco, Kostas, Michał, Philip, Ronan, Sam, Sebastian, Victor, and Wojciech. My thanks also to Sylvy for many important conversations.

PTO

I am extraordinarily lucky to have good friends in Manchester as well: Anja, Clément, Dan, Deacon, Gabriel, Jake, Kai, Mahah, Marcello, Ray, and Rose among many others. I am glad to count Alex, Anastasia, Cathal, Hannah, Lucy, and Catherine and Rafael among my closest friends.

Substantial parts of this DPhil were completed while I enjoyed the hospitality of Feichín & Mags. Their company, with Donncha, Medb, Fergal, Lauren, Kilian, and Ina was deeply appreciated.

I am grateful to my parents Celia & Colin, and brother Conor, for a lifetime of encouragement and support. My successes are theirs.

Finally, I thank Sunny for spreading joy every day.

Abstract

This thesis is a study of undecidability in some field theories. Specifically, we are interested in geometrically oriented problems and have focused our attention in two directions along these lines. The first direction bases on determining the decidability of certain sets of first-order sentences over positive characteristic function fields. We will draw parallel to the problem of algorithmically determining in some cases the existence of points on varieties in positive characteristic function fields; equivalently the existence of certain maps between varieties over other positive characteristic fields.

The second direction bases on determining the decidability of first-order consequences of nonempty finite collections of $\mathcal{L}_r$-sentences, true in fields with plenty of geometric structure. This is connected to the former direction by the fact that a decidable field has a recursive axiomatisation – what if we study a (nonempty) finite subset of the axiomatisation? Undecidability results.

Motivated by classification-theoretic conjectures, we will examine 'wilder' classes of fields in turn and generalise a result of Ziegler to NIP henselian nontrivially valued fields (and beyond). We move to PAC & PRC fields and prove they are *finitely undecidable*, resolving two open questions of Shlapentokh & Videla, and describe the difficulties that arise in adapting the proof to PpC fields. We pose the question: *is every infinite field finitely undecidable?*

Contents

Chapter 1

Introduction

1.1 Hilbert's 'Geometric' Tenth Problem

Posed by David Hilbert in 1900 [Hil00], Hilbert's *Tenth* problem was to determine the decidability of the existential theory of arithmetic (though this was not how Hilbert phrased it). This was determined as *undecidable* in 1970, through the work of Martin Davis, Hilary Putnam, Julia Robinson, and Yuri Matiyasevich [DPR61, Mat70]. However this is the question as a logician would phrase it – the beauty behind this problem is its equivalent number-theoretic and algebro-geometric formulations. A number theorist might ask if there is an effective procedure to determine if a given Diophantine equation has a solution over $\mathbb{Z}$, while an algebraic geometer might query whether one can algorithmically determine when a $\mathbb{Q}$-variety V has an integral point. These are in fact equivalent questions (see [Koe14, §4.1]), hence all *undecidable*.

In the last half century there has been an explosion of activity in this area of computability, and now many more theories are known to be existentially undecidable (mostly through reducing the question to solving Hilbert's Tenth Problem). Moving to the positive characteristic 'geometric setting' (i.e. function fields of varieties), in the 1990s Pheidas and Videla demonstrated the existential undecidability of the simplest such function fields: $\mathbb{F}_q(t)$ where $\mathbb{F}_q$ is a finite field [Phe91, Vid94]. This was followed

shortly by Shlapentokh, who in 1996 showed (nearly[1]) all function fields of curves over finite fields are existentially undecidable [Shl96]. Around this time, answers were also sought for positive characteristic function fields over infinite fields of constants (see e.g. [KR92a, Shl00]) and function fields of higher transcendence degree (see [Shl02a, Shl05]). Eisenträger in 2012 showed the existential undecidability of a function field of transcendence degree greater than 1 over an algebraically closed field of odd characteristic [Eis12] (generalising Kim & Roush [KR92b]), and in 2013 Eisenträger & Shlapentokh showed the existential undecidability of *any* function field of characteristic p *not* containing $\widetilde{\mathbb{F}_p}$ (originally announced in [ES13], this was later published in [ES17]. See *Theorems 1.1 & 1.2 ibid.*). As it stands the only[2] problem left to solve in this area is 'Hilbert's Tenth Problem over $\widetilde{\mathbb{F}_p}(\mathcal{C})$', i.e. the existential decidability of the function field of a curve over an algebraically closed field of characteristic p.

We will mention that the decidability problem for the full theory of a positive characteristic function field has been completely solved. Indeed, first Ershov [Eršˇ65b] in 1965/Penzin [Pen73] in 1973 demonstrated the undecidability of $\mathtt{Th}(\mathbb{F}_q(t))$. This was generalised by Cherlin to infinite perfect constant subfields [Che84], and generalised further by Pheidas [Phe04]. Finally Eisenträger & Shlapentokh solved this problem in complete generality, showing every function field of positive characteristic has an undecidable theory ([ES09] and [ES17, Theorem 1.3]). We will also note this recollection has been focused on *positive* characteristic *function fields* – there are many interesting algebraic structures (even e.g. characteristic *zero* function fields, or positive characteristic *coordinate rings*) that we have not mentioned. The interested reader is invited to explore [PZ00].

Implicitly, all of the above undecidability results are for theories of function fields K in *the language of rings* $\mathcal{L}_r = \{0, 1, +, \times\}$ expanded by a set of *constants* which are interpreted as the elements of some recursive finitely generated subfield of K. What if we altered this basic assumption? It appears to be a well known fact that Hilbert's Tenth

[1] Shlapentokh proved this for odd characteristic; the even characteristic case was resolved by Eisenträger in 2003 [Eis03].

[2] The author is not aware of a result on the existential decidability of $\widetilde{\mathbb{F}_2}(V)$ for V a $\widetilde{\mathbb{F}_2}$-variety of dimension > 1, though this would be a minor gap in the literature, if indeed present.

Problem over $\mathbb{F}_q[t]$ with coefficients in $\mathbb{F}_p$ is solvable, or equivalently that $\mathtt{Th}_{\exists^+}(\mathbb{F}_q[t])$ in the language of rings *without additional constants* is decidable (it is very important that we consider the *positive* existential theory of $\mathbb{F}_q[t]$. The *existential* theory – allowing negations – is undecidable, implicitly by [PZ99, Theorem 2.1]). The natural question to subsequently ask is whether Hilbert's Tenth Problem over the fraction field $\mathbb{F}_q(t)$ with coefficients in $\mathbb{F}_p$ is similarly solvable. This is more difficult to answer – perhaps because in this context, the language of rings has an implicit geometric flavour. Certainly, consider the unary predicate F defining the nonconstant elements of $\mathbb{F}_q(t)$, i.e. $\mathbb{F}_q(t) \models F(x) \iff x \in \mathbb{F}_q(t) \setminus \mathbb{F}_q$, and note that $F(\mathbb{F}_q(t))$ is $\exists^+$-$\emptyset$-definable in the language of rings. Thus, we might equally have motivation to frame the above questions in the 'geometric' language $\mathcal{L}_F = \{0, 1, +, \times, F\}$. From the perspective of geometry, the subtlety between these problems is highlighted:

Theorem 1.1.1. *There exists an algorithm which upon input an affine $\mathbb{F}_p$-variety[3] $\mathscr{V}$ outputs "YES" if there exists an $\mathbb{F}_p$-morphism $\mathbb{A}^1 \to \mathscr{V}$, and "NO" otherwise.*

There <u>does not</u> exist an algorithm which upon input an affine $\mathbb{F}_p$-variety $\mathscr{V}$ outputs "YES" if there exists a <u>nonconstant</u> $\mathbb{F}_p$-morphism $\mathbb{A}^1 \to \mathscr{V}$, and "NO" otherwise.

Proof. The former follows from the aforementioned decidability of $\mathtt{Th}_{\exists^+}(\mathbb{F}_q[t])$ in the language of rings without additional constants. The latter is [PZ99, Theorem 2.1]. ■

It is an open problem, whether there exists an algorithm which upon input an affine $\mathbb{F}_p$-variety $\mathscr{V}$ outputs "YES" if there exists a (nonconstant) $\mathbb{F}_p$-<u>rational map</u> $\mathbb{A}^1 \dashrightarrow \mathscr{V}$, and "NO" otherwise.

In the first third of this thesis we will seek to answer decidability questions in the geometric language. In *Chapter 2* we recall a result of Pasten (§2.1) and generalise techniques of Eisenträger & Shlapentokh (§2.2) to conclude undecidability for some fields, in the language of rings augmented by a predicate B_l defining 'good behaviour' relative to a fixed prime l (elements that are *l-behaved*; see *Definition 2.2.1*). We then make some progress in §2.4 eliminating this arithmetic-controlling predicate B_l, though

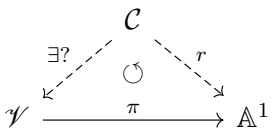
[3] Given to the algorithm as a finite list of elements of $\mathbb{F}_p[X_1, \ldots, X_n]$ for some $n \geq 1$.

we are unable to prove *existential* undecidability results (§2.4 explains why). We are able to get some distance by using a single initial universal quantifier:

Corollary 2.4.8. *Let K be the function field of a curve, of odd characteristic and constant subfield $C \subsetneq \widetilde{\mathbb{F}_p}$. There exists $d \in C$ such that $\mathtt{Th}_{\forall^1\exists}(K; \mathcal{L}_F(d))$ is undecidable.*

Note as the element $d \in C$ is algebraic over $\mathbb{F}_p$, $\mathtt{Th}_{\exists}(K; \mathcal{L}_F(d))$ is decidable if and only if $\mathtt{Th}_{\exists}(K; \mathcal{L}_F)$ is. Also note that *any* function field is the function field of a curve, under a suitable interpretation of F. As in *Theorem 1.1.1*, this can be reformulated in geometric terms.

Corollary 2.4.8 (reformulated). *Let $\mathcal{C}$ be an absolutely irreducible curve defined over a finite field $\mathbb{F}_q$ of odd characteristic. No algorithm exists which, upon input an $\mathbb{F}_q$-morphism $\pi : \mathscr{V} \to \mathbb{A}^1$ of affine $\mathbb{F}_q$-varieties, outputs "YES" if for all nonconstant $\mathbb{F}_q$-rational maps $r : \mathcal{C} \dashrightarrow \mathbb{A}^1$ there exists an $\mathbb{F}_q$-rational map $\mathcal{C} \dashrightarrow \mathscr{V}$ making the below diagram commute, and "NO" otherwise.*



Following a suggestion due to E. Hrushovski, in §2.5 we also demonstrate a scenario where a natural subset of l-behaved elements is existentially $\mathcal{L}_F$-definable with parameters in a finite field (this will be when the function field has sufficiently high genus, indicating the use of the predicate B_l is in a sense 'not too strong' and only applicable to low genus function fields).

1.2 Further Afield and Further, A Field?

In the latter two-thirds of the thesis, *Chapters 3 & 4*, we move from considering specific questions about a field's geometry to the following more elementary question in field theory:

Problem 1.2.1. *Does there exist an infinite, finitely axiomatisable field?*

This folkloric problem was posed explicitly by I. Kaplan at the 2016 Oberwolfach workshop on *Definability and Decidability Problems in Number Theory* [KPSV16, Q4]. It remains open, though speculation would have it be answered in the negative. This relates closely to another elementary question:

Problem 1.2.2. *Does there exist a finitely axiomatisable theory of fields which is decidable and has an infinite model?*

That is, this problem is to ascertain the existence of an infinite field F and a collection of first-order sentences T in the language of rings $\mathcal{L}_r$, such that $T \subseteq \mathtt{Th}(F)$, T is finitely axiomatised and closed under logical consequence, T models the field axioms, and there exists a decision procedure to determine membership of T.

Of course, answering *Problem 1.2.1* positively immediately answers *Problem 1.2.2; T* can be taken to be the $\mathcal{L}_r$-theory of the field answering *Problem 1.2.1.* In contrapositive, answering *Problem 1.2.2* in the negative (as the empirical evidence suggests might indeed be the case) would answer *Problem 1.2.1* in the negative too. This is the focus of modern investigations. One approach to answering *Problem 1.2.2* in the negative was established by Ziegler [Zie82] and generalised further by Shlapentokh & Videla [SV14]. Define:

Definition 1.2.3. Let $\mathcal{L}$ be a language. An *$\mathcal{L}$-theory* T is a set of $\mathcal{L}$-sentences closed under logical consequence. A *subtheory* of T is a subset T' of $\mathcal{L}$-sentences of T, closed under logical consequence, and T' is a *finite* subtheory if it is nonempty and finitely axiomatised.

Ziegler's idea was to take a finite subtheory of the $\mathcal{L}_r$-theory of a 'large enough' field with a powerful model completeness property (he considered $\mathbb{C}$, $\widetilde{\mathbb{F}_p(t)}$, $\mathbb{R}$ and $\mathbb{Q}_p$) and prove it to be a subtheory of a field interpreting arithmetic. Therefore by a result of Tarski (*Theorem A.8;* see *Appendix A* for more detail) there is no finite subtheory of $\mathtt{ACF}_0$, $\mathtt{ACF}_p$, $\mathtt{RCF}$, or $p\mathtt{CF}$ that is decidable. With this in mind we forward the following definition[4]:

[4]Shlapentokh & Videla [SV14] call this property *finite hereditary undecidability*; for notational ease we remove the word "hereditary" (thanks to W. Wołoszyn for this suggestion).

Definition 1.2.4. A theory T is *finitely undecidable* if every finite subtheory of T is undecidable.

This contrasts with an *essentially undecidable* theory T; one where not only T is undecidable, but every consistent extension of T in the same language is also undecidable (see [TMR53] for a general discussion on this subject). This is also sharper than *hereditary undecidability;* where T and *all* its nonempty subtheories are undecidable (see *Appendix A* for further discussion, and [TMR53, Sho93].) For example, the common $\mathcal{L}_r$-theory of fields is hereditarily undecidable.

What infinite fields are finitely undecidable? (A *field* is finitely undecidable if its theory in the language of rings is.) That is the motivating question for this half of the thesis. If there exists a field satisfying *Problem 1.2.1*, this field is not finitely undecidable; however we will show there is a considerably broad class of fields whose members are finitely undecidable. In particular, most (if not all) infinite fields whose model theory in the language of rings is well understood will be finitely undecidable, as we will argue.

Shlapentokh & Videla [SV14, Theorem 2] generalise Ziegler's construction away from specific field theories and furnish a general collection of field theories, consisting of specific sentences incompatible with `ACF`, they prove to be finitely undecidable. The author in *Chapter 3* will, following motivation from general model-theoretic dividing lines, adapt Ziegler's argument to the theories $\mathtt{SCF}_{p,v}$ and the complete theories of certain henselian valued fields. This will also serve as a brief indication as to how Ziegler's argument can pass to expansions of the field language (cf. §3.5). The main result of *Chapter 3* is:

Corollary 3.4.10. *Let (K, v) be an equicharacteristic 0 or mixed characteristic henselian nontrivially valued field. Then $\mathtt{Th}(K; \mathcal{L}_{val})$ is finitely undecidable.*

Let (K, v) be an equicharacteristic $p > 0$ NIP henselian nontrivially valued field. Then $\mathtt{Th}(K; \mathcal{L}_{val})$ is finitely undecidable.

Furthermore, assuming the NIP Fields Conjecture*, every infinite NIP field is finitely undecidable.*

Another approach to answering *Problem 1.2.1* was suggested to the author by E.

Hrushovski, who indicated the possibility that existing arguments could be adapted from the undecidability results on theories of "pseudo-closed" fields such as PAC, PRC, and PpC (the theories of *pseudo-algebraically closed*, *pseudo-real closed*, and *pseudo-p-adically closed* fields, respectively). The discussion of this – which, incidentally, follows nicely from the model-theoretic motivations of *Chapter 3* – forms the last third of this thesis (*Chapter 4*).

First, we adapt the arguments of Cherlin, van den Dries & Macintyre [CvdDM80] and independently Ershov [Ers81] to prove *every PAC field is finitely undecidable* (*Corollary 4.1.21*). Next, we adapt the work of Haran & Jarden [HJ85, Har84] to show more generally *every PRC field is finitely undecidable* too (*Corollary 4.2.16*). As a consequence we answer two open questions of Shlapentokh & Videla [SV14, §6] – see *Remark 4.2.18*. We are unable to use this method to prove finite undecidability of PpC fields – §4.3 explains why – but we can determine *no* bounded[5] *PpC field is finitely axiomatizable* (*Theorem 4.3.9*) after setting up the correct machinery to adjust work of Haran & Jarden [HJ88]. (The reader unfamiliar with [HJ85, HJ88] should consult *Appendices B & C*.) This gives the author confidence to forward the following problem:

Problem 1.2.5. *Does there exist an infinite field that is* not *finitely undecidable?*

If *Problem 1.2.5* is resolved in the negative, this gives a negative answer to *Problems 1.2.1 & 1.2.2*. Assuming (admittedly powerful) classification-theoretic conjectures, progress can be made on at least understanding the shape this problem takes: model-theoretically 'tame' structures will be finitely undecidable, and already many model-theoretically 'wild' structures have this property (e.g. the theories of all number fields and global function fields by J. Robinson, resp. Rumely [Rob59, Rum80], and more generally the theory of any positive characteristic function field by Eisenträger & Shlapentokh [ES17] or any infinite finitely generated field by Poonen [Poo07, Remark 5.2]).

In *Appendix A*, for reference we explicitly give two key hereditary undecidability results – the first due to Tarski, the second Ershov – which can be difficult to access in the literature.

[5] A field K is *bounded* if $\forall n > 1$, K has finitely many separable algebraic extensions of degree n.

1.3 Notation & Conventions

Let us set out the notations and conventions used in this thesis.

Algebraic: if K is a field then $\widetilde{K}$ will denote its algebraic closure, while K^s denotes its separable closure. $(L)^q$ will denote the set of q-th powers of the field L, whilst L^q is the set of tuples over L of length q. The henselisation of a field L will be denoted L^h, and the completion $\widehat{L}$ (the valuation will be clear from context). L^* denotes the nonzero elements of L. The compositum of two fields F, K will be denoted FK.

For a field F, a *positive cone* or an *ordering* is a subset $P \subseteq F$ such that P is closed under addition and multiplication, $-1 \notin P$, $P \cup -P = F$, and if $x \in F$ then $x^2 \in P$. Let $X(F)$ denote the space of orderings of F, equipped with the *Harrison* topology whose subbasis is $\{\{P \in X(F) : a \in P\} : a \in F^*\}$. Ordered fields are treated well in [Raj93, Chapter 15].

By a *K-variety* $\mathscr{V}$ we will mean an integral, separated scheme of finite type over the field K. $\mathscr{V}$ is *geometrically irreducible* if $\mathscr{V} \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K^s)$ is irreducible. A *curve* $\mathcal{C}$ is a K-variety such that $K(\mathcal{C})$ has transcendence degree 1 over K. For $x \in \mathscr{V}$, denote the stalk at x by $\mathcal{O}_{\mathscr{V},x}$; this is a local ring with maximal ideal $\mathfrak{m}_x$.

If G is a profinite group and $S \subseteq G$, denote by $\langle S \rangle$ the least closed normal subgroup of G containing S.

Model-theoretic: (Cf. [Mar02, §1.1].) Denote by $\mathrm{Sent}(\mathcal{L})$ the set of first-order sentences in the language $\mathcal{L}$, $\mathrm{Form}^n(\mathcal{L})$ the set of $\mathcal{L}$-formulae in $\leq n$ variables, and $\mathrm{Form}(\mathcal{L}) = \bigcup_{n\geq 0} \mathrm{Form}^n(\mathcal{L})$. $\mathtt{Th}(M;\mathcal{L})$ denotes the complete theory of the structure M in the language $\mathcal{L}$.

An *existential sentence* is a first-order sentence of the form $\exists x_1, \ldots, \exists x_k\, \theta(x_1, \ldots, x_k)$, where θ is a quantifier-free $\mathcal{L}$-formula. Such a sentence is called *positive* if the negation connective does not appear in θ. A *$\forall^m\exists$-sentence* is a first-order sentence of the form $\forall x_1, \ldots, \forall x_m \exists y_1, \ldots, \exists y_n\, \rho(x_1, \ldots, x_m, y_1, \ldots, y_n)$, where ρ is a quantifier-free $\mathcal{L}$-formula, for any $n \geq 0$. Let $\mathtt{Th}_\exists(M;\mathcal{L})$, $\mathtt{Th}_{\exists^+}(M;\mathcal{L})$, and $\mathtt{Th}_{\forall^m\exists}(M;\mathcal{L})$ denote the subset of $\mathtt{Th}(M;\mathcal{L})$ consisting of existential, positive existential, and $\forall^m\exists$-sentences respec-

tively. More generally, let $\mathrm{Sent}_{\exists}(\mathcal{L}), \mathrm{Sent}_{\exists^+}(\mathcal{L})$, and $\mathrm{Sent}_{\forall^m\exists}(\mathcal{L})$ denote the subset of $\mathrm{Sent}(\mathcal{L})$ consisting of existential, positive existential, and $\forall^m\exists$-sentences respectively. Let $\mathrm{Form}_{\exists}(\mathcal{L})$ denote the subset of $\mathrm{Form}(\mathcal{L})$ consisting existential $\mathcal{L}$-formulae.

We fix $\mathcal{L}_r = \{0, 1, +, \times\}$ as the language of rings, $\mathcal{L}_{oag} = \{0, +, \leq\}$ as the language of ordered abelian groups, $\mathcal{L}_{val} = \{0, 1, +, \times, \mathcal{O}\}$ as the language of valued fields (where $\mathcal{O}$ is interpreted as a valuation ring, with the valuation clear from context), $\mathcal{L}_{gr} = \{R\}$ as the language of graphs (where R is interpreted as a binary, symmetric, irreflexive relation), and $\mathcal{L}_F = \{0, 1, +, \times, F\}$ as the *geometric* language of rings, where if K is a function field with field of constants k, the unary predicate F is interpreted as the nonconstant elements of K. Namely $F(K) = K \setminus k$. If $\mathcal{L}$ is a language and S a set of constant symbols not in $\mathcal{L}$, define $\mathcal{L}(S)$ to be the expansion of $\mathcal{L}$ by constant symbols $s \in S$. If $S = \{a_1, \ldots, a_n\}$ we may write $\mathcal{L}(a_1, \ldots, a_n)$ for $\mathcal{L}(S)$.

If M, N are $\mathcal{L}$-structures, $M \leq N$ denotes that M is an $\mathcal{L}$-substructure of N, while $M \lneq N$ denotes that M is a *proper* $\mathcal{L}$-substructure of N (we suppress mention of $\mathcal{L}$). If the $\mathcal{L}$-structures M, N are elementarily equivalent, this shall be written $M \equiv_{\mathcal{L}} N$. Alternatively, if $E \leq M, N$ then $M \equiv_E N$ denotes that M and N are elementarily equivalent over the common substructure E.

A language is assumed to be finite unless otherwise stated (most relevant for *Appendix A*) and implicitly contains the equality predicate "$=$", which we do not typically write.

Other: The arrows $\twoheadrightarrow$ and $\hookrightarrow$ denote a surjective and injective map respectively. Disjoint union is denoted "$\sqcup$". If the group G acts on the space X, the action of $g \in G$ on $x \in X$ is denoted x^g. If A, B are subsets of a ring, $A \cdot B = \{ab : a \in A, b \in B\}$ and $A \pm B = \{a \pm b : a \in A, b \in B\}$. "WLOG" initialises "without loss of generality", while "TFAE" initialises "the following are equivalent". If $\sum_\gamma a_\gamma t^\gamma$ is a formal sum over a field k, its *support* $\mathrm{supp}(\sum_\gamma a_\gamma t^\gamma) := \{\gamma : a_\gamma \neq 0\}$.

1.3.1 Neostability

When we speak of "model-theoretically tame" structures, or fields "whose model theory is understood", we are referring to theories that satisfy well known and well understood classification properties that make these theories easier to survey. The first dividing line we will draw is between the *stable* and *unstable* theories. For this discussion, fix a background monster model $\mathfrak{C}$ of the theory in question, such that all subsets mentioned have small cardinality relative to $\mathfrak{C}$. Cf. [TZ12, Chapter 6–8].

Definition 1.3.1. A formula $\phi(x, y)$ has the *order property* if there are sequences $(a_i)_{i\in\omega}$, $(b_j)_{j\in\omega}$ such that $\mathfrak{C} \models \phi(a_i, b_j) \iff i < j$. A theory is *stable* if no formula in its language has the order property.

See Tent & Ziegler [TZ12, Chapter 8] for more information; in particular it is explained how stable theories have few types, and these types behave well under extensions of the parameter sets they are defined over (viz. the machinery of *forking* and *dividing*). There is also a natural notion of 'independence' for stable theories (*forking independence*), that in e.g. algebraically closed fields of characteristic 0 corresponds to algebraic independence. Indeed, stable theories can be characterised as those theories with a ternary 'forking independence relation' $\downarrow$ that satisfies a certain list of properties [TZ12, §8.5] we will not cover here. Algebraically closed fields of a fixed characteristic, separably closed fields of a fixed characteristic & degree of imperfection, and differentially closed fields of a fixed characteristic are all examples of (complete) stable theories.

As the definition suggests, the notion of a stable theory is completely orthogonal to the notion of a theory with a linear order. How do we generalise the concept of a stable theory? *NIP theories* are permitted an order (but nothing more general), whereas *simple theories* generalise some of the forking machinery behind stable theories.

Definition 1.3.2. A formula $\phi(x, y)$ has the *independence property* if there are sequences $(a_i)_{i\in\omega}$, $(b_J)_{J\in\mathcal{P}(\omega)}$ such that $\mathfrak{C} \models \phi(a_i, b_J) \iff i \in J$. A theory is *NIP* if no formula in its language has the independence property.

See Simon [Sim15] for more information. Examples of such theories include (all

stable theories, and) algebraically closed valued fields of a fixed characteristic and residue characteristic, $\mathbb{Q}_p$ in the language of valued fields, and RCF in the language of ordered rings. On the other hand, there are simple theories:

Definition 1.3.3. A formula $\phi(x, y)$ has the *tree property* if there are $(a_\eta)_{\eta \in \omega^{<\omega}}$ and $k \geq 2$ such that:

- $\forall \sigma \in \omega^\omega$, $\{\phi(x, a_{\sigma|_n}) : n < \omega\}$ is consistent (with $\mathfrak{C}$);
- $\forall \eta \in \omega^{<\omega}$, $\{\phi(x, a_{\eta \circ n}) : n < \omega\}$ is k-inconsistent[6] (where $\circ$ denotes concatenation of sequences).

A theory is *simple* if no formula in its language has the tree property.

Simple theories can also be characterised by a notion of forking independence, but we shall not do this here: the curious reader is invited to explore [Wag00]. Standard examples include (all stable theories, and) the random graph in the language of graphs, pseudo-finite fields, and imperfect bounded PAC fields.

Finally, while there are many more common dividing lines we have not yet mentioned, we will mention *rosy theories* as they are the broadest class of theories for which the author is aware of a field-theoretic conjecture. According to [Kru15], the motivation for *rosy theories* (cf. [Ons02]; originally suggested by T. Scanlon) is as the most general context which "allows the application of techniques from stability theory, especially of basic forking calculus" [Kru15, p. 347].

Definition 1.3.4. [Kru15, pp. 347–348]. T is *rosy* if there is a ternary relation $\mathop{\smile\!\!\!\!\!\!|}$ on small subsets of $\mathfrak{C}^{eq}$ satisfying all the basic properties of forking independence in simple theories, except for the *Independence Theorem*.

This definition arises from [EO07]. Furthermore, rosy theories admit a specific independence relation denoted $\mathop{\smile\!\!\!\!\!\!|}^{\text{þ}}$, known as þ-*independence* ("thorn-independence"; see [EO07, Def. 2.1]) which is the "weakest" independence relation for T [EO07, Theorem 3.3]. Using þ-independence, we may define a *rank* on types (the $U^{\text{þ}}$-*rank*) "the same

[6] Every k-element subset of $\{\phi(x, a_{\eta \circ n})\}$ is inconsistent.

way as U-rank is defined in stable theories by means of $\perp$" [Kru15, p. 349]. Then we may define *superrosy* theories:

Definition 1.3.5. [EO07, Fact 4.4]. T is *superrosy* if and only if every type has bounded U^{b}-rank.

It should be emphasised that the reader need not be overly familiar with this machinery, merely be aware of its existence (and be willing to believe certain well-established, motivating conjectures later on). These properties (and many more) can be arranged in an attractive illustration that provides a lens through which to view the model-theoretic universe:

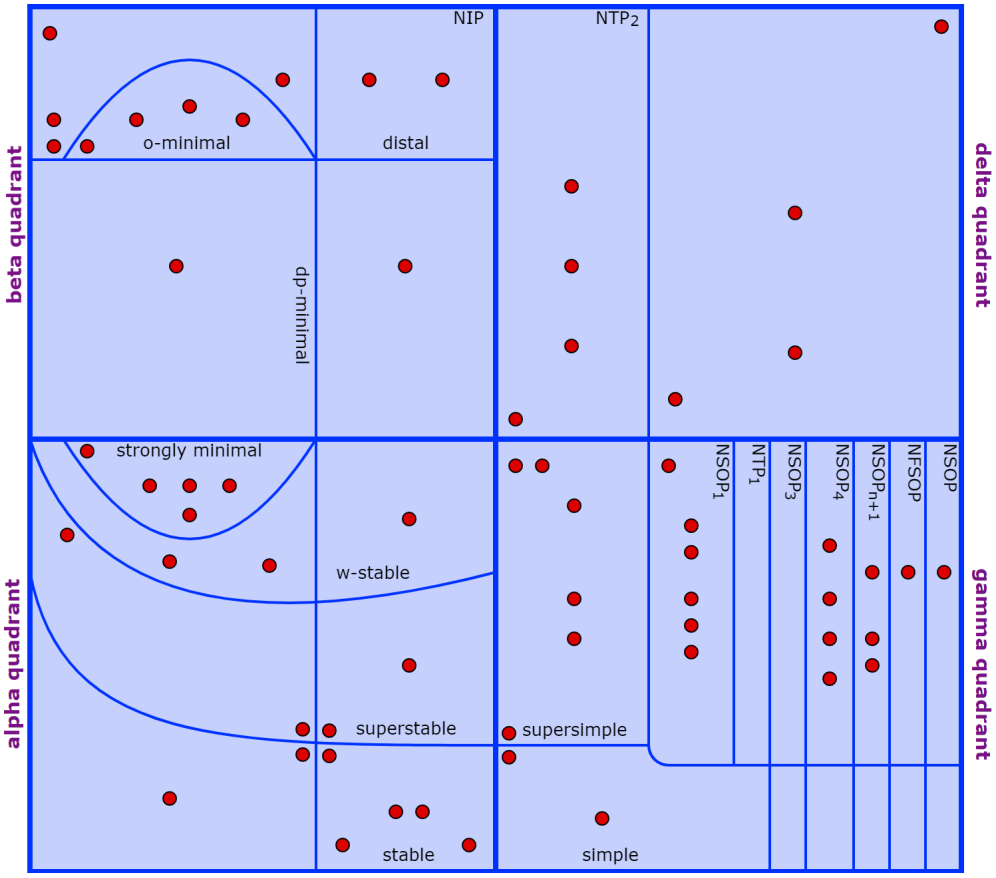


Figure 1.1: Snapshot of the model-theoretic universe with Shelah's dividing lines. Red points are theories. Source: `forkinganddividing.com`, accessed 02/2022.

In *Figure 1.1*, a label is attached to the smallest box containing theories of that

label; e.g. everything in the left half of the image is NIP. (Super)rosy theories are not pictured here, however (super)simple theories are a *proper* subset of (super)rosy theories, as it is known the theory of a formally real bounded pseudo-real closed field that is not real closed is NTP_2, has IP, and is not simple (see [Mon17, §4.1]), yet is superrosy (a consequence of [Ons02, Theorem A.1.1.2 & Corollary 2.5.2.3]). We will discuss "formally real pseudo-real closed fields" in §4.2.

Chapter 2

Well-Behaved Machinery

In modern publications (cf. [ES17, Shl96, Shl00, Shl07]) there is a standard two-step process to conclude existential undecidability of the function field K of a curve $\mathcal{C}$ with field of constants C in characteristic $p > 0$. Denote $C_0 := \widetilde{\mathbb{F}_p} \cap C$.

STEP 1: Define the "Denef" predicate $\mathrm{Den}_p(x, y) \iff \exists s \in \mathbb{N}\ \ x = y^{p^s} \vee y = x^{p^s} \iff \exists s \in \mathbb{Z}\ \ x = y^{p^s}$.

STEP 2: Define for a nonconstant 'special' element $u \in K$, with $\mathrm{ord}_{\mathfrak{p}}\, u = 1$ for some prime $\mathfrak{p}$ of K, a set $\mathrm{INT}(K, \mathfrak{p}, u)$ with the property that if $x \in \mathrm{INT}(K, \mathfrak{p}, u)$ then $\mathrm{ord}_{\mathfrak{p}}\, x \geq 0$, and if $x \in C_0(u)$ and $\mathrm{ord}_{\mathfrak{p}}\, x \geq 0$ then $x \in \mathrm{INT}(K, \mathfrak{p}, u)$.

We will apply the following results in *Chapter 2*.

Theorem 2.0.1. *Let p be a prime number. Then $\mathtt{Th}_{\exists^+}(\mathbb{N}; 0, 1, +, |_p, \leq)$ is undecidable, where $|_p$ is the binary predicate defined by $a|_p b \iff \exists s \in \mathbb{N},\ b = p^s a \vee a = p^s b$.*

Proof. Pheidas [Phe87, Theorem 1] proved $\mathtt{Th}_{\exists^+}(\mathbb{N}; 0, 1, +, |^p)$ is undecidable, where now $n|^p m \iff \exists s \in \mathbb{N},\ m = p^s n$. This relation is $\exists^+$-definable in $\mathtt{Th}_{\exists^+}(\mathbb{N}; 0, 1, +, |_p, \leq)$, as $x|^p y \iff x|_p y \wedge x \leq y$. We conclude $\mathtt{Th}_{\exists^+}(\mathbb{N}; 0, 1, +, |_p, \leq)$ is undecidable. ∎

Theorem 2.0.2. *Let K be a field and let $f(T_1, \ldots, T_{n_1}, X_1, \ldots X_{n_2}, Y_1, \ldots, Y_{n_3})$, $g(X, T_1, \ldots, T_{n_1}) \in K[X, T_1, \ldots, T_{n_1}, X_1, \ldots, X_{n_2}, Y_1, \ldots, Y_{n_3}]$ be polynomials with coefficients in K. Assume the degree of g in X is positive and the same for all values of*

$T_1, \ldots, T_{n_1}$ *(i.e. writing* $g(X, T_1, \ldots, T_{n_1}) = g_k(T_1, \ldots, T_{n_1})X^k + \cdots + g_0(T_1, \ldots, T_{n_1})$ *as a polynomial in* X *over* $K[T_1, \ldots, T_{n_1}]$*,* $g_k(t_1, \ldots, t_{n_1}) \neq 0$ *for all* $t_1, \ldots, t_{n_1} \in K$*, and* $k > 0$*). Let* $A \subseteq K^{n_1}$ *be defined as follows:*

$$(t_1, \ldots, t_{n_1}) \in A \iff \exists x_1, \ldots, x_{n_2} \in K,\ x \in \widetilde{K},\ y_1, \ldots, y_{n_3} \in K(x) \text{ s.t.}$$
$$g(x, t_1, \ldots, t_{n_1}) = 0 \wedge f(t_1, \ldots, t_{n_1}, x_1, \ldots, x_{n_2}, y_1, \ldots, y_{n_3}) = 0.$$

Then A *has a diophantine definition over* K*, i.e. there exists a polynomial* $h(T_1, \ldots, T_{n_1}, X_1, \ldots, X_{n_4}) \in K[T_1, \ldots, T_{n_1}, X_1, \ldots, X_{n_4}]$ *such that*

$$(t_1, \ldots, t_{n_1}) \in A \iff \exists x_1, \ldots, x_{n_4} \in K \text{ s.t. } h(t_1, \ldots, t_{n_1}, x_1, \ldots, x_{n_4}) = 0.$$

Moreover, the coefficients of h *depend only on the coefficients and degrees of* g *and* f*, and can be computed effectively and uniformly from the coefficients of* g *and* f*.*

Proof. A similar formulation is found in [ES17, §3] and follows from [Shl07, Lemma B.7.5] exactly; that the coefficients of h can be "computed effectively and uniformly from the coefficients of g and f" is [Shl07, p. 335] following *Remark B.7.4 ibid.* ■

Now, recall the following definition(s) and notation(s), from [Shl07, §B.7]:

Definition 2.0.3. [Shl07, Definitions B.7.1 & B.7.2]. Let K be a field and L a finite extension of K. Let $\Omega = \{\omega_1, \ldots, \omega_d\}$ be a basis of L over K, let $\pi : K^d \to L$ be defined by $(f_1, \ldots, f_d) \mapsto \sum_{i=1}^d f_i\omega_i$, and let $\sigma = (\sigma_1, \ldots, \sigma_d)$ be a linear K-section of π defined by $\sigma_j(\sum_{i=1}^d f_i\omega_i) = f_j$. We may extend σ to *polynomials* over L, by defining

$$\sigma_j(q(z_1, \ldots, z_m)) = \sum_{i_1, \ldots, i_m} \sigma_j(a_{i_1, \ldots, i_m}) z_1^{i_1} \ldots z_m^{i_m},$$

for $q(z_1, \ldots, z_m) = \sum_{i_1, \ldots, i_m} a_{i_1, \ldots, i_m} z_1^{i_1} \ldots z_m^{i_m} \in L[z_1, \ldots, z_m]$.

Let $p(x_1, \ldots, x_m, w_1, \ldots, w_n)$ be a polynomial over L. For $1 \leq j \leq d$, define the j*th*

coordinate polynomial of p with respect to Ω and $(x_1, \ldots, x_m)$ to be

$$p_j^{\Omega}(x_{1,1}, \ldots, x_{m,d}, w_1, \ldots, w_n) = \sigma_j \left(p(\textstyle\sum_{i=1}^{d} x_{1,i}\omega_i, \ldots, \sum_{i=1}^{d} x_{m,i}\omega_i, w_1, \ldots, w_n) \right).$$

Remark 2.0.4. One can confirm from this definition that p_j^{Ω} is a polynomial over K, and

$$p(\textstyle\sum_{i=1}^{d} x_{1,i}\omega_i, \ldots, \sum_{i=1}^{d} x_{m,i}\omega_i, w_1, \ldots, w_n) = \sum_{i=1}^{d} p_i^{\Omega}(x_{1,1}, \ldots, x_{m,d}, w_1, \ldots, w_n)\omega_i.$$

Consider the case where K is a characteristic $p > 0$ one-variable function field, with (perfect) constant subfield $C \subsetneq \widetilde{\mathbb{F}_p}$, and $C(b)/C$ is a finite extension of degree d with basis $\Omega = \{1, b, b^2, \ldots, b^{d-1}\}$, and $L = KC(b) = K(b)$. Then L has constant subfield $C(b)$ and Ω is a basis for L/K ([Ros02, Propositions 8.1 & 8.3]). If $\mathbb{F}_q/\mathbb{F}_p$ is a finite extension with $\mathbb{F}_q \subseteq C$, and $p(x_1, \ldots, x_m, w_1, \ldots, w_n)$ is a polynomial over $\mathbb{F}_q(b) \subset L$, then $p(\sum_{i=1}^{d} x_{1,i}b^{i-1}, \ldots, \sum_{i=1}^{d} x_{m,i}b^{i-1}, w_1, \ldots, w_n)$ is a polynomial over $\mathbb{F}_q(b)$ and for all $1 \leq j \leq d$, $p_j^{\Omega}(x_{1,1}, \ldots, x_{m,d}, w_1, \ldots, w_n)$ is a polynomial over $\mathbb{F}_q$. □

We will require the following:

Lemma 2.0.5. *Let K be a positive characteristic one-variable function field with constant subfield $C \subsetneq \widetilde{\mathbb{F}_p}$, and let $C(b)/C$ be a finite extension of degree d. Let $\mathbb{F}_q/\mathbb{F}_p$ be a finite extension with $\mathbb{F}_q \subseteq C$, and $P(X_0, \ldots, X_k) \in \mathbb{F}_q(b)[X_0, \ldots, X_k]$. Fix $\{i_1, \ldots, i_{n+m}\} \subseteq \{1, \ldots, k\}$. Then, for $w \in K$:*

$$\exists x_1, \ldots, x_k \in K(b),\ P(x_1, \ldots, x_k, w) = 0 \wedge \bigwedge_{j=1}^{n} F(x_{i_j}) \wedge \bigwedge_{j=n+1}^{n+m} \neg F(x_{i_j}) \tag{2.1}$$

$$\iff$$

$$\exists x_{1,1}, \ldots, x_{k,d} \in K,\ \bigwedge_{j=1}^{d} P_j^{\Omega}(x_{1,1}, \ldots, x_{k,d}, w) = 0 \quad \wedge$$

$$\bigwedge_{j=1}^{n} \left(\bigvee_{l=1}^{d} F(x_{i_j,l}) \right) \wedge \bigwedge_{j=n+1}^{n+m} \left(\bigwedge_{l=1}^{d} \neg F(x_{i_j,l}) \right),$$

where $\Omega = \{1, b, \ldots, b^{d-1}\}$ *is a basis for* $K(b)/K$*, as well as for* $C(b)/C$*, and the polynomials* $P_j^{\Omega}(x_{1,1}, \ldots, x_{k,d}, w)$ *are defined over* $\mathbb{F}_q$*.*

Proof. From *Remark 2.0.4* we see $K(b) = KC(b)$ has basis Ω and for $1 \leq j \leq d$, the polynomial P_j^{Ω} is defined over $\mathbb{F}_q$. Now, fix $w \in K$. To prove the forward implication, fix witnesses $a_1, \ldots a_k \in K(b)$ and for $1 \leq i \leq k$, $1 \leq j \leq d$, set $a_{i,j} := \sigma_j(a_i) \in K$. By definition, $a_i = \sum_{j=1}^{d} a_{i,j} b^{j-1}$. From *Remark 2.0.4* we see $P(a_1, \ldots, a_k, w) = 0$ implies $\bigwedge_{j=1}^{d} P_j^{\Omega}(a_{1,1}, \ldots, a_{k,d}, w) = 0$ as Ω is a basis for $K(b)/K$.

Recall $K \models \neg F(z)$ if and only if $z \in C$. For any $1 \leq l \leq k$, $K(b) \models F(a_l)$ if and only if $K \models F(a_{l,1}) \vee \cdots \vee F(a_{l,d})$, and $K(b) \models \neg F(a_l)$ if and only if $K \models \neg F(a_{l,1}) \wedge \cdots \wedge \neg F(a_{l,d})$, as the constant subfield of $K(b)$ is $C(b)$ exactly (*Remark 2.0.4*) and Ω is a basis for $C(b)/C$.

From this we conclude the forward implication. For the reverse implication, fix witnesses $a_{1,1}, \ldots, a_{k,d} \in K$. For $1 \leq i \leq k$ define $a_i = \sum_{j=1}^{d} a_{i,j} b^{j-1}$. From *Remark 2.0.4* we see $\bigwedge_{j=1}^{d} P_j^{\Omega}(a_{1,1}, \ldots, a_{k,d}, w) = 0$ implies $P(a_1, \ldots, a_k, w) = 0$, as Ω is a basis for $K(b)/K$. The paragraph above allows us to conclude the reverse implication, as desired. ∎

2.1 Definability of the Denef Predicate

Step 1 is concluded in our setting (in the language $\mathcal{L}_F$, no parameters from the underlying field permitted) using arithmetic properties detailed by Pasten [Pas17] for all odd primes p (in fact, Pasten's method produces an $\mathcal{L}_F$-formula for the Denef predicate *uniform* in such p). We begin with the below theorem – all results in this subsection are obtained from Pasten [Pas17], and elaborated here for the sake of exposition, that parameters from K are not necessary when using the language $\mathcal{L}_F$.

Theorem 2.1.1. [Pas17, Remark 1, Theorem 1.6]. *Let* $g \geq 0$*,* $d \geq 1$ *be integers and let* $p > 2$ *be a prime. Let*

$$M = M(g, d, p) = \left\lceil \frac{1}{d} \left(4g + 12 + 8 \sum_{i=1}^{\lceil (d-1)/2 \rceil} p^i \right) \right\rceil.$$

Then we have the following:

Let k be a field of characteristic p and let K be a one variable function field of genus g defined over k. Let $F_1, \ldots, F_M \in \mathbb{F}_p[X]$ be pairwise coprime irreducible polynomials of degree d. Take $f, h \in K$ both nonconstant. There exists $s \in \mathbb{N}$ such that $f = h^{p^s}$ or $h = f^{p^s}$ if and only if $F_i(f)F_i(h)$ is a square in K for each $i = 1, \ldots, M$. ■

Theorem 2.1.2. *Let $g \geq 0$ be an integer. There exists an existential $\mathcal{L}_F$-formula $\varphi_g(x, y)$ with the following property:*

Given any prime $p > 2$, any field k of positive characteristic p, and any function field K/k of a curve of genus g, for every pair of elements $f, h \in K$,

$$K \models \varphi_g(f, h) \iff \exists s \in \mathbb{N} \text{ s.t. } f = h^{p^s} \text{ or } h = f^{p^s}.$$

Proof. This is a minor adaptation of [Pas17, Theorem 1.5] to remove the dependency on the parameter. For $d \geq 1$, let M_d be the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[X]$. One may first prove for sufficiently large[1] primes d, $M_d > M = M(g, d, p)$ from *Theorem 2.1.1.* Therefore we may always chose distinct monic irreducible polynomials $F_1, \ldots, F_M \in \mathbb{F}_p[X]$ as required for *Theorem 2.1.1.*

Let $\phi_{g,p}(x, y)$ be the formula

$$\bigwedge_{i=1}^{M} \exists z \ (\widetilde{F}_i(x)\widetilde{F}_i(y) = z^2),$$

where $\widetilde{F}_i$ is a lift of F_i from $\mathbb{F}_p[X]$ to $\mathbb{Z}[X]$. Let k' be the constant subfield of K. By *Theorem 2.1.1*, if $K \models \phi_{g,p}(f, h) \vee (\neg F(f) \wedge \neg F(h))$ then either $f, h \in k'$ or $\exists s \in \mathbb{N}$ s.t. $f = h^{p^s}$ or $h = f^{p^s}$. Conversely, if $\exists s \in \mathbb{N}$ s.t. $f = h^{p^s}$ or $h = f^{p^s}$, then $K \models \phi_{g,p}(f, h)$.

Note that if $p > 4g + 12$ we may take $d = 1$ (hence $M = 4g + 12$) and chose polynomials $F_i = X - i$ for $i = 1, \ldots, M$. Hence for $p > 4g + 12$, we may chose $\phi_{g,p}$ uniformly in p; denote this ϕ_g.

Let $\chi_g(x, y)$ be the formula

[1] Pasten notes that $d \geq 2\log(12 + \sqrt{8g + 168})$ suffices.

$$\left(\left[\phi_g(x,y) \wedge \bigwedge_{p\leq 4g+12} p \neq 0\right] \vee \left[\bigvee_{p\leq 4g+12} \{p = 0 \wedge \phi_{g,p}(x,y)\}\right]\right),$$

and $\varphi_g(x,y)$ be the formula

$$\begin{aligned}&\big(F(x) \wedge F(y) \wedge \chi_g(x,y)\big) \quad \vee \\ &\qquad \big(\neg F(x) \wedge \neg F(y) \wedge \exists u, v\big[F(u) \wedge F(v) \wedge \chi_g(u,v) \wedge \chi_g(ux,vy)\big]\big)\end{aligned}$$

We claim this is the required formula. Indeed, if $f = h^{p^s}$ or $h = f^{p^s} \in K$ for $s \in \mathbb{N}$, then either the first or second disjunct of φ_g is satisfied, depending on whether f, h are both constant or not. On the other hand, if $K \models \varphi_g(f,h)$, then either f, h are nonconstant and $f = h^{p^s}$ or $h = f^{p^s}$ for $s \in \mathbb{N}$, or f, h are constant and there exists $s_1, s_2 \in \mathbb{N}$, $u, v \in K \setminus k'$ such that $u = v^{p^{s_1}}$ or $v = u^{p^{s_1}}$, and $uf = (vh)^{p^{s_2}}$ or $vh = (uf)^{p^{s_2}}$.

Hence, either $f = v^{p^{s_2}-p^{s_1}}h^{p^{s_2}}$, or $h = u^{p^{s_2}-p^{s_1}}f^{p^{s_2}}$, or $h = v^{p^{s_1}+s_2-1}f^{p^{s_2}}$, or $f = u^{p^{s_1}+s_2-1}h^{p^{s_2}}$. In the former two cases, if $s_1 \neq s_2$, this forces v or u to be constant; a contradiction. Therefore either $f = h^{p^{s_2}}$ or $h = f^{p^{s_2}}$ in this case. In the latter two cases, if either s_1 or s_2 is not 0, this again forces v or u to be constant; a contradiction. Therefore in this case $f = h = h^{p^0}$, as desired. ■

Hence Step 1 is immediately concluded:

Corollary 2.1.3. *Let K be the function field of a curve over a field of characteristic $p > 2$. The Denef predicate Den_p is existentially $\mathcal{L}_F$-$\emptyset$-definable in K.* ■

2.2 Integrality

The ideas behind the machinery presented here originate with Ershov [Eršˇ65b] and Penzin [Pen73], J. Robinson [Rob49, Rob59] and Rumely [Rum80]. They have been used extensively in this context by Shlapentokh (e.g. [Shl93, Shl96, Shl98, Shl02a, Shl02b, Shl05,

Shl15], and explained in detail in [Shl07, Chapter 4]), and Eisenträger-Shlapentokh [ES17]. Indeed, the process below is identical to [ES17, §6] with the exception that here we draw attention to any parameters used. The goal is to produce an existentially $\mathcal{L}_r$-defined subset of any function field, which forces its members to have 'small' poles. We will use a parameter in defining this set, but keep careful control on what exact properties this parameter satisfies.

Let p be any prime, and K be a one variable function field of characteristic $p > 0$ with any subfield of constants C. Denote the algebraic closure of $\mathbb{F}_p$ in C by C_0. Let l be a prime, not necessarily distinct to p.

Definition 2.2.1.[2] An element $u \in K$ is *l-behaved* if there exists a prime $\mathfrak{p}$ of K such that $v_{\mathfrak{p}}(u) > 0$, $v_{\mathfrak{p}}(u) \not\equiv 0 \mod l$, and $[Kv_{\mathfrak{p}} : C] \not\equiv 0 \mod l$. Define:

$$\mathfrak{z}_b(u) := \prod\{\mathfrak{p}^{v_{\mathfrak{p}}(u)} \ : \ v_{\mathfrak{p}}(u) > 0,\, v_{\mathfrak{p}}(u) \not\equiv 0 \mod l,\, [Kv_{\mathfrak{p}} : C] \not\equiv 0 \mod l\},$$

the *l-behaved factor* of the zero divisor $\mathfrak{z}(u)$ of u.

To begin, we assume the following unless otherwise stated:

Assumption ($\star$). There exists a prime $l \neq p$ such that C_0 contains an l-th primitive root of unity and, for some $a \in C_0$, K does not contain any root of $T^l - a$.

E.g. if K is global, C_0 will be a finite field $\mathbb{F}_{p^n}$; ($\star$) amounts to assuming $l|(p^n - 1)$. Assume there exists $u \in K$ such that u is l-behaved, and fix the following notation:

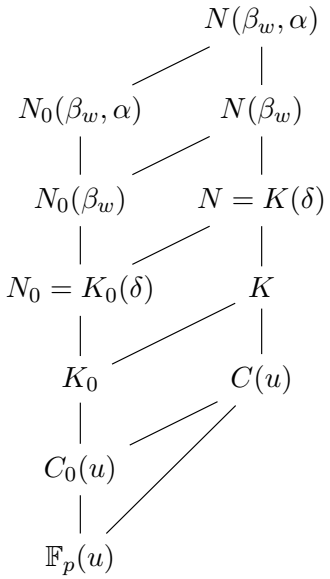
- Let K_0 denote the algebraic closure of $C_0(u)$ in K.
- Let $\delta \in \widetilde{K}$ be a root of $T^l - (u + 1)$.
- For $w \in K$, let $h_w = \frac{w^l}{u} + \frac{1}{u^l} = \frac{w^l u^{l-1}+1}{u^l}$.
- Let $\beta_w \in \widetilde{K}$ be a root of $T^l - (\frac{1}{h_w} + 1)$.
- Let $\alpha \in \widetilde{K}$ be a root of $T^l - a$.

[2] Terminology with thanks to R. O'Gorman.

Lemma 2.2.2. *$K_0/C_0(u)$ is a finite extension, i.e. K_0 is a function field over C_0.*

Proof. As C_0 is perfect, C/C_0 is a regular extension, and furthermore $C(u)/C_0(u)$ is regular ([FJ08, Lemma 2.7.5]), hence $C(u)$ is linearly disjoint from K_0 over $C_0(u)$. If $[K_0 : C_0(u)] > [K : C(u)] = n$, then there exist $x_0, \ldots, x_n \in K_0$ linearly independent over $C_0(u)$. By definition, $x_0, \ldots, x_n$ remain linearly independent over $C(u)$, contradicting $[K : C(u)] = n$. We conclude $[K_0 : C_0(u)] \leq [K : C(u)] < \infty$ as required. ∎

Consider the following extensions:



We have the following series of lemmas from [ES17]. From this point onward, we will interchange the notations "$v_{\mathfrak{p}}$" and "$\mathrm{ord}_{\mathfrak{p}}$" for a prime $\mathfrak{p}$.

Lemma 2.2.3. *Let G be a field of positive characteristic p possessing a primitive l-th root of unity ξ_l. Let $\alpha \in \widetilde{G}$ be a root of the equation $X^l - a = 0$, where $a \in G$. Let $\alpha_j = \xi_l^j \alpha$, $j = 0, \ldots, l-1$, and let*

$$P(X_0, \ldots, X_{l-1}) = \prod_{j=0}^{l-1} (X_0 + X_1\alpha_j + \cdots + X_{l-1}\alpha_j^{l-1}) \in G[X_0, \ldots, X_{l-1}].$$

If $[G(\alpha) : G] = l$, then for $a_0, \ldots, a_{l-1} \in G$, $\mathrm{Norm}_{G(\alpha)/G}(a_0 + a_1\alpha + \cdots + a_{l-1}\alpha^{l-1}) = P(a_0, \ldots, a_{l-1})$. Moreover if $\alpha \in G$, then for any $y \in G$ the equation $P(X_0, \ldots, X_{l-1}) = y$ has solutions $x_0, \ldots, x_{l-1} \in G$.

Proof. Cf. [ES17, Lemma 6.3] for the statement (the above is weaker). If $[G(\alpha) : G] = l$, by definition of the norm map, for $a_0, \ldots, a_{l-1} \in G$:

$$\mathrm{Norm}_{G(\alpha)/G}(a_0 + a_1\alpha + \cdots + a_{l-1}\alpha^{l-1}) = P(a_0, \ldots, a_{l-1}).$$

A priori P is defined over $G(\alpha)$ – however as its coefficients are invariant under $\mathrm{Aut}(G(\alpha)/G)$, it in fact is defined over G. The proof of "Moreover ..." is given as part of the argument for [ES17, Lemma 6.3] on *p. 2131 ibid.* ■

Lemma 2.2.4. [ES17, Lemma 6.4]. *Let G/H be a Galois extension of algebraic function fields of degree k. Let $\mathfrak{p}$ be a prime of H with only one, unramified, factor in G. Let $x \in H$ be such that $\mathrm{ord}_{\mathfrak{p}}\, x \not\equiv 0 \mod k$. Then x is not a norm of an element of G.* ■

Lemma 2.2.5. [ES17, Lemma 6.5]. *Let G/H be an unramified extension of local fields of degree k. Let $\mathfrak{m}$ be the prime of H. Let $x \in H$ be such that $\mathrm{ord}_{\mathfrak{m}}\, x \equiv 0 \mod k$. Then x is a norm of some element of G.* ■

Lemma 2.2.6. [ES17, Lemma 6.7]. *Let L be a function field of characteristic p possessing an l-th primitive root of unity. Let $z \in L$ and let γ be a root of the equation $X^l - z = 0$. If for some L-prime $\mathfrak{a}$, $\mathrm{ord}_{\mathfrak{a}}(z) < 0$ and $\mathrm{ord}_{\mathfrak{a}}(z) \not\equiv 0$ modulo l then $\mathfrak{a}$ is completely ramified in $L(\gamma)/L$. Also, if z is integral at $\mathfrak{a}$ and z is equivalent to a nonzero l-th power modulo $\mathfrak{a}$, then $\mathfrak{a}$ will split completely in $L(\gamma)$.* ■

Applied to the fields in question, they have the following corollary:

Corollary 2.2.7. [ES17, Corollary 6.8]. *The following statements are true about the extensions N/K, N_0/K_0:*

(1) There is no constant field extension.

(2) The factors of $\mathfrak{z}(u)$ split completely, into factors of relative inertial degree 1.

(3) Any factor $\mathfrak{q}$ of $\mathfrak{pl}(u)$ (the pole divisor of u) where $\mathrm{ord}_{\mathfrak{q}}(u) \not\equiv 0 \mod l$ ramifies completely into factors of inertial degree 1.

In particular, when $[N : K] > 1$ *(resp.* $[N_0 : K_0] > 1$*), for any prime* $\widehat{\mathfrak{q}}$ *of* N *(resp.* N_0*) over* $\mathfrak{p}\mathfrak{l}(u)$*,* $\operatorname{ord}_{\widehat{\mathfrak{q}}}(u) \equiv 0 \mod l$*.*

Proof. Recall $N = K(\delta)$ and $N_0 = K_0(\delta)$, where δ is a root of the polynomial $T^l - (u+1) = 0$. Hence (2) and (3) are direct consequences of *Lemma 2.2.6.* The "in particular" is also a direct consequence of (3).

Suppose (for the purpose of contradicting (1)) the constant field C' of $K(\delta)$ is a proper extension of C. Consider $\alpha \in C' \setminus C$; then $[C(\alpha) : C] = [K(\alpha) : K]$ (this is [Sti09, Lemma 3.6.2][3]). As $l = [K(\delta) : K(\alpha)][K(\alpha) : K]$, and l is prime, either $K(\alpha) = K$ or $K(\delta) = K(\alpha)$. The former is not permitted, as we assumed $\alpha \in C' \setminus C$, and the latter implies $K(\delta)/K$ is a constant field extension, also a contradiction. We conclude the constant field of N is that of K. This argument also holds when we replace K by K_0 and C by C_0, concluding the lemma. ■

Lemma 2.2.8. *For* $w \in K$*, the following statements are true in* $N(\beta_w)$*:*

(1) If $\widehat{\mathfrak{p}}$ *is a prime of* $N(\beta_w)$ *and* $\widehat{\mathfrak{p}} | \mathfrak{z}_b(u)$ *in* $N(\beta_w)$ *while* $\operatorname{ord}_{\widehat{\mathfrak{p}}}(w) < \frac{1-l}{l} \operatorname{ord}_{\widehat{\mathfrak{p}}}(u)$*, then* $f(\widehat{\mathfrak{p}}/\overline{\mathfrak{p}}) = f(\overline{\mathfrak{p}}/\mathfrak{p}) = 1$*, where* $\overline{\mathfrak{p}} = \widehat{\mathfrak{p}} \cap N$ *and* $\mathfrak{p} = \overline{\mathfrak{p}} \cap K$*.*

(2) If $\widehat{\mathfrak{p}}$ *is a prime of* $N(\beta_w)$ *and* $\widehat{\mathfrak{p}} | \mathfrak{z}_b(u)$ *in* $N(\beta_w)$ *while* $\operatorname{ord}_{\widehat{\mathfrak{p}}}(w) < \frac{1-l}{l} \operatorname{ord}_{\widehat{\mathfrak{p}}}(u)$*, then* $\operatorname{ord}_{\widehat{\mathfrak{p}}}(h_w) \not\equiv 0 \mod l$*.*

(3) If $\mathfrak{t}$ *is a prime of* $N(\beta_w)$ *and* $\mathfrak{t} \nmid \mathfrak{z}(u)$*, then* $\operatorname{ord}_{\mathfrak{t}}(h_w) \equiv 0 \mod l$*.*

(4) If $\mathfrak{p}$ *is a prime of* K *such that* $\mathfrak{p} | \mathfrak{z}_b(u)$ *and* $\operatorname{ord}_{\mathfrak{p}}(w) \geq \frac{1-l}{l} \operatorname{ord}_{\mathfrak{p}}(u)$*, then* $\operatorname{ord}_{\mathfrak{p}}(h_w) \equiv 0 \mod l$*.*

Proof. First, a calculation. Suppose $\mathfrak{p}$ is a prime of K such that $\mathfrak{p} | \mathfrak{z}_b(u)$. Then:

$$\begin{aligned} \operatorname{ord}_{\mathfrak{p}}(h_w) &= \operatorname{ord}_{\mathfrak{p}}(w^l u^{l-1} + 1) - l \operatorname{ord}_{\mathfrak{p}}(u) \\ &= \min\{l \operatorname{ord}_{\mathfrak{p}}(w) + (l-1) \operatorname{ord}_{\mathfrak{p}}(u), 0\} - l \operatorname{ord}_{\mathfrak{p}}(u), \end{aligned}$$

[3]Technically for the results in [Sti09, §3.6], Stichtenoth assumes the constant subfield is perfect, however this is not used in the proof of *Lemma 3.6.2 ibid.*

as $\operatorname{ord}_{\mathfrak{p}}(u) \not\equiv 0 \mod l$. If $\operatorname{ord}_{\mathfrak{p}}(w) < \frac{1-l}{l} \operatorname{ord}_{\mathfrak{p}}(u)$, then $\operatorname{ord}_{\mathfrak{p}}(w^l u^{l-1}+1) = l \operatorname{ord}_{\mathfrak{p}}(w) + (l-1)\operatorname{ord}_{\mathfrak{p}}(u)$, and $\operatorname{ord}_{\mathfrak{p}}(h_w) \not\equiv 0 \mod l$.

Now, (1) & (2). Let $\mathfrak{p} \,|\mathfrak{z}_b(u)$ in K and note by *Corollary 2.2.7*, $\mathfrak{p}$ splits completely in N into factors of inertial degree 1. For any primes $\widehat{\mathfrak{p}}|\overline{\mathfrak{p}}|\,\mathfrak{p}$ in $N(\beta_w)$ (resp. N), we have $\operatorname{ord}_{\widehat{\mathfrak{p}}}(h_w) = \operatorname{ord}_{\overline{\mathfrak{p}}}(h_w) = \operatorname{ord}_{\mathfrak{p}}(h_w)$ and $f(\widehat{\mathfrak{p}}/\overline{\mathfrak{p}}) = f(\overline{\mathfrak{p}}/\,\mathfrak{p}) = 1$, as by *Lemma 2.2.6*, $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ split completely in their extensions. We reach the desired conclusion for (2) from our initial calculation.

Part (3) is [ES17, Lemma 6.9 (3)] exactly. Part (4) is a straightforward calculation based on the first paragraph. ■

We now replicate the sufficient and necessary conditions of [ES17, Lemmas 6.11 & 6.12] for $w \in K$ to have 'small' poles at factors $\mathfrak{p}$ of $\mathfrak{z}_b(u)$, in terms of a norm equation.

Lemma 2.2.9. *If* $\operatorname{ord}_{\mathfrak{p}}(w) < \frac{1-l}{l} \operatorname{ord}_{\mathfrak{p}}(u)$ *at any factor* $\mathfrak{p} \,|\mathfrak{z}_b(u)$ *in* K*, then there is no* $x \in N(\beta_w, \alpha)$ *such that* $\operatorname{Norm}_{N(\beta_w,\alpha)/N(\beta_w)}(x) = h_w$.

Proof. Let $\widehat{\mathfrak{p}}$ be a factor of $\mathfrak{z}_b(u)$ in $N(\beta_w)$ over $\mathfrak{p}$; by *Lemma 2.2.6*, $\mathfrak{p}$ splits completely in N/K and $N(\beta_w)/N$, hence $\operatorname{ord}_{\widehat{\mathfrak{p}}}(w) = \operatorname{ord}_{\mathfrak{p}}(w) < \frac{1-l}{l} \operatorname{ord}_{\mathfrak{p}}(u) = \frac{1-l}{l} \operatorname{ord}_{\widehat{\mathfrak{p}}}(u)$. By the same reasoning as in the proof of *Corollary 2.2.7 (1)* (replacing K by N, δ by β_w, and noting the condition $\operatorname{ord}_{\mathfrak{p}}(w) < \frac{1-l}{l} \operatorname{ord}_{\mathfrak{p}}(u)$ ensures h_w is nonconstant) there is no constant field extension in $N(\beta_w)/N$. Since $f(\widehat{\mathfrak{p}}/\,\mathfrak{p}) = 1$, the equation

$$T^l - a = 0 \tag{2.2}$$

has no root in the residue field of $\widehat{\mathfrak{p}}$ in $N(\beta_w)$ if and only if (2.2) has no root in the residue field of $\mathfrak{p}$ in K. Indeed, this is the case, as by design (2.2) has no root in K (hence C), and $[Kv_{\mathfrak{p}} : C] \not\equiv 0 \mod l$. Therefore $\widehat{\mathfrak{p}}$ cannot split in the extension $N(\beta_w, \alpha)/N(\beta_w)$, as the extension is of prime degree and the residue field of $\widehat{\mathfrak{p}}$ must extend. (Note $N(\beta_w, \alpha)/N(\beta_w)$ is proper, as the constant subfields of K, N and $N(\beta_w)$ are all equal and do not contain α.) If h_w is to be a norm in this extension, then $\operatorname{ord}_{\widehat{\mathfrak{p}}}(h_w) \equiv 0 \mod l$ by *Lemma 2.2.4;* however by *Lemma 2.2.8 (2)*, we see that

$\mathrm{ord}_{\mathfrak{p}}(h_w) \not\equiv 0 \mod l$, and by the argument of *Lemma 2.2.8*, $\mathrm{ord}_{\widehat{\mathfrak{p}}}(h_w) = \mathrm{ord}_{\mathfrak{p}}(h_w)$. This is a contradiction, as desired. ■

Lemma 2.2.10. *For $w \in C_0(u)$, if $\mathrm{ord}_{\mathfrak{p}}(w) \geq \frac{1-l}{l}\,\mathrm{ord}_{\mathfrak{p}}(u)$ for all factors $\mathfrak{p}\,|\mathfrak{z}_b(u)$ in K, then there exists $x \in N(\beta_w, \alpha)$ such that $\mathrm{Norm}_{N(\beta_w,\alpha)/N(\beta_w)}(x) = h_w$.*

Proof. First, note that it is sufficient to prove there exists $x \in N_0(\beta_w, \alpha)$ such that $\mathrm{Norm}_{N_0(\beta_w,\alpha)/N_0(\beta_w)}(x) = h_w$. Indeed, $x \in N_0(\beta_w, \alpha)$ has the same $N_0(\beta_w)$-coordinates with respect to the power basis of α as in $N(\beta_w)$, hence x has the same conjugates over $N(\beta_w)$ and $N_0(\beta_w)$, hence x has the same norm.

Next we claim *the divisor of h_w is an l-th power of another divisor in $N_0(\beta_w)$*. We may assume $N_0(\beta_w)/N_0$ is a proper extension; otherwise $\frac{h_w+1}{h_w}$ is an l-th power in $N_0(\beta_w) = N_0$ and hence $\mathrm{ord}_{\mathfrak{t}}(h_w) \equiv 0 \bmod l$ for all primes $\mathfrak{t}$ of $N_0(\beta_w)$, so we immediately conclude the claim. Suppose $\mathfrak{q}$ is a prime of $N_0(\beta_w)$: we break into the following cases.

(1) If $\mathrm{ord}_{\mathfrak{q}}(u) \leq 0$, then $\mathrm{ord}_{\mathfrak{q}}(h_w) = \mathrm{ord}_{\mathfrak{q}}(w^l u^{l-1} + 1) - l\,\mathrm{ord}_{\mathfrak{q}}(u) \equiv 0 \bmod l$. Indeed, if $\mathrm{ord}_{\mathfrak{q}}(u) < 0$, then $\mathrm{ord}_{\mathfrak{q}}(u) \equiv 0 \bmod l$ by *Corollary 2.2.7*.

(2) We show there does not exist $\mathfrak{q}$ such that $\mathrm{ord}_{\mathfrak{q}}(u) > 0$ and $\mathrm{ord}_{\mathfrak{q}}(w) < 0$. Indeed, as $w \in C_0(u)$, $\mathrm{ord}_{\mathfrak{q}}(w) = e(\mathfrak{q}\,/u)\,\mathrm{ord}_u(w)$, where $e(\mathfrak{q}\,/u)$ is the ramification degree of $\mathfrak{q}$ over (the prime) (u) of $C_0(u)$. Hence $\mathrm{ord}_{\mathfrak{q}}(w) < 0$ implies $\mathrm{ord}_u(w) < 0$, which implies $\mathrm{ord}_{\widehat{\mathfrak{q}}}(w) \leq -\mathrm{ord}_{\widehat{\mathfrak{q}}}(u)$ for all $\widehat{\mathfrak{q}}|\mathfrak{z}_b(u)$ in K. As we are assuming $\mathrm{ord}_{\widehat{\mathfrak{q}}}(w) \geq \frac{1-l}{l}\,\mathrm{ord}_{\widehat{\mathfrak{q}}}(u)$, consequently

$$-(l-1)\,\mathrm{ord}_{\widehat{\mathfrak{q}}}(u) \leq l\,\mathrm{ord}_{\widehat{\mathfrak{q}}}(w) \leq -l\,\mathrm{ord}_{\widehat{\mathfrak{q}}}(u),$$

a contradiction.

(3) If $\mathrm{ord}_{\mathfrak{q}}(u) > 0$, $\mathrm{ord}_{\mathfrak{q}}(w) = 0$, then by calculation $\mathrm{ord}_{\mathfrak{q}}(h_w) \equiv 0 \mod l$.

(4) If $\mathrm{ord}_{\mathfrak{q}}(u) > 0$ and $\mathrm{ord}_{\mathfrak{q}}(w) > 0$, as $w \in C_0(u)$, $\mathrm{ord}_{\mathfrak{q}}(w) = e(\mathfrak{q}\,/u)\,\mathrm{ord}_u(w)$ forces $\mathrm{ord}_u(w) > 0$, thus $\mathrm{ord}_{\mathfrak{q}}(w) \geq \mathrm{ord}_{\mathfrak{q}}(u)$. Therefore $\mathrm{ord}_{\mathfrak{q}}(h_w) \equiv 0 \bmod l$ as required.

Observe there is a *finite* extension $\widehat{N}_0/\mathbb{F}_p(u)$ such that $w \in \widehat{N}_0$, the divisor of h_w is an l-th power of another divisor of $\widehat{N}_0$, and α is of degree l over $\widehat{N}_0$. By a similar argument as in the beginning of the lemma, it is sufficient to solve $\mathrm{Norm}_{\widehat{N}_0(\beta_w,\alpha)/\widehat{N}_0(\beta_w)}(x) = h_w$. As $\widehat{N}_0(\beta_w,\alpha)/\widehat{N}_0(\beta_w)$ is a constant field extension, it is unramified, hence by Weil [Wei74, Corollary, p. 226] *locally* every unit is a norm. Therefore by *Lemma 2.2.5* and the Strong Hasse Principle [Rei03, Theorem 32.9], h_w is a norm, as required. ■

We finish this argument with the following theorem and corollary:

Theorem 2.2.11. *Let $\alpha_j = \xi_l^j \alpha$ for $j = 0, \ldots, l-1$, and let*

$$P(X_0, \ldots, X_{l-1}) = \prod_{j=0}^{l-1} (X_0 + X_1\alpha_j + \cdots + X_{l-1}\alpha_j^{l-1}).$$

If $N(\beta_w) \models \exists a_0, \ldots, a_{l-1}(P(a_0, \ldots, a_{l-1}) = h_w)$, then $\mathrm{ord}_{\mathfrak{p}}(w) \geq \frac{1-l}{l} \mathrm{ord}_{\mathfrak{p}}(u)$ for all factors $\mathfrak{p} \,|\mathfrak{z}_b(u)$ in K. Conversely if $w \in C_0(u)$ and $\mathrm{ord}_{\mathfrak{p}}(w) \geq \frac{1-l}{l} \mathrm{ord}_{\mathfrak{p}}(u)$ for all factors $\mathfrak{p} \,|\mathfrak{z}_b(u)$ in K, then $N(\beta_w) \models \exists a_0, \ldots, a_{l-1}(P(a_0, \ldots, a_{l-1}) = h_w)$. ■

Corollary 2.2.12. *Assume ($\star$) and that there exists an l-behaved $u \in K$. There is a set $\mathrm{INT}_l(u) \subset K$ such that if $w \in \mathrm{INT}_l(u)$, then $\mathrm{ord}_{\mathfrak{p}}(w) \geq 0$ for all $\mathfrak{p} \,|\mathfrak{z}_b(u)$, and $u^n \in \mathrm{INT}_l(u)$ for all $n \in \mathbb{N}$.*

Moreover $\mathrm{INT}_l(u)$ is $\mathcal{L}_r(a)$-existentially definable with one parameter u, and the properties "$w \in \mathrm{INT}_l(u) \implies \mathrm{ord}_{\mathfrak{p}}(w) \geq 0$ for all $\mathfrak{p} \,|\mathfrak{z}_b(u)$", "$u^n \in \mathrm{INT}_l(u)$ for all $n \in \mathbb{N}$" are uniform in l-behaved u.

Proof. First we will rewrite "$P(X_0, \ldots, X_{l-1}) = h_w$" as a polynomial equation over $\mathbb{F}_p(a)[u]$ with variables in K. This can be done with *Theorem 2.0.2*, as for each $w \in K$, the extension $N(\beta_w)/K$ is finite. Explicitly, we do this in three steps:

(1) Notice the coefficients of P are in $\mathbb{F}_p(a) \subset K$, by *Lemma 2.2.3*. In addition, $[\mathbb{F}_p(a) : \mathbb{F}_p] < \infty$ by ($\star$).

(2) The extension $N(\beta_w)/N$: here we set $n_1 = 1$, $n_2 = 0$, $n_3 = l$, $t_1 = w$, $x = \beta_w$,

$g(X, t_1) = h_w X^l - (h_w + 1)$, and $f(t_1, X_0, \ldots, X_{l-1}) = P(X_0, \ldots, X_{l-1}) - h_w$. As u is by design not an l-th power in K, h_w is never zero. Therefore there exists a polynomial $q(t_1, x_1, \ldots, x_k) \in \mathbb{F}_p(a)[u][T_1, X_1, \ldots, X_k]$ such that, for $w \in K$,

$$\begin{aligned} & N(\beta_w) \models \exists a_0, \ldots, a_{l-1}(P(a_0, \ldots, a_{l-1}) = h_w) \\ \iff \quad & N \models \exists b_1, \ldots, b_k(q(w, b_1, \ldots, b_k) = 0). \end{aligned}$$

We emphasise q has coefficients in $\mathbb{F}_p(a)[u]$.

(3) The extension N/K: here we set $n = 1$, $n_2 = 0$, $n_3 = k$, $x = \delta$, $g(X, t_1) = X^l - (u+1)$, and $f(t_1, x_1, \ldots, x_k) = q(t_1, x_1, \ldots, x_k)$. Therefore $\{w \in K : N(\beta_w) \models \exists a_0, \ldots, a_{l-1}(P(a_0, \ldots, a_{l-1}) = h_w)\}$ is $\mathcal{L}_r(a)$-existentially definable in K with parameter u, as claimed.

Let $\varphi(w, u)$ be the $\exists$-$\mathcal{L}_r(a)$-formula with parameter u given by the above process; i.e. for l-behaved u, $K \models \varphi(w, u)$ implies $\operatorname{ord}_\mathfrak{p}(w) \geq \frac{1-l}{l} \operatorname{ord}_\mathfrak{p}(u)$ for all $\mathfrak{p} \,|\mathfrak{z}_b(u)$, and if $\operatorname{ord}_\mathfrak{p}(w) \geq \frac{1-l}{l} \operatorname{ord}_\mathfrak{p}(u)$ for all $\mathfrak{p} \,|\mathfrak{z}_b(u)$ and $w \in C_0(u)$, then $K \models \varphi(w, u)$.

Let $A := \{w^l u^{l-1} : K \models \varphi(w, u)\}$. Then for l-behaved u, $x \in A$ implies $\operatorname{ord}_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p} \,|\mathfrak{z}_b(u)$, and if $\frac{x}{u^{l-1}} \in (C_0(u))^l$ and $\operatorname{ord}_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p} \,|\mathfrak{z}_b(u)$, then $x \in A$. Now, define:

$$\mathrm{INT}_l(u) = \{x_1 \cdots x_l : x_1, \ldots, x_l \in A \cup \mathbb{F}_p \cup \{u\}\}.$$

For l-behaved u, if $x \in \mathrm{INT}_l(u)$ then $\operatorname{ord}_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p} \,|\mathfrak{z}_b(u)$ by design. By construction $u^n \in \mathrm{INT}_l(u)$ for all $n \in \mathbb{N}$. Finally, $\mathrm{INT}_l(u)$ is $\mathcal{L}_r(a)$-existentially definable with one parameter u, and the properties "$x \in \mathrm{INT}_l(u) \implies \operatorname{ord}_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p} \,|\mathfrak{z}_b(u)$", "$u^n \in \mathrm{INT}_l(u)$ for all $n \in \mathbb{N}$" are uniform in l-behaved u, as desired. ■

This is sufficient for Step 2.

2.3 p-behaviour

We can deduce all of §2.2 for "p-behaviour" by modifying the extensions $N(\beta_w, \alpha)/N(\beta_w)/N/K$ to be Artin-Schreier, then modifying slightly the statements of *Lemma 2.2.8 – Corollary 2.2.12* as done by Eisenträger & Shlapentokh [ES17]. Our underlying assumption is now the following instead:

Assumption ($\star'$). For some $a \in C_0$, K does not contain any root of $T^p - T - a$.

Take $u \in K$ p-behaved (recall *Definition 2.2.1*). In addition, fix the following notation for this subsection:

- Let $\delta' \in \widetilde{K}$ be a root of $T^p - T - u$.
- For $w \in K$, $h_w = \frac{w^p}{u} + \frac{1}{u^p}$ still.
- Let $\beta'_w \in \widetilde{K}$ be a root of $T^p - T - \frac{1}{h_w}$.
- Let $\alpha' \in \widetilde{K}$ be a root of $T^p - T - a$.

Once again, consider the extensions $N(\beta'_w, \alpha')/N(\beta'_w)/N = K(\delta')/K/C(u)/\mathbb{F}_p(u)$, and $N_0(\beta'_w, \alpha')/N_0(\beta'_w)/N_0 = K_0(\delta')/K_0/C_0(u)/\mathbb{F}_p(u)$. Our main tool is the following:

Lemma 2.3.1. [ES17, Lemma 6.6]. *Let L be a function field of characteristic p. Let $z \in L$ and let $\gamma \in \widetilde{L}$ be a root of the equation $X^p - X - z = 0$. If for some L-prime $\mathfrak{a}$, $\mathrm{ord}_\mathfrak{a}(z) \not\equiv 0 \mod p$ and $\mathrm{ord}_\mathfrak{a}(z) < 0$, then $\mathfrak{a}$ is completely ramified in $L(\gamma)/L$. At the same time all zeros of z will split completely in $L(\gamma)/L$, i.e. into factors of relative degree 1.* ■

Applied to the extensions in question, we recover *Corollary 2.2.7, Lemma 2.2.8* (with $l = p$), *Lemma 2.2.9* & *Lemma 2.2.10*. We deduce:

Theorem 2.3.2. *Let $\alpha_j = \alpha' + j$ for $j = 0, \ldots, p-1$. Let*

$$P(X_0, \ldots, X_{p-1}) = \prod_{j=0}^{p-1} (X_0 + X_1\alpha_j + \cdots + X_{p-1}\alpha_j^{p-1}).$$

If $N(\beta'_w) \models \exists a_0, \ldots, a_{p-1}(P(a_0, \ldots, a_{p-1}) = h_w)$*, then* $\mathrm{ord}_{\mathfrak{p}}(w) \geq \frac{1-p}{p} \mathrm{ord}_{\mathfrak{p}}(u)$ *for all factors* $\mathfrak{p} \,|\mathfrak{z}_b(u)$ *in* K*. Conversely if* $w \in C_0(u)$ *and* $\mathrm{ord}_{\mathfrak{p}}(w) \geq \frac{1-p}{p} \mathrm{ord}_{\mathfrak{p}}(u)$ *for all factors* $p|\mathfrak{z}_b(u)$ *in* K*, then* $N(\beta'_w) \models \exists a_0, \ldots, a_{p-1}(P(a_0, \ldots, a_{p-1}) = h_w)$*.*

Proof. Note that all solutions to an equation $X^p - X - a = 0$ in $\widetilde{K}$ can be written in the form $\beta + i$, $i = 0, \ldots, p-1$, where β is any solution of the equation. Also note that, assuming $\alpha' \notin N(\beta'_w)$, $\mathrm{Norm}_{N(\beta'_w, \alpha')/N(\beta'_w)}(a_0 + a_1\alpha' + \cdots + a_{p-1}\alpha'^{p-1}) = P(a_0, \ldots, a_{p-1})$ for $a_0, \ldots, a_{p-1} \in N(\beta'_w)$. The theorem follows from the aforementioned lemmas. ■

Corollary 2.3.3. *Assume* $(\star')$ *and that there exists a* p*-behaved* $u \in K$*. There is a set* $\mathrm{INT}_p(u) \subset K$ *such that if* $w \in \mathrm{INT}_p(u)$*, then* $\mathrm{ord}_{\mathfrak{p}}(w) \geq 0$ *for all* $\mathfrak{p} \,|\mathfrak{z}_b(u)$*, and* $u^n \in \mathrm{INT}_p(u)$ *for all* $n \in \mathbb{N}$*.*

Moreover $\mathrm{INT}_p(u)$ *is* $\mathcal{L}_r(a)$*-existentially definable with one parameter* u*, and "*$w \in \mathrm{INT}_p(u) \implies \mathrm{ord}_{\mathfrak{p}}(w) \geq 0$ *for all* $\mathfrak{p} \,|\mathfrak{z}_b(u)$*", "*$u^n \in \mathrm{INT}_p(u)$ *for all* $n \in \mathbb{N}$*" are uniform in* p*-behaved* u*.* ■

2.4 Assembly & Results

Before using the above machinery, we have the following lemmas on the ubiquity of l-behaviour.

Lemma 2.4.1. *Let* K *be a one variable algebraic function field of positive characteristic,* $u \in K$ *nonconstant, and* l *prime. If* $[K : C(u)] \not\equiv 0 \mod l$ *then* u *is* l*-behaved.*

Proof. Recall $\deg(\mathfrak{z}(u)) = [K : C(u)]$. Thus, we have assumed $\deg(\mathfrak{z}(u)) \not\equiv 0 \mod l$. In particular there must exist a prime $\mathfrak{p} \,|\mathfrak{z}(u)$ with $v_{\mathfrak{p}}(u) > 0$, $v_{\mathfrak{p}}(u) \not\equiv 0 \mod l$ and $[Kv_{\mathfrak{p}} : C] \not\equiv 0 \mod l$. Therefore u is l-behaved by definition, as desired. ■

Corollary 2.4.2. *For any nonconstant* $u \in K$*, there exist only finitely many primes* l *such that* u *is* not l*-behaved.* ■

Lemma 2.4.3. *Let K be the function field of a curve, of positive characteristic and not containing the algebraic closure of a finite field. There exists a finite constant extension $\breve{K}/K$ and a prime l such that:*

(1) For $\breve{K}$, either $(\star)$ is satisfied with l, or $(\star')$ is satisfied with $l = p$;

(2) There exists $u \in K$ such that, as an element of $\breve{K}$, u is l-behaved and $\mathrm{ord}_{\breve{\mathfrak{p}}}(u) = 1$ for some prime $\breve{\mathfrak{p}}|_{\mathfrak{z}b}(u)$ of $\breve{K}$.

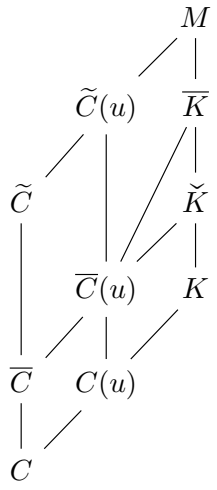
Proof. This is an application of [ES17, §6.1] exactly, which we will now outline. Recall C denotes the field of constants of K, and $C_0 = \widetilde{\mathbb{F}_p} \cap C$. By [ES17, Lemma 6.2] there exists a prime l such that either $l \neq p$ and for some $a \in C_0$, $T^l - a$ is irreducible, or $l = p$ and for some $a \in C_0$, $T^p - T - a$ is irreducible.

First assume C_0 is infinite. Let $M = K\widetilde{C}$. As the constant subfield of M is perfect (and K is a one variable function field) there exists $z \in K$ such that $M/\widetilde{C}(z)$ is a finite separable extension, and thus by the *Primitive Element Theorem*, $M = \widetilde{C}(\gamma, z)$ for some $\gamma \in M$. Note as $M/\widetilde{C}(z)$ is finite, and C_0 is infinite, we may find a change of variables $u = \frac{z-c_1}{z-c_2} \in K$ with distinct $c_1, c_2 \in C_0$, such that:

- u has only simple zeros and poles in M;
- u does not have zeros or poles at the zeros of the discriminant of the power basis of γ;
- γ is integral with respect to the zero and pole divisors of u;
- $\widetilde{C}(z) = \widetilde{C}(u)$.[4]

Let $p_\gamma(x) \in \widetilde{C}(z)[x]$ be the monic irreducible polynomial of γ. Let $\Gamma \subset \widetilde{C}$ be the finite set so that $p_\gamma(x)$ is a polynomial over $\Gamma \cup \{z\}$. Let $\Delta \subset \widetilde{C}$ be the finite set of roots of $p_\gamma(x) \bmod \mathfrak{z}(u)$ and $p_\gamma(x) \bmod \mathfrak{pl}(u)$. Define $\overline{K} = K(\gamma, \Gamma, \Delta, \mu_l)$, where $\mu_l \in \widetilde{\mathbb{F}_p}$ is a primitive l-th root of unity (if $l \neq p$). Denote the constant subfield of $\overline{K}$ by $\overline{C}$ (this is a finite extension of C), and define $\breve{K} = K\overline{C}$. We will consider the tower of fields:

[4] This is an immediate consequence of $u = \frac{z-c_1}{z-c_2}$.



By construction, $p_\gamma(x) \in \overline{C}(z)[x] = \overline{C}(u)[x]$, and $\overline{K}/\overline{C}(u)$ remains separable. By the second and third bullet points, and [Ros02, Proposition 8.5], $\mathfrak{z}(u)$ and $\mathfrak{pl}(u)$ do not ramify in this extension. By [Lan94, Chapter 1, §8, Proposition 25], $\mathfrak{z}(u)$ and $\mathfrak{pl}(u)$ split into factors of relative degree 1 in $\overline{K}/\overline{C}(u)$, hence the factors of $\mathfrak{z}(u)$ and $\mathfrak{pl}(u)$ in $\overline{K}$ are of inertial and ramification degree 1.

Consequently, as the constant subfield of $\breve{K}$ is $\overline{C}$, $\breve{K}/\overline{C}(u)$ is separable and $\mathfrak{z}(u)$ and $\mathfrak{pl}(u)$ split into factors of inertial and ramification degree 1. Hence, as an element of $\breve{K}$, u is r-behaved for *any* prime r. As $\overline{C}/C$ is a finite extension, by [ES17, Lemma 6.2] $\breve{K}$ satisfies the conditions of the theorem.

Now assume C_0 is finite. Fix a nonarchimedian prime $\mathfrak{q}$ of K; as $\mathcal{O}_\mathfrak{q}$ is a discrete valuation ring, there exists $u \in K$ nonconstant with $\mathrm{ord}_\mathfrak{q}(u) = 1$, and $K/C(u)$ finite. Choose any prime $l \neq p$ sufficiently large such that $[Kv_\mathfrak{q} : C] < l$; then u is l-behaved in K and $\mathfrak{q} \,|\mathfrak{z}_b(u)$. Let $\breve{K} = K(\mu_l)$ with field of constants $\overline{C}$. By construction, $\mathfrak{z}(u)$ and $\mathfrak{pl}(u)$ do not ramify, and if $\breve{\mathfrak{q}}|\mathfrak{q}$, then $[\breve{K}v_{\breve{\mathfrak{q}}} : \overline{C}] \leq [Kv_\mathfrak{q} : C] < l$, hence u is l-behaved as an element of $\breve{K}$. Writing $\overline{C}_0 = \widetilde{\mathbb{F}_p} \cap \overline{C}$, as $\overline{C}_0/C_0$ is finite, $\overline{C}_0$ is finite, hence $(\star)$ is satisfied with l. This concludes the lemma. ■

Remark 2.4.4. Note the construction of $\breve{K}$ does not depend on any element of K; if $\breve{K}$ is taken as preexisting and fixed, *Lemma 2.4.3* proves that subsequently $\breve{K}$ has l-behaved elements. □

Define the unary predicate B_l by $K \models B_l(u) \iff u$ is l-behaved in K.

Theorem 2.4.5. *Let K be the function field of a curve, of characteristic $p > 2$ and not containing $\widetilde{\mathbb{F}_p}$. There exists a finite constant extension $\check{K}/K$ such that for some prime l and $a \in \check{K} \cap \widetilde{\mathbb{F}_p}$, $\mathtt{Th}_{\forall^1\exists^+}(\check{K}; \mathcal{L}_F(a) \cup \{\neg B_l\})$ is undecidable.*

Proof. We may assume WLOG K satisfies the conditions on $\check{K}$ of *Lemma 2.4.3*. If $K \models B_l(u)$, by *Corollary 2.2.12/2.3.3* the set $\mathrm{INT}_l(u)$ has an explicit positive-existential $\mathcal{L}_r(a)$-definition: denote by $\Gamma(u, w)$ this $\mathcal{L}_r(a)$-formula. By *Corollary 2.1.3*, we can give a parameter-free existential $\mathcal{L}_F$-definition of the Den_p predicate. Following [ES17, §2] and using our above machinery, we can then recursively translate members of $\mathrm{Form}_{\exists^+}(\{0, 1, +, |_p, \leq\})$ to members of $\mathrm{Form}_{\exists}(\mathcal{L}_F(a))$.

Let $\mathcal{L}_{Ph}$ denote the language $\{0, 1, +, |_p, \leq\}$. Reserve variables x_i for $\mathcal{L}_{Ph}$ and variables y_i for $\mathcal{L}_F(a)$. For each unnested[5] atomic $\mathcal{L}_{Ph}$-formula ϕ, associate an $\exists$-$\mathcal{L}_F(a)$-formula ϕ' as follows:

- $x_i = x_j \longmapsto$ the formula $\gamma_=(u, y_i, y_j) := \Gamma(u, \frac{y_i}{y_j}) \wedge \Gamma(u, \frac{y_j}{y_i})$;
- $x_i = \underbrace{1 + \cdots + 1}_{n \text{ times}} \longmapsto \gamma_=(u, y_i, \underbrace{u \cdots u}_{n \text{ times}})$;
- $x_i + x_j = x_k \longmapsto \gamma_=(u, y_i y_j, y_k)$;
- $x_i \leq x_j \longmapsto \Gamma(u, \frac{y_j}{y_i})$;
- $x_i |_p x_j \longmapsto \exists z(\gamma_=(u, y_i, z) \wedge \mathrm{Den}_p(z, y_j))$.

This can be extended to atomic $\mathcal{L}_{Ph}$-formulae, then arbitrary positive-existential $\mathcal{L}_{Ph}$-formulae, by adding the rules

- $\bigwedge_i \phi_i \longmapsto \bigwedge_i \phi_i'; \qquad \bigvee_i \phi_i \longmapsto \bigvee_i \phi_i'$;
- $\exists x_{i_1}, \ldots, x_{i_n}\, \phi(x_{i_1}, \ldots, x_{i_n}) \longmapsto \exists y_{i_1}, \ldots, y_{i_n}\, (\bigwedge_j \Gamma(u, y_{i_j}) \wedge \phi'(y_{i_1}, \ldots, y_{i_n}))$.

One can confirm on sentences this is a recursive map $\mathrm{Sent}_{\exists^+}(\mathcal{L}_{Ph}) \to \mathrm{Form}^1_{\exists}(\mathcal{L}_F(a))$. We claim for $\varphi \in \mathrm{Sent}_{\exists^+}(\mathcal{L}_{Ph})$:

[5] Recall *Definition A.1* and [Hod93, Theorem 2.6.1]: every atomic $\mathcal{L}_{Ph}$-formula is logically equivalent to an existentially quantified conjunction of positive unnested atomic $\mathcal{L}_{Ph}$-formulae.

$$(\mathbb{N};\mathcal{L}_{Ph}) \models \varphi \iff (K;\mathcal{L}_F(a)\cup\{\neg B_l\}) \models \forall u(B_l(u)\to\varphi'(u)). \tag{2.3}$$

Assume $K \models \forall u(B_l(u)\to\varphi'(u))$. By *Lemma 2.4.3* there exists an l-behaved $\breve{u}\in K$ with $\mathrm{ord}_{\mathfrak{p}}(\breve{u})=1$ for some nonarchimedian prime $\mathfrak{p}\,|\mathfrak{z}_b(\breve{u})$. With this parameter, $\mathbb{N}$ (as an $\mathcal{L}_{Ph}$-structure) is interpretable in K, in the sense of *Definition A.2:* indeed, setting $\delta(x)=\Gamma(\breve{u},x)$ and $f:\delta(K)\to\mathbb{N}$; $w\mapsto \mathrm{ord}_{\mathfrak{p}}(w)$, *Definition A.2* is satisfied. Hence as $K\models\varphi'(\breve{u})$, $\mathbb{N}\models\varphi$.

The argument for the forward implication requires the $\mathcal{L}_{Ph}$-embedding $\mathbb{N}\to\mathbb{N}$ given by $1\mapsto n$ for any fixed $n\geq 1$: for any positive-existential $\mathcal{L}_{Ph}$-sentence φ, written $\varphi(1)$, we have $\mathbb{N}\models\varphi(1)\to\forall n(n\neq 0\to\varphi(n))$. Consequently, if $K\models\exists u(B_l(u)\wedge\neg\varphi'(u))$ has a witness $\breve{u}$, then $K\models(\neg\varphi)'(\breve{u})$ for $\breve{u}\in K$ l-behaved, and setting $\breve{n}=\mathrm{ord}_{\mathfrak{p}}(\breve{u})$ for some $\mathfrak{p}\,|\mathfrak{z}_b(\breve{u})$ gives $\mathbb{N}\models\neg\varphi(\breve{n})$, a contradiction. Therefore (2.3) is satisfied; we conclude the desired undecidability result from *Theorem 2.0.1.* ■

One would hope to conclude the undecidability of $\mathtt{Th}_{\exists}(K;\mathcal{L}_F\cup\{B_l\})$ – possibly allowing an expansion of the language by constant symbols – by this method (by which we mean forming a recursive map $\mathrm{Sent}_{\exists^+}(\mathcal{L}_{Ph})\to\mathrm{Sent}_{\exists}(\mathcal{L}_F\cup\{B_l\})$ where elements of $\mathbb{N}$ are in some way associated to elements of K integral at a prime $\mathfrak{p}$, using only l-behaved parameters) however this is not possible. Indeed, without additional restrictions on u, one may only try to form an interpretation of $\mathbb{N}$ as an $\{0,+,|_p,\leq\}$-structure in K by this method. For example, if $K=\mathbb{F}_p(t)$, p odd, $l=2$, then the Frobenius map given by $x\mapsto x^p$ is a $\mathcal{L}_F\cup\{B_2\}$-embedding $\mathbb{F}_p(t)\hookrightarrow\mathbb{F}_p(t)$, and $\mathrm{ord}_{\mathfrak{p}}(x)\neq\mathrm{ord}_{\mathfrak{p}}(x^p)$ for $x\in\mathbb{F}_p(t)$ with $\mathrm{ord}_{\mathfrak{p}}(x)>0$. Therefore, in general *arithmetic is not interpretable along these lines*, as the constant "1" would be definable in $\mathbb{N}$ using multiplication.

Note that although the question of the undecidability of $\mathtt{Th}_{\exists}(K;\mathcal{L}_F\cup\{B_l\})$ can be reduced to that of $\mathtt{Th}_{\exists^+}(\mathbb{N};0,+,|_p,\leq)$, this theory is *decidable* by an unpublished result of K. Kartas, communicated to the author by E. Hrushovski.

While existential undecidability results in the language $\mathcal{L}_F\cup\{B_l\}$ seem for the moment out of reach, we are able to refine and extend *Theorem 2.4.5* using an algebraic

characterisation of *l-misbehaviour*. Consider the following classical result by Leahey:

Theorem 2.4.6. [Lea67, Theorem, p. 817]. *Let F be a finite field of order p^n where p is a prime, $p \equiv 3 \mod 4$, and n is odd. Let $f \in F[X]$ and suppose that $f = a \cdot f_1^{e_1} \cdots f_r^{e_r}$ with $a \in F$, and $f_i \in F[X]$ is the factorisation of f into an element of F and monic irreducible polynomials in $F[X]$.*

Then f can be written as the sum of two squares in $F[X]$ if and only if e_i is even for those f_i with odd degree. ■

We can adapt the proof of this for the following use: let K be the function field of a curve, with constant subfield C an algebraic extension of $\mathbb{F}_p$, where $p > 2$. We retain the assumption that $\widetilde{\mathbb{F}_p} \not\subseteq C$, and note in this case $C = C_0$.

Corollary 2.4.7. *Assume K satisfies either $(\star)$ with l prime such that $T^l - a$ is irreducible for some $a \in C$, or $(\star')$ and fix $a \in C$ such that $T^p - T - a$ is irreducible. Denote by $\alpha \in \widetilde{\mathbb{F}_p} \setminus C$ a root of the former (resp. the latter) polynomial.*

Then $u \in K$ is not a norm of $K(\alpha)/K$ if and only if u or $\frac{1}{u}$ is l-behaved, if and only if $\frac{u}{u^2+b}$ is l-behaved for all $b \in C^*$.

Proof. Suppose u is l-behaved; it has a prime factor $\mathfrak{p} \,|\mathfrak{z}(u)$ of inertial degree & ramification index in u both coprime to l. In the extension $K(\alpha)/K$, $\mathfrak{p}$ does not ramify [Ros02, Proposition 8.5], and by assumption $[Kv_\mathfrak{p} : C]$ is coprime to l, hence the equation $X^l - a = 0$ (resp. $X^p - X - a = 0$) has no root in $Kv_\mathfrak{p}$. Thus $\mathfrak{p}$ is inert in $K(\alpha)$, as $[K(\alpha) : K]$ is prime and the residue field of $\mathfrak{p}$ must extend. By *Lemma 2.2.4*, as $\mathrm{ord}_\mathfrak{p}(u)$ is coprime to l, u is not a norm in $K(\alpha)/K$.

If $\frac{1}{u}$ is l-behaved, then we conclude by the same argument that $\frac{1}{u}$ is not a norm in $K(\alpha)/K$. By the multiplicative property of norms, this forces u not to be a norm of $K(\alpha)/K$, as desired.

Conversely, suppose that u and $\frac{1}{u}$ are not l-behaved. For all primes $\mathfrak{p} \,|\mathfrak{z}(u) \cdot \mathfrak{pl}(u)$, either $\mathrm{ord}_\mathfrak{p}(u) \equiv 0 \mod l$, or $[Kv_\mathfrak{p} : C] \equiv 0 \mod l$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the primes falling into the latter category; they split completely in $K(\alpha)/K$ by [Ros02, Proposition 8.11].

Let $\{\widehat{\mathfrak{p}}_{1,j},\dots,\widehat{\mathfrak{p}}_{l,j}\}$ be the primes of $K(\alpha)$ over $\mathfrak{p}_j$ for $1\leq j\leq n$: locally, as

$$l=[K(\alpha):K]=\sum_{\mathfrak{q}\,|\,\mathfrak{p}_j}[K(\alpha)_{\mathfrak{q}}:K_{\mathfrak{p}_j}]=[K(\alpha)_{\widehat{\mathfrak{p}}_{1,j}}:K_{\mathfrak{p}_j}]+\cdots+[K(\alpha)_{\widehat{\mathfrak{p}}_{l,j}}:K_{\mathfrak{p}_j}],$$

this forces $K(\alpha)_{\widehat{\mathfrak{p}}_{i,j}}=K_{\mathfrak{p}_j}$ for $1\leq i\leq l$. Therefore for each $1\leq i\leq l$, $1\leq j\leq n$, u is trivially a norm of $K(\alpha)_{\widehat{\mathfrak{p}}_{i,j}}/K_{\mathfrak{p}_j}$. Let $K'/\mathbb{F}_p(u)$ be a finite extension (recall $K/C(u)$ is finite, where $C/\mathbb{F}_p$ is algebraic) such that

- $a\in K'$, $[K'(\alpha):K']=l$, $K'\subset K$;
- For all primes $\mathfrak{p}\,|\mathfrak{z}(u)\cdot\mathfrak{pl}(u)$ of K', either $\mathrm{ord}_{\mathfrak{p}}(u)\equiv 0 \bmod l$, or
- (Denoting the constant field of K' by C') $[K'v_{\mathfrak{p}}:C']\equiv 0 \bmod l$ and $\mathfrak{p}$ splits completely in the extension $K'(\alpha)/K'$.

Again, this third point forces u to trivially be a norm of $K'(\alpha)_{\widehat{\mathfrak{p}}_i}/K'_{\mathfrak{p}}$ for such $\mathfrak{p}$, where $\{\widehat{\mathfrak{p}}_1,\dots,\widehat{\mathfrak{p}}_l\}$ are the primes of $K'(\alpha)$ over $\mathfrak{p}$.

The extension $K'(\alpha)/K'$ is an unramified extension of global fields, hence by Weil [Wei74, Corollary, p. 226] locally every unit is a norm. Therefore, by *Lemma 2.2.5*, the paragraph immediately above, and the Strong Hasse Principle [Rei03, Theorem 32.9], u is a norm of $K'(\alpha)/K'$. By the same argument in the first paragraph of *Lemma 2.2.10*, u is a norm of $K(\alpha)/K$, as desired. The final equivalence is a consequence of the fact $\mathfrak{z}(\frac{u}{u^2+b})=\mathfrak{z}(u)\cdot\mathfrak{pl}(u)$ for all $b\in C^*$. ■

Corollary 2.4.8. *Let K be the function field of a curve, of odd characteristic p and constant subfield $C\subsetneq\widetilde{\mathbb{F}_p}$. There exists $d\in C$ such that $\mathtt{Th}_{\forall^1\exists}(K;\mathcal{L}_F(d))$ is undecidable.*

Proof. Let $\breve{K}$ be the finite extension of K constructed in *Lemma 2.4.3* (cf. *Remark 2.4.4*), and $-':\mathrm{Sent}_{\exists^+}(\mathcal{L}_{Ph})\to\mathrm{Form}^1_{\exists}(\mathcal{L}_F(a))$ the recursive map from pp. 32–33. Consider the expansion of the $\mathcal{L}_F(a)$-structure $\breve{K}$ to the language $\mathcal{L}_F(a)\cup\{K\}$, where (abusing notation) K is a unary predicate interpreted in $\breve{K}$ as the subfield K. Following

Theorem 2.4.5, we will confirm (for $\varphi \in \mathrm{Sent}_{\exists^+}(\mathcal{L}_{Ph})$)

$$\begin{aligned} & (\breve{K}; \mathcal{L}_F(a) \cup \{\neg B_l\}) \models \forall u (B_l(u) \to \varphi'(u)) \\ \iff \quad & (\breve{K}; \mathcal{L}_F(a) \cup \{K\}) \models \forall u \in K,\, \Omega_\varphi(u) \end{aligned} \tag{2.4}$$

where $\Omega_\varphi(v)$ is an existential $\mathcal{L}_F(a)$-formula in one free variable, defining the set of elements $v \in \breve{K}$ such that

$$\exists x \in \breve{K}(\alpha)\ \mathrm{Norm}_{\breve{K}(\alpha)/\breve{K}}(x) = v \qquad \text{or} \qquad \breve{K} \models \varphi'(\tfrac{v}{v^2+1}). \tag{2.5}$$

We begin by verifying:

Claim. (2.5) is $\exists$-$\mathcal{L}_F(a)$-expressible in $\breve{K}$.

Proof. Recall α satisfies $X^l - a = 0$, where $a \in \widetilde{\mathbb{F}_p}$. Let $P(X_0, \dots, X_{l-1}) \in \mathbb{F}_p(a)[X_0, \dots, X_{l-1}]$ be the polynomial of *Lemma 2.2.3* such that for $a_0, \dots a_{l-1} \in \breve{K}$, $P(a_0, \dots, a_{l-1}) = \mathrm{Norm}_{\breve{K}(\alpha)/\breve{K}}(a_0 + a_1\alpha + \cdots + a_{l-1}\alpha^{l-1})$. Then:

$$\exists x \in \breve{K}(\alpha)\ \mathrm{Norm}_{\breve{K}(\alpha)/\breve{K}}(x) = v \iff \exists a_0, \dots, a_{l-1} \in \breve{K} \text{ s.t. } P(a_0, \dots, a_{l-1}) = v,$$

hence the norm condition of (2.5) is expressible as an $\exists$-$\mathcal{L}_r(a)$-formula $\varpi(v)$ in one variable over $\breve{K}$, as required. ♦

Claim. Equivalence (2.4) holds.

Proof. The forward implication is straightforward: $\varphi'(u)$ is in particular satisfied by l-behaved elements of the form $\frac{u}{u^2+1} \in K$. From *Corollary 2.4.7*, we conclude the desired result. For the reverse implication, by *Lemma 2.4.3* there exists $u \in K$ such that, as an element of $\breve{K}$, u is l-behaved and $\mathrm{ord}_{\breve{\mathfrak{p}}}(u) = 1$ for some prime $\breve{\mathfrak{p}} | \mathfrak{z}_b(u)$ (and hence it cannot be a norm of $\breve{K}(\alpha)/\breve{K}$ by *Corollary 2.4.7*). So $\breve{K} \models \varphi'(\frac{u}{u^2+1})$ where $\mathrm{ord}_{\breve{\mathfrak{p}}}(\frac{u}{u^2+1}) = 1$ still. With this parameter, $\mathbb{N}$ (as an $\mathcal{L}_{Ph}$-structure) is interpretable in $\breve{K}$, in the sense of *Definition A.2:* this is p. 33. Thus $\mathbb{N} \models \varphi$ and $\breve{K} \models \forall u (B_l(u) \to \varphi'(u))$ by (2.3). ♦

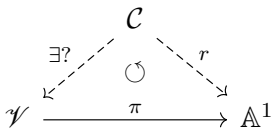
Finally, let us show there is an element $d \in C$ such that $\mathtt{Th}_{\forall^1\exists}(K; \mathcal{L}_F(d))$ is undecidable. We note that, from *Lemma 2.4.3*, $\breve{K} = K(b)$ has constant subfield $C(b)$; a finite simple extension of C where $b \in \widetilde{\mathbb{F}_p}$ (this follows from the *Primitive Element Theorem*, as C is perfect). As $a \in \breve{K} \cap \widetilde{\mathbb{F}_p} = C(b)$, there exists a finite extension $\mathbb{F}_p(d)/\mathbb{F}_p$ such that $\mathbb{F}_p(d) \subseteq C$ and $a \in \mathbb{F}_p(d, b)$. Apply *Lemma 2.0.5* with $\mathbb{F}_q = \mathbb{F}_p(d)$ (one may write the $\exists$-$\mathcal{L}_F(a)$-formula $\Omega_\varphi(u)$ as a disjunction of formulae of the form (2.1)). Thus there exists an $\exists$-$\mathcal{L}_F(d)$-formula $\Omega^\varphi(u)$ such that

$$K(b) \models \forall u \in K,\, \Omega_\varphi(u) \quad \iff \quad K \models \forall u\, \Omega^\varphi(u). \tag{2.6}$$

From the equivalences of (2.6) & (2.4), the undecidability of $\mathtt{Th}_{\forall^1\exists}(K; \mathcal{L}_F(d))$ follows from *Theorem 2.0.1*, as in *Theorem 2.4.5*. ■

Remark 2.4.9. This is not an unexpected result: by the work of Anscombe & Fehm [AF16] it is known $\mathtt{Th}_{\forall^1\exists}(\mathbb{F}_q(t))$ in the language of rings without additional constants is undecidable (cf. [AF16, Remark 7.9] where a similar argument *not* using the valuation may be used; undecidability follows from Pheidas & Videla [Phe91, Vid94]). □

Corollary 2.4.10. *Let $\mathcal{C}$ be an absolutely irreducible curve defined over a finite field $\mathbb{F}_q$ of odd characteristic. No algorithm exists which, upon input an $\mathbb{F}_q$-morphism $\pi : \mathscr{V} \to \mathbb{A}^1$ of affine $\mathbb{F}_q$-varieties, outputs "YES" if for all nonconstant $\mathbb{F}_q$-rational maps $r : \mathcal{C} \dashrightarrow \mathbb{A}^1$ there exists an $\mathbb{F}_q$-rational map $\mathcal{C} \dashrightarrow \mathscr{V}$ making the below diagram commute, and "NO" otherwise.*



Proof. This is rewriting *Corollary 2.4.8*, assuming C is finite, à la [Koe16a, Corollary 3′] & [Poo09, §1.2]. ■

2.5 Other Properties of l-behaviour

Here we remark that for some function fields it is possible to existentially $\mathcal{L}_F$-define a *nontrivial* (that is, nonempty and contains nonconstant elements) subset of l-behaved elements, for some primes l.

First, we note there is a strong connection (though not an equivalence) between l-behaved elements of a function field, and non-l-th powers of that function field, and that for some function fields of curves it is possible to $\mathcal{L}_F$-$\emptyset$-existentially define a nontrivial (in the above sense) subset of the non-l-th powers for some primes l.

Theorem 2.5.1. *Let $p > 3$. A nontrivial (in the above sense) subset of $\mathbb{F}_q(t) \setminus (\mathbb{F}_q(t))^2$ is existentially $\mathcal{L}_F$-$\emptyset$-definable.*

Proof. Fix $\alpha \in \mathbb{F}_p^*$. Consider the curve $\mathcal{E} : y^2 = x^3 + \alpha$; this is a smooth curve of genus 1, defined over $\mathbb{F}_p$. This curve cannot have nonconstant $\mathbb{F}_q(t)$-points as a consequence of the Hurwitz genus formula [Sti09, Corollary 3.5.6]; this proves the set $\{u : F(u) \wedge \exists x\,(u = x^3 + \alpha)\}$ is a subset of $\mathbb{F}_q(t) \setminus (\mathbb{F}_q(t))^2$, as desired. ■

Lemma 2.5.2. *Let K be a function field of positive characteristic and l, r distinct primes. Then $u \in K$ is l-behaved if and only if u^r is l-behaved.*

Proof. Let C denote the field of constants of K. $u \in K$ is l-behaved if and only if there exists a prime $\mathfrak{p} \,|_{\mathfrak{z}}(u)$ of K such that $v_{\mathfrak{p}}(u) \not\equiv 0 \bmod l$ and $[Kv_{\mathfrak{p}} : C] \not\equiv 0 \bmod l$, if and only if (as $v_{\mathfrak{p}}(u^r) = r \cdot v_{\mathfrak{p}}(u)$) there exists a prime $\mathfrak{p} \,|_{\mathfrak{z}}(u^r)$ of K such that $v_{\mathfrak{p}}(u^r) \not\equiv 0 \bmod l$ and $[Kv_{\mathfrak{p}} : C] \not\equiv 0 \bmod l$, if and only if u^r is l-behaved, as required. ■

Remark 2.5.3. Along a similar vein, if $\sigma : K \to L$ is an isomorphism of function fields, notice that $u \in K$ is l-behaved if and only if $\sigma(u) \in L$ is l-behaved. Indeed, this follows from three facts: first, if $\mathfrak{p}$ is a prime of K, then there is a corresponding (discrete) valuation ring $\mathcal{O}_{\mathfrak{p}}$ with maximal ideal $\mathfrak{p}$. Under the isomorphism, $\sigma(\mathcal{O}_{\mathfrak{p}})$ is a (discrete) valuation ring with maximal ideal $\sigma(\mathfrak{p})$, hence corresponds to a prime

of L (denoted "$\sigma(\mathfrak{p})$"). Second, for all $a \in K$, $\mathrm{ord}_{\sigma(\mathfrak{p})}(\sigma(a)) = \mathrm{ord}_{\mathfrak{p}}(a)$. Finally, $Kv_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p} \cong \sigma(\mathcal{O}_{\mathfrak{p}})/\sigma(\mathfrak{p}) = Lv_{\sigma(\mathfrak{p})}$. Together these facts bring us to the desired conclusion. □

Finally, the following theorem is due to a suggestion of E. Hrushovski.

Theorem 2.5.4. *Let k be a field algebraic over $\mathbb{F}_p$, $p > 2$, not algebraically closed, and $\mathcal{C}$ a smooth, geometrically irreducible, projective curve over k of genus at least 2. There exists a prime l such that a nontrivial (in the above sense) subset of l-behaved elements is existentially $\mathcal{L}_F$-definable in $k(\mathcal{C})$ (with one parameter $a \in k \subset \widetilde{\mathbb{F}_p}$).*

Proof. We may write $k(\mathcal{C})$ as the fraction field of $k[X_1, X_2]/(P)$, where $P \in k[X_1, X_2]$ and $\mathcal{C}$ is given by the projectivisation of $P = 0$. Fix elements $x_1 = X_1 + (P)$, $x_2 = X_2 + (P) \in k(\mathcal{C})$; any nonconstant solution $y_1, y_2 \in k(\mathcal{C})$ of $P = 0$ gives rise to an injective map $k(\mathcal{C}) \to k(\mathcal{C})$ through $x_1 \mapsto y_1,\ x_2 \mapsto y_2$, which corresponds uniquely to a nonconstant endomorphism $\mathcal{C} \to \mathcal{C}$ by [Sil09, II.2, Theorem 2.4]. By the Riemann-Hurwitz formula [Sil09, II.5, Theorem 5.9], any nonconstant *separable* endomorphism of $\mathcal{C}$ is an isomorphism (any such $f : \mathcal{C} \to \mathcal{C}$ necessarily has degree 1, and hence is an isomorphism by [Sil09, II.2, Corollary 2.4.1]). Therefore by the decomposition of [Sil09, II.2, Corollory 2.12], any nonconstant solution of $P = 0$ in $k(\mathcal{C})$ is of the form $(g(x_1)^{p^r}, g(x_2)^{p^r})$ where $r \geq 0$ and $g \in \mathrm{Aut}(k(\mathcal{C}))$.

Let $l > p$ be a prime sufficiently large such that x_1 is l-behaved in $k(\mathcal{C})$ (which exists by *Corollary 2.4.2*). As x_1 is l-behaved, so is $g(x_1)^{p^r}$ by *Lemma 2.5.2 & Remark 2.5.3*. Therefore the first component (say) of every nonconstant solution of P in $k(\mathcal{C})$ is l-behaved for this l. There exists $a \in \widetilde{\mathbb{F}_p}$ such that $P(X_1, X_2) \in \mathbb{F}_p(a)[X_1, X_2]$; the formula $\vartheta(x) = \exists v(F(x) \wedge F(v) \wedge P(x, v) = 0)$ existentially $\mathcal{L}_F(a)$-defines a nontrivial subset of l-behaved elements in $k(\mathcal{C})$, as desired. ■

Chapter 3

Finite Undecidability I: Closedness

In the previous chapter, we were interested in determining the decidability of a certain set of first-order sentences with a geometric motivation – specifically we considered existential or $\forall^1\exists$-$\mathcal{L}_F$-sentences corresponding to the diagram solvability of certain embedding problems (viz. *Corollary 2.4.10*). Instead of focusing on a specific field, and specific sentences about its geometry, what if we instead asked about *the decidability of the consequences of a given first-order statement?* Very loosely: given a first-order $\mathcal{L}_r$-sentence φ, (that – for example – captures some behaviour of a field's absolute Galois group, or a field's arithmetic) does there exist an algorithm which, upon input $\psi \in \mathrm{Sent}(\mathcal{L}_r)$, always determines correctly when $\varphi \vdash \psi$? This is the sort of question we will consider in *Chapters 3 & 4*. We will assume the reader is familiar with *Appendix A*.

3.1 First Exploration by Ziegler

Ziegler's main result of [Zie82] is the construction of a field K_q satisfying the following theorem:

Theorem 3.1.1. [Zie82, Theorem, p. 270]. *Let L be the field $\mathbb{C}$, $\widetilde{\mathbb{F}_p(t)}$, $\mathbb{R}$, or $\mathbb{Q}_p$, and $q \neq p$ prime, and A a countable structure. There exists a field $K_q \subset L$ such that*

(1) A is interpretable (with parameters) in K_q;

(2) If the intermediate field $K_q \subset H \subset L$ is finite over K_q, either $[H : K_q] = 1$ or $q|[H : K_q]$. ■

Remark 3.1.2. More precisely, Ziegler's construction ensures $\mathbb{Z}$ is definable when $L = \mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}_p$. When $L = \widetilde{\mathbb{F}_p(t,z)}$, where t, z are transcendental and algebraically independent over $\mathbb{F}_p$, a gentle modification of this method allows one to construct $K_q \subset L$ such that $\mathbb{F}_p[t]$ is definable in K_q, and $q|[H : K_q]$ for all proper finite extensions $K_q \subset H \subset L$. (This Shlapentokh & Videla do as part of a greater generalisation in [SV14]; cf. *Theorems 3.3 & 4.1 ibid.*) □

Recall from *Definition 1.2.4* the terminology "finitely undecidable", and that a "finite subtheory" of an $\mathcal{L}$-theory T is a nonempty finitely axiomatised subtheory of T.

Corollary 3.1.3. Let p be prime. $\mathtt{ACF}_0$, $\mathtt{ACF}_p$, $\mathtt{RCF}$, *and* $p\mathtt{CF}$ *are finitely undecidable.*

Proof. [Zie82, Corollary, p. 270]; we present the proof fully for exposition. Fix $L = \mathbb{C}, \mathbb{R}, \mathbb{Q}_p$ or $\widetilde{\mathbb{F}_p(t,z)}$, and let T be a finite subtheory of $\mathtt{Th}(L; \mathcal{L}_r)$. Let P be the set of primes distinct to p. For each $q \in P$, use *Theorem 3.1.1* (*resp. Remark 3.1.2*) to obtain a field $K_q \subset L$ such that $\mathbb{Z}$ (resp. $\mathbb{F}_p[t]$) is definable in K_q, and $q|[H : K_q]$ for all proper finite extensions $K_q \subset H \subset L$. Let $\mathcal{U}$ be a nonprincipal ultrafilter on P, and let $\mathbb{K}$ be the ultraproduct $\prod_{q \in P} K_q/\mathcal{U}$.

We claim that $\mathbb{K}$ is relatively algebraically closed in $L^{\mathcal{U}}$. Indeed, suppose $f = (f_q) \in \mathbb{K}[X]$ has a root $\alpha = (\alpha_q) \in L^{\mathcal{U}}$. In which case, $\{q : f_q(\alpha_q) = 0\} \in \mathcal{U}$, hence $\{q : [K_q(\alpha_q) : K_q] \leq \deg(f)\} \in \mathcal{U}$. Consequently, as $q|[H : K_q]$ for all proper finite extensions $K_q \subset H \subset L$, $\{q : [K_q(\alpha_q) : K_q] = 1\} \in \mathcal{U}$. Hence $\alpha \in \mathbb{K}$ as desired.

By the model theory of algebraically/real closed/p-adically closed fields[1], we deduce $\mathbb{K} \equiv L^{\mathcal{U}}$ ($\equiv L$ by *Łoś' Theorem*; specifically [CK12, Theorem 4.1.9]). Therefore $\mathbb{K} \models T$. As T is finitely axiomatised, by *Łoś' Theorem* there must exist some $q \in P$ such that

[1] See [Mar02, §3.2 & 3.3] as a reference for the former two, and [PR84, §5] for the latter.

$K_q \models T$. Thus by *Remark 3.1.2 & Corollary A.10*, $\mathtt{Th}(K_q; \mathcal{L}_r)$ is hereditarily undecidable, making T undecidable as required. ■

One can see the key step in this corollary was using the following property inherent to the considered fields L:

$$K \text{ relatively algebraically closed in } L \implies K \equiv L. \tag{♭}$$

In §3.2 we will outline Ziegler's construction of the field K_q, with a minor discrepancy for L a separably closed field. In §3.3 we outline Ziegler's construction in the case $L = \mathbb{Q}_p$ but again with changes so his method works for any equicharacteristic 0 henselian valued field. Later in the chapter we will discuss extending this construction to more difficult cases that avoid property (♭).

3.2 Separably Closed Fields

To save referring the reader to another text, we will outline Ziegler's construction in this subsection. To make this a more interesting exercise we shall prove *the theory of any separably closed field is finitely undecidable*; not considered by Ziegler in [Zie82].

Let $\mathtt{SCF}$ denote the theory of separably closed fields, $\mathtt{SCF}_p$ the theory of separably closed fields of characteristic p, and $\mathtt{SCF}_{p,v}$ the theory of separably closed fields of characteristic p and degree of imperfection v. We shall assume for this section the reader is familiar with [Del99]. As $\mathtt{SCF}_0 = \mathtt{ACF}_0$ and $\mathtt{SCF}_{p,0} = \mathtt{ACF}_p$, we will not consider the cases $p = 0$ or $p > 0$, $v = 0$ (the case $v = \infty$ will be considered separately in *Corollary 3.2.8*).

Let $q \neq p$ be a prime number, $L = \left(\widetilde{\mathbb{F}_p(t)}(e_1, \ldots, e_v)\right)^s$ where $\{e_1, \ldots, e_v\}$ are transcendental and algebraically independent over $\widetilde{\mathbb{F}_p(t)}$. Note $L \models \mathtt{SCF}_{p,v}$, as $\widetilde{\mathbb{F}_p(t)}$ is perfect. First we have:

Proposition 3.2.1. *For each prime $q \neq p$, there exists a field $K_q \subset L$ such that:*

(1) $\mathbb{F}_p[t]$ is definable (with parameters) in K_q;

(2) If the intermediate field $K_q \subset H \subset L$ is finite and separable *over K_q, then $[H : K_q] = 1$ or is divisible by q.*

To prove this, we require a construction. Let $F = \left(\widetilde{\mathbb{F}_p(t)}(e_1, \ldots, e_{v-1})\right)^s \subset L$; we construct a field $K_q \subset L$ such that

$$F = \{a \in K_q : \forall b \in K_q^* \ ([1 + b \in (K_q)^q \wedge a^q + b^{-1} \in (K_q)^q] \to b \in (K_q)^q)\},$$
$$\mathbb{F}_p[t] = \{r \in F : \forall r_1 \neq r_2 \in F \text{ s.t. } r_1 + r_2 = r,\ e_v^q - r_1 \text{ or } e_v^q - r_2 \in (K_q)^q\}.$$

This will suffice to prove *Proposition 3.2.1 (1).* We take K_q to be the union of a sequence

$$F(e_v) = E_0 \subset E_1 \subset E_2 \subset \ldots$$

within L of finite separable extensions $E_i/F(e_v)$. Obtaining *Proposition 3.2.1 (2)* while ensuring F and $\mathbb{F}_p[t]$ are definable in this way requires us to keep a tight rein on the q-th roots in K_q. To that end, we will also carefully construct a sequence:

$$\emptyset = S_0 \subset S_1 \subset S_2 \subset \ldots$$

of finite subsets $S_i \subset E_i$, ultimately desiring $K_q \setminus (K_q)^q = \bigcup_i S_i$. As the structures E_i we build are function fields, we have the powerful tools of valuation theory at our disposal to achieve this. To ensure we do not introduce an incompatibility between $K_q \setminus (K_q)^q$ and F or $\mathbb{F}_p[t]$, we will ask the following rule ([Zie82, p. 273]) to be obeyed at each point of the sequence (E_i, S_i):

There is a family of discrete valuations $\{v_s\}_{s \in S_i}$ on E_i such that $v_s(F) = 0$ and $q \nmid v_s(s)$ for $s \in S_i$. In addition, for all $r_1 \neq r_2 \in F$ with $r_1 + r_2 \in \mathbb{F}_p[t]$, either $\forall s \in S_i$, $q | v_s(e_v^q - r_1)$, or $\forall s \in S_i$, $q | v_s(e_v^q - r_2)$. (♣)

We will reference the following two standard lemmas, taken directly from [Zie82, §3]:

Lemma 3.2.2. [Zie82, Lemma 1]. *Let (H_1, v_1) be a discretely valued field, H_2/H_1 a*

finite extension, and q a prime such that $q \nmid [H_2 : H_1]$. Then there is an extension of v_1 to H_2, which we denote v_2, such that $q \nmid (v_2H_2 : v_1H_1)$. ■

Lemma 3.2.3. [Zie82, Lemma 2]. *Let (H, v) be a valued field and q a prime distinct to $\mathrm{char}(Hv)$. For $a \in H \setminus (H)^q$ with $q|v(a)$, there is an extension of valued fields $(H(\sqrt[q]{a}), w)/(H, v)$ such that $wH(\sqrt[q]{a}) = vH$.* ■

We will also require the following fact:

Definition 3.2.4. Valuations v_1, v_2 on a field K are *dependent* if $\mathcal{O}_{v_1}\mathcal{O}_{v_2} \subsetneq K$.

Lemma 3.2.5. *If v_1, v_2 are dependent discrete valuations on a field K, then $v_1 = v_2$ (by which we mean $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$).*

Proof. The valuation ring of a discrete valuation is maximal [EP05, Corollary 2.3.2], hence $\mathcal{O}_{v_1} = \mathcal{O}_{v_1}\mathcal{O}_{v_2} = \mathcal{O}_{v_2}$ as desired. ■

The construction begins with an enumeration $a_0, a_1, a_2, \ldots$ of the elements of L separably algebraic over $F(e_v)$, each repeated countably infinitely many times. Suppose (E_i, S_i) is already constructed – Ziegler considers now four cases based on the equivalence class of i mod 4:

Construction.

Case 1: $i = 4n$. If $q|[E_i(a_n) : E_i]$, then $(E_{i+1}, S_{i+1}) = (E_i, S_i)$. Otherwise set $(E_{i+1}, S_{i+1}) = (E_i(a_n), S_i)$ and using *Lemma 3.2.2* extend each valuation v_s, $s \in S_i$, from E_i to E_{i+1} in a way preserving (♣).

Case 2: $i = 4n + 1$. Unless $a_n \in E_i \setminus S_i$, set $(E_{i+1}, S_{i+1}) = (E_i, S_i)$. Otherwise, if for some v_s, $s \in S_i$, we have $q \nmid v_s(a_n)$ then define $(E_{i+1}, S_{i+1}) = (E_i, S_i \cup \{a_n\})$ and set $v_{a_n} := v_s$. This ensures (♣) holds for $i + 1$. If $q|v_s(a_n)$ for all $s \in S_i$, then we take $(E_{i+1}, S_{i+1}) =^2 (E_i(\sqrt[q]{a_n}), S_i)$ and extend every valuation according to *Lemma 3.2.3*.

[2]Note $L = (L)^q$ as L is separably closed and $q \neq p$. In addition, we consider $\sqrt[q]{a_n} \in E_i$ if $a_n \in (E_i)^q$.

CASE 3: $i = 4n + 2$. Unless $a_n \in E_i \setminus F$, let $(E_{i+1}, S_{i+1}) = (E_i, S_i)$. If $a_n \in E_i \setminus F$ let v be a discrete valuation on E_i, trivial on F, which is negative on a_n. If the second condition in (♣) does not already hold for $\{v, \{v_s\}_{s\in S_i}\}$ in E_i, then there exists $r \in F$ such that $q \nmid v(e_v^q - r)$ and $q|v_s(e_v^q - r)$ for all $s \in S_i$. By the strong triangle inequality, there is at most one such r. As $L = (L)^q$, we may set $E = E_i(\sqrt[q]{e_v^q - r})$ and extend the valuations $\{v, \{v_s\}_{s\in S_i}\}$ sensibly as above. We conclude the second condition of (♣) holds for $(E, \{v, \{v_s\}_{s\in S_i}\})$.

If v is independent to v_s for every $s \in S_i$: let $\{v, v_{s_1}, \ldots, v_{s_k}\}$ be the distinct valuations of $\{v, \{v_s\}_{s\in S_i}\}$. By the *Approximation Theorem* [EP05, Theorem 2.4.1], there exists $b \in E$ such that $v(b)$ is the smallest positive element in the value group of v (hence $q|v(1 + b)$, $q|v(a_n^q + b^{-1})$) and $q|v_{s_j}(b)$, $q|v_{s_j}(1 + b)$, $q|v_{s_j}(a_n^q + b^{-1})$ for $1 \le j \le k$. As $b, 1 + b, a_n^q + b^{-1} \in (L)^q = L$, we may define

$$(E_{i+1}, S_{i+1}) = \left(E\left(\sqrt[q]{1 + b}, \sqrt[q]{a_n^q + b^{-1}}\right), S_i \cup \{b\}\right).$$

Extending $\{v_b = v, \{v_s\}_{s\in S_i}\}$ as above, we know (♣) holds as it did on E.

If v is dependent with $v_{\widehat{s}}$ for some $\widehat{s} \in S_i$: by *Lemma 3.2.5* $v = v_{\widehat{s}}$. Let $\{v_{s_1}, \ldots, v_{s_l}\}$ be the distinct valuations of $\{v, \{v_s\}_{s\in S_i}\}$, assuming WLOG $v = v_{s_1}$. By the *Approximation Theorem* [EP05, Theorem 2.4.1], there exists $b \in E$ such that $v_{s_1}(b)$ is the smallest positive element in the value group of v_{s_1}, and $q|v_{s_j}(b)$, $q|v_{s_j}(1 + b)$, $q|v_{s_j}(a_n^q + b^{-1})$ for $2 \le j \le l$. As $b, 1 + b, a_n^q + b^{-1} \in (L)^q = L$, we may define

$$(E_{i+1}, S_{i+1}) = \left(E\left(\sqrt[q]{1 + b}, \sqrt[q]{a_n^q + b^{-1}}\right), S_i \cup \{b\}\right).$$

Extending $\{v_b = v_{s_1}, \{v_s\}_{s\in S_i}\}$ as above, again (♣) holds on (E_{i+1}, S_{i+1}). (This case allows $b \in S_i$ without issue, by *Lemma 3.2.5*.)

CASE 4: $i = 4n + 3$. Unless $a_n \in F \setminus \mathbb{F}_p[t]$ we set $(E_{i+1}, S_{i+1}) = (E_i, S_i)$. Otherwise, first observe $B = \{r \in F : \exists s \in S_i \text{ s.t. } q \nmid v_s(e_v^q - r)\}$ is finite. Next, for

$r \in F^*$ there exists a discrete valuation v_r on $F(e_v)$, trivial on F, for which $v_r(e_v^q - r)$ is the smallest positive element of its valuation group (this follows as $X^q - r \in F[X]$ has no multiple factors). For each such r, we choose an extension w_r of v_r to E_i, and by the construction of E_i/F, the set $C = \{r \in F^* : q | w_r(e_v^q - r)\}$ is finite. Choose $r_1 \in F^*$ such that $r_1 \neq a_n$, $2r_1 \neq a_n$, and $r_1 \notin C, \{a_n\} - C, \mathbb{F}_p[t] \pm B, \{a_n\} - (\mathbb{F}_p[t] \pm B)$. Let $r_2 = a_n - r_1$ and finally define:

$$(E_{i+1}, S_{i+1}) = (E_i, S_i \cup \{e_v^q - r_1, e_v^q - r_2\}).$$

One can prove $\{w_{r_1}, w_{r_2}, \{v_s\}_{s \in S_i}\}$ satisfies (♣) based on this construction.

These correspond to guaranteeing *Proposition 3.2.1 (1)* (Case 1), *Proposition 3.2.1 (2)* (Case 2), the definition of F by ensuring there is a 'reason' b is excluded (Case 3 + ♣), and the definition of $\mathbb{F}_p[t]$ (Case 4 + ♣); again, by ensuring there is a 'reason' a_n is excluded. This is highlighted by the following lemma:

Lemma 3.2.6. *Set $K_q = \bigcup_i E_i$. The above construction ensures we have the following features of K_q, and the definitions of F and $\mathbb{F}_p[t]$ we intended:*

(1) $F \subset (K_q)^q$.

(2) $K_q \setminus (K_q)^q = \bigcup_i S_i$.

(3) $F = \{a \in K_q : \forall b \in K_q^* \ [(1 + b \in (K_q)^q \wedge a^q + b^{-1} \in (K_q)^q) \to b \in (K_q)^q]\}$.

(4) $\mathbb{F}_p[t] = \{r \in F : \forall r_1 \neq r_2 \in F \ (r_1 + r_2 = r) \to (e_v^q - r_1 \in (K_q)^q \vee e_v^q - r_2 \in (K_q)^q)\}$.

Proof. We follow [Zie82, §4] as much as possible.

(1) As F is separably closed, and $q \neq p$, $F = (F)^q$.

(2) Let $a \in (K_q)^q$. For all sufficiently large i, $a \in (E_i)^q$; hence $q | v(a)$ for all v trivial on F. Therefore by (♣) we have $a \notin S_i$; consequently $a \notin \bigcup_i S_i$. Conversely if

$a \in K_q \setminus (K_q)^q$, then for some n sufficiently large we have $a = a_n$ and $a \in E_{4n+1}$. By CASE 2 of the construction, $a \in S_{4n+2}$. This proves $K_q \setminus (K_q)^q = \bigcup_i S_i$.

(3) Fix $a \in F$. Suppose for some nonzero $b \in K_q$ that $1 + b, a^q + b^{-1} \in (K_q)^q$. Let i be so large that $1 + b, a^q + b^{-1} \in (E_i)^q$. Let v be any valuation on E_i that is trivial on F. If $v(b) > 0$, then $v(b) = -v(a^q + b^{-1})$ is divisible by q. If $v(b) < 0$, then $v(b) = v(1 + b)$ is divisible by q. Hence $q|v(b)$ always. By (♣), $b \notin S_i$; by (2) therefore $b \in (K_q)^q$. Conversely, if $a \in K_q \setminus F$, we may choose n sufficiently large such that $a = a_n \in E_{4n+2}$. In CASE 3 we make it such that in S_{4n+3} there is a b with $1 + b, a^q + b^{-1} \in (E_{4n+3})^q$. This concludes the proof.

(4) Let $r_1 + r_2 \in \mathbb{F}_p[t]$, with $r_1 \neq r_2 \in F$. If it is the case that $e_v^q - r_1, e_v^q - r_2 \notin (K_q)^q$, then for some sufficiently large i, they belong to S_i. However this contradicts (♣). If we suppose $r \in F \setminus \mathbb{F}_p[t]$, for some sufficiently large n it is the case that $a_n = r$. Then by CASE 4 there exists $r_1 \neq r_2 \in F$, $r_1 + r_2 = r$, such that $e_v^q - r_1, e_v^q - r_2 \in S_{4n+4}$. By (2) this ensures $e_v^q - r_1, e_v^q - r_2 \notin (K_q)^q$; again a contradiction. ■

Proof of Proposition 3.2.1:

First, as F and $\mathbb{F}_p[t]$ are definable, arithmetic is interpretable in K_q (in the sense of *Definition A.2*). Next, note that $K_q/F(e_v)$ is a separable extension, as by construction it is a union of finite separable extensions, and $K_q \subseteq F(e_v)^s$. Let $K_q \subset H \subset L$ be a finite separable extension. Then $H = K_q(a)$ for some $a \in L$ by the *Primitive Element Theorem*. As $K_q(a)/F(e_v)$ is separable, for some n sufficiently large we have $a = a_n$ and

$$[E_{4n}(a_n) : E_{4n}] = [K_q(a) : K_q],$$

as we assume $a \notin K_q$. By construction, $q|[E_{4n}(a) : E_{4n}]$. ■

Combining these fields in a nonprincipal ultraproduct allows us to conclude the desired undecidability result.

Corollary 3.2.7. *Let p be a prime and $v \in \mathbb{N}_{>0}$. Then $\mathtt{SCF}_{p,v}$ is finitely undecidable.*

Proof. Let $L = \left(\widetilde{\mathbb{F}_p(t)}(e_1, \ldots, e_v)\right)^s$ as before *Proposition 3.2.1.* Let P be the set of primes distinct to p. For each $q \in P$, use *Proposition 3.2.1* to obtain a field K_q satisfying *(1) & (2) ibid.* Let $\mathcal{U}$ be a nonprincipal ultrafilter on P and let $\mathbb{K}$ be the ultraproduct $\prod_{q \in P} K_q/\mathcal{U}$.

We claim that $\mathbb{K}$ is relatively separably closed in $L^{\mathcal{U}}$. Indeed, suppose $f = (f_q) \in \mathbb{K}[X]$ is separable and has a root $\alpha = (\alpha_q) \in L^{\mathcal{U}}$. In which case

$$\{q : f_q(x) \in K_q[X] \text{ separable, and } f_q(\alpha_q) = 0\} \in \mathcal{U},$$
$$\text{hence } \{q : K_q(\alpha_q)/K_q \text{ separable and } [K_q(\alpha_q) : K_q] \leq \deg(f)\} \in \mathcal{U}.$$

By *Proposition 3.2.1 (2)*, $\{q : [K_q(\alpha_a) : K_q] = 1\} \in \mathcal{U}$, and thus $\alpha \in \mathbb{K}$ as desired.

Therefore $\mathbb{K}$ is a separably closed field of characteristic p. Recall $\{e_1, \ldots, e_v\}$ is a p-basis for L. As they are p-independent in L, and by construction $e_1, \ldots, e_v \in K_q$, they remain p-independent in K_q. Hence the degree of imperfection of K_q is at least v, for each q. Moreover, by construction $K_q/\widetilde{\mathbb{F}_p(t)}(e_1, \ldots, e_v)$ is an algebraic (separable) extension. As algebraic extensions do not increase the degree of imperfection, the degree of imperfection of K_q is at most v. Thus by *Łoś' Theorem* the degree of imperfection of $\mathbb{K}$ is v exactly. We conclude that $\mathbb{K} \models \mathtt{SCF}_{p,v}$, and hence $\mathbb{K} \models T$ for any finite subtheory $T \subseteq \mathtt{SCF}_{p,v}$.

Since T is finitely axiomatised, there exists some prime q such that $K_q \models T$. By *Lemma 3.2.6 & Corollary A.10*, $\mathtt{Th}(K_q; \mathcal{L}_r)$ is hereditarily undecidable, making T undecidable as required. ∎

Corollary 3.2.8. *Let p be prime. Then $\mathtt{SCF}_{p,\infty}$ is finitely undecidable.*

Proof. Let T be a finite subtheory of $\mathtt{SCF}_{p,\infty}$, which we assume is axiomatised by the axioms of a field of characteristic p, such that each separable polynomial over the field has a root in the field, and for each $n \in \mathbb{N}_{>0}$ the statement "the degree of imperfection is greater than n". By the *Compactness Theorem*, there exists a finite subset Δ of this

axiomatisation such that $\Delta \models T$. For some finite ν sufficiently large, $\mathtt{SCF}_{p,\nu} \models \Delta$, hence T is a finite subtheory of $\mathtt{SCF}_{p,\nu}$. The result follows from *Corollary 3.2.7.* ■

Example 3.2.9. For all primes $p > 0$ and $v \in \mathbb{N} \cup \{\infty\}$, the theory $\mathtt{SCF}_{p,v}$ is known to be decidable (see [Del99, pp. 146–153] for exposition). Therefore *Corollaries 3.2.7 & 3.2.8* put a bound on further possible decidability results for these theories. □

It is worth remarking that, modulo some conjectures, these results are in connection with aspects of classification theory. It is a theorem of Macintyre [Mac71] that every infinite ω-stable field is a model of $\mathtt{ACF}_p$ for some $p \geq 0$ (a consequence of *Theorem 1, §7 ibid.*). From the 1970's we have the following conjecture:

Conjecture (Stable Fields). *Every infinite stable field is separably closed.* ■

This is known in some cases, such as for the aforementioned ω-stable [Mac71] or superstable infinite fields [CS80, Theorem 1], or for infinite stable fields of weight 1 [KP11, Theorem 1.7] or finite dp-rank [HP19, Proposition 7.3]. Recently, Johnson et al. proved the conjecture for infinite large stable fields [JTWY21, Theorem D].

Corollary 3.2.10. *Assume the Stable Fields Conjecture. Then every infinite stable field is finitely undecidable.* ■

Let us use this connection to classification theory to motivate which fields to consider next. Outside of stability theory, there are two orthogonal directions in which to travel: one direction attempts to extend the theories of forking, dividing and independence of types to more general contexts (e.g. [super]simple, [super]rosy), while the other direction aims to understand theories with a modest notion of order (e.g. o-minimal, dp-minimal, NIP). The latter direction contains theories we are already familiar with: $\mathtt{RCF}$ in the language of ordered rings is o-minimal, $p\mathtt{CF}$ in the language of valued fields is distal and dp-minimal. One might wonder what other field theories could be present under this banner – and there is a conjecture of Shelah that would answer this question:

Conjecture (Shelah/NIP Fields). *Every infinite NIP*[3] *field is either separably closed, real closed, or admits a nontrivial henselian valuation.*

Theorem 3.2.11. [HHJ20, Proposition 6.2 (2)]. *Assume the NIP Fields Conjecture. Then every infinite NIP field is either real closed, separably closed, or admits a nontrivial henselian valuation* definable in the language of rings. ■

Therefore a sensible goal would be to prove that every field with a nontrivial $\mathcal{L}_r$-definable henselian valuation is finitely undecidable. Or more so, that every complete $\mathcal{L}_{val}$-theory of henselian nontrivially valued fields is finitely undecidable, where $\mathcal{L}_{val}$ is the language of valued fields.

3.3 Equicharacteristic 0 Henselian Valued Fields

The previous subsection did not address the aspects of Ziegler's construction relevant to $\mathbb{Q}_p$; these aspects will be seen in this subsection. In this subsection we will consider a pair of valued fields (R, v_R), (T, v_T), and an additional field F, under the following assumptions:

Assumption ($\otimes$).

(1) $R \subset F \subset T$, $v_R = v_T|_R$, *and* (T, v_T) *is a henselian immediate extension of* (R, v_R)*;*

(2) R *(thence* $v_R R$ *and* Rv_R*) is countable, and if* $\mathrm{char}(R) > 0$ *then* R *is transcendental over its prime subfield;*

(3) There are uncountably many elements of T *transcendental over* R*;*

(4) $F = T \cap R(\overline{x})^s$*, where* $R(\overline{x})$ *is a purely transcendental, finite transcendence degree extension of* R*;*

(5) Let $q > \max\{\mathrm{char}(R), \mathrm{char}(Rv_R)\}$ *be prime; then* $T = (T)^q \cdot F^*$.

[3]The class of NIP theories contains the classes of o-minimal, distal, and dp-minimal theories; see *Figure 1.1.*

First we will give a concrete example of a pair of valued fields where these assumptions are satisfied. Let k be a field and Γ a nontrivial ordered abelian group. Consider the multiplicative group of formal monomials $\{t^\gamma : \gamma \in \Gamma\}$, where $t^0 = 1$ and $t^{\gamma_1} \cdot t^{\gamma_2} = t^{\gamma_1+\gamma_2}$. Define $k[\Gamma]$ to be the set of formal series $\sum_\gamma a_\gamma t^\gamma$ where $a_\gamma \in k$ and only finitely many a_γ are nonzero. Addition and multiplication are defined by

$$\sum_\gamma a_\gamma t^\gamma + \sum_\gamma b_\gamma t^\gamma = \sum_\gamma (a_\gamma + b_\gamma) t^\gamma;$$
$$\left(\sum_\gamma a_\gamma t^\gamma\right) \cdot \left(\sum_\gamma b_\gamma t^\gamma\right) = \sum_\gamma \left(\sum_{\gamma_1+\gamma_2=\gamma} a_{\gamma_1} b_{\gamma_2}\right) t^\gamma.$$

These operations are confirmed to be well-defined, and $k[\Gamma]$ an integral domain, by [Mar18, §2.4]. This domain comes with a natural valuation $v_\Gamma(\sum_\gamma a_\gamma t^\gamma) := \min \operatorname{supp}(\sum_\gamma a_\gamma t^\gamma)$. Define $k(\Gamma)$ to be the fraction field of this valued domain. Further define $k((\Gamma))$ as the set whose elements are formal series $\sum_\gamma a_\gamma t^\gamma$ with well-ordered support. By [Mar18, §2.4], $(k((\Gamma)), v_\Gamma)$ is a well-defined, spherically complete, immediate henselian overfield of $(k(\Gamma), v_\Gamma)$.

Lemma 3.3.1. *Let $e \in \mathbb{N}$, k and Γ be countable, and v be a henselian valuation on $k((\Gamma))$ which factors through v_Γ, i.e. there exists a valuation v' on k such that*[4] *$v = v' \circ v_\Gamma$. For $t_1, \ldots, t_e \in k((\Gamma))$ transcendental and algebraically independent over $k(\Gamma)$, the pair of valued fields $(R, v_R) = (k(\Gamma), v|_{k(\Gamma)})$, $(T, v_T) = (k((\Gamma)), v)$, and $F = k((\Gamma)) \cap (k(\Gamma)(t_1, \ldots, t_e))^s$ satisfy* Assumption $(\otimes)$.

Proof. Properties *(1) & (4)* follow by definition. Property *(2)* follows by construction, and as $k(\Gamma)$ is countable (from its definition). Property *(3)* can be seen by a cardinality argument (cf. [vdD14, p. 82]): fixing $\gamma \in \Gamma^{>0}$ there is an injection $(\mathbb{N}; 0, +, <) \hookrightarrow (\Gamma; 0, +, <)$ given by $n \mapsto n \cdot \gamma$, and by definition $|k((\Gamma))| \geq |k|^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0}$, while $|k(\Gamma)^s| = \aleph_0$.

Property *(5)* requires more work: we adapt [Zie82, Lemma 3]. Clearly $(k((\Gamma)))^q \cdot F^* \subseteq k((\Gamma))$; we are required to show that for all $a \in k((\Gamma))^*$, there exists $b \in F^*$ such that

[4] By "$v' \circ v_\Gamma$" we mean the composition of places $res_{v'}$, res_{v_Γ}, which give rise to the valuations as per usual (cf. [FJ08, Construction 2.2.6]).

$ab^{-1} \in (k((\Gamma)))^q$. Choose $b \in F^*$ such that $v_\Gamma(a-b) > v_\Gamma(a)$; this can be done by setting $b \in k(\Gamma)^* \subset F^*$ to be the initial term of a. Then $v_\Gamma(ab^{-1}-1) > v_\Gamma(ab^{-1})$, hence $ab^{-1} \equiv 1 \bmod \mathfrak{m}_{v_\Gamma}$. By Hensel's Lemma (regardless of v, $(k((\Gamma)), v_\Gamma)$ is henselian), ab^{-1} is a q-th power in $k((\Gamma))$, as desired. ■

Using *Assumption* ($\otimes$), we shall construct a field extension $R \subset K_q \subset T$ such that $\mathbb{Z}$ or $\mathbb{F}_p[z]$ (where $p = \mathrm{char}(R) > 0$ and $z \in R$ is transcendental over $\mathbb{F}_p$) is $\mathcal{L}_{val}$-definable in K_q, and if $K_q(a) \subset T$ is a proper finite separable extension of K_q, then $q|[K_q(a) : K_q]$. We must be slightly more careful than in the pp. 44–46 CONSTRUCTION, as we shall see below.

By *Assumption* ($\otimes$) there exists an element $t \in T$ transcendental over F. The field K_q will be the union of a specific sequence of finite separable extensions of $F(t)$ in T:

$$R \subset F \subset F(t) = E_0 \subset E_1 \subset E_2 \subset \cdots \quad \subset T.$$

As before, we will also construct a sequence $\emptyset = S_0 \subset S_1 \subset S_2 \subset \cdots$ of finite subsets $S_i \subset E_i \cap (T)^q$, ultimately desiring a close relationship between $K_q \setminus (F^* \cdot (K_q)^q)$, $(K_q \cap (T)^q) \setminus (K_q)^q$, and $\bigcup_i S_i$. We will desire F & $\mathbb{Z}$ (if $\mathrm{char}(R) = 0$; $\mathbb{F}_p[z]$ otherwise) to have the following definitions, similar to as before:

$$F = \{a \in K_q : \forall b \in K_q \cap (T)^q \setminus \{0\}, ([1 + b \in (K_q)^q \wedge a^q + b^{-1} \in (K_q)^q] \to b \in (K_q)^q)\},$$

$$\mathbb{Z} \text{ (resp. } \mathbb{F}_p[z]) = \{u \in F : \forall u_1 \neq u_2 \in F \text{ s.t. } u_1 + u_2 = u,\ t^q - u_1 \text{ or } t^q - u_2 \in (K_q)^q\}.$$

Denote by "$v_T|_{E_i}$" the restriction of v_T to $E_i \subset T$. To again ensure we do not introduce an incompatibility between $(K_q \cap (T)^q) \setminus (K_q)^q$ and F or $\mathbb{Z}$ (resp. $\mathbb{F}_p[z]$), the following rule will be enforced during the construction:

There is a family of discrete valuations $\{v_s\}_{s \in S_i}$ on E_i such that $v_s(F) = 0$ and $q \nmid v_s(s)$ for $s \in S_i$. In addition, for all $u_1 \neq u_2 \in F$ with $u_1 + u_2 \in \mathbb{Z}$ (resp. $\mathbb{F}_p[z]$), either $\forall s \in S_i$, $q|v_s(t^q - u_1)$, or $\forall s \in S_i$, $q|v_s(t^q - u_2)$. (♥)

We have the following lemma:

Lemma 3.3.2. *Let u be a nontrivial discrete valuation on $F(t)$, trivial on F, and u' an extension of u to E_i. Then u' and $v_T|_{E_i}$ are independent (in the sense of* Definition 3.2.4*).*

Proof. Assume u' and $v_T|_{E_i}$ are dependent: by [EP05, Theorem 2.3.4] they induce the same topology on E_i. Thus there exists $a \in E_i$ such that $a \cdot \mathfrak{m}_{u'} \subseteq \mathfrak{m}_{v_T|_{E_i}}$ $(= \mathfrak{m}_{v_T} \cap E_i)$. However, as $R \subset F \subset E_i$ (and thus $u'(R) = 0$, while $v_R R = v_T T$), there exists $f \in a \cdot \mathfrak{m}_{u'}$ with $v_T(f) = v_T|_{E_i}(f) < 0$; a contradiction. ■

Fix an enumeration $a_0, a_1, \ldots$ of the elements of T separably algebraic over $F(t)$, each repeated countably infinitely many times. Suppose (E_i, S_i) is already constructed – and consider the following modified construction.

Modified Construction. (cf. [Zie82, §3])

Case 1: $i = 4n$. As on p. 44.

Case 2: $i = 4n+1$. If $a_n \notin E_i$, $a_n \notin (T)^q$, or $a_n \in S_i$ then set $(E_{i+1}, S_{i+1}) = (E_i, S_i)$. Otherwise proceed as on p. 44.

Case 3: $i = 4n + 2$. Unless $a_n \in E_i \setminus F$, let $(E_{i+1}, S_{i+1}) = (E_i, S_i)$. If $a_n \in E_i \setminus F$ let w be a discrete valuation on E_i (considered as a function field extension of $F(t)/F$), trivial on F, which is negative on a_n. By *Lemma 3.3.2*, w and $v_T|_{E_i}$ are independent. Let us define a finite separable extension E/E_i: if the second condition of (♥) already holds for $\{w, \{v_s\}_{s\in S_i}\}$ in E_i, set $E = E_i$. Otherwise there exists $u \in F$ such that $q \nmid w(t^q - u)$ and $q | v_s(t^q - u)$ for all $s \in S_i$. By the strong triangle inequality, there is at most one such u.

Under *Assumption* $(\otimes)(5)$ there exists $d \in F^*$ such that $d(t^q - u) \in (T)^q$. Thus we may set $E = E_i(\sqrt[q]{d(t^q - u)})$ and extend the valuations $\{v_s\}_{s\in S_i}$ sensibly as before (and let w' be any extension to E of w). We conclude the second condition of (♥) now holds for $(E, \{w', \{v_s\}_{s\in S_i}\})$.

If w' is independent to v_s for every $s \in S_i$: let $\{w', v_{s_1}, \ldots, v_{s_k}\}$ be the distinct valuations of $\{w', \{v_s\}_{s\in S_i}\}$. By the *Approximation Theorem* [EP05, Theorem 2.4.1], there exists $b \in E$ such that $w'(b)$ is the smallest positive element of its value group, $q|v_{s_j}(b)$ and $v_{s_j}(b) < 0, -v_{s_j}(a_n^q)$ for $1 \leq j \leq k$. Notice $q|w'(1+b)$, $q|w'(a_n^q+b^{-1})$, and $q|v_s(a_n^q+b^{-1})$, $q|v_s(1+b)$ for all $s \in S_i$.

We also wish $b, 1+b, a_n^q + b^{-1} \in (T)^q$. This can be achieved with further care by using the *Approximation Theorem* and Hensel's Lemma: by *Lemma 3.3.2* and [EP05, Corollary 2.3.2], $v_T|_E$, w', and v_{s_j} for $1 \leq j \leq k$ are pairwise independent. Let $d \in (E)^q \subset (T)^q$ have $v_T|_E(d) > 0$. Using the *Approximation Theorem*, we choose $b \in E$ so that in addition $v_T|_E(b-d) > v_T|_E(d)$. Then by Hensel's Lemma, $b \in E \cap (T)^q$, and since $v_T|_E((b+1)-1) = v_T|_E(b)$ and $v_T|_E((b+a_n^{-q})-a_n^{-q}) = v_T|_E(b)$, we have $1+b, b+a_n^{-q} \in E \cap (T)^q$. (Hence $a_n^q + b^{-1} \in E \cap (T)^q$.) We define

$$(E_{i+1}, S_{i+1}) = (E(\sqrt[q]{1+b}, \sqrt[q]{a_n^q + b^{-1}}), S_i \cup \{b\}).$$

Extending $\{v_b = w', \{v_s\}_{s\in S_i}\}$ as in Case 2, (♥) holds as it did on E.

Now assume w' is dependent with $v_{\widehat{s}}$ for some $\widehat{s} \in S_i$: in which case, $w' = v_{\widehat{s}}$ by *Lemma 3.2.5*. Let $\{v_{s_1}, \ldots, v_{s_l}\}$ be the distinct valuations of $\{w', \{v_s\}_{s\in S_i}\}$, assuming WLOG $w' = v_{s_1}$. By *Lemma 3.3.2* and [EP05, Corollary 2.3.2], $v_T|_E$, and v_{s_j} for $1 \leq j \leq l$ are pairwise independent. Let $d \in (E)^q \subset (T)^q$ have $v_T|_E(d) > 0$. Using the *Approximation Theorem*, we choose $b \in E$ so that $v_T|_E(b-d) > v_T|_E(d)$, $v_{s_1}(b)$ is the smallest positive element of its value group, $q|v_{s_j}(b)$ and $v_{s_j}(b) < 0, -v_{s_j}(a_n^q)$ for $2 \leq j \leq l$. By Hensel's Lemma, $1+b, a_n^q + b^{-1} \in E \cap (T)^q$, and we may define

$$(E_{i+1}, S_{i+1}) = (E(\sqrt[q]{1+b}, \sqrt[q]{a_n^q + b^{-1}}), S_i \cup \{b\}).$$

Extending $\{v_b = w', \{v_s\}_{s\in S_i}\}$ as in Case 2, (♥) holds on (E_{i+1}, S_{i+1}). (Again this case allows for $b \in S_i$ without issue, by *Lemma 3.2.5*.)

CASE 4: $i = 4n+3$. As on pp. 45–46. Recall this step extends $\{v_s\}_{s\in S_i}$ to $\{v_s\}_{s\in S_{i+1}} = \{w_{r_1}, w_{r_2}, \{v_s\}_{s\in S_i}\}$. The valuations w_{r_1}, w_{r_2} are independent to $v_T|_{E_i}$ by *Lemma 3.3.2*, and (♥) is satisfied.

Now we can show the following (cf. *Lemma 3.2.6*):

Lemma 3.3.3. *Set $K_q = \bigcup_i E_i$. The above construction ensures we have the following features of K_q under* Assumption ($\otimes$):

(1) $(K_q \cap (T)^q) \setminus (K_q)^q = \bigcup_i S_i$.

(2) $F^* \cdot (\bigcup_i S_i) = K_q \setminus (F^* \cdot (K_q)^q)$.

(3) $F = \{a \in K_q : \forall b \in K_q \cap (T)^q \setminus \{0\}, ([1 + b \in (K_q)^q \wedge a^q + b^{-1} \in (K_q)^q] \to b \in (K_q)^q)\}$.

(4) $\mathbb{Z}$ *(resp.* $\mathbb{F}_p[z]$*)* $= \{u \in F : \forall u_1 \neq u_2 \in F \text{ s.t. } u_1 + u_2 = u, t^q - u_1 \text{ or } t^q - u_2 \in F^* \cdot (K_q)^q\}$.

Proof. In [Zie82, §4], but for exposition:

(1) Let $a \in (K_q \cap (T)^q) \setminus (K_q)^q$. For some n sufficiently large, $a_n = a$ and $a_n \in E_{4n+1}$. CASE 2 of the above construction assures $a_n \in S_{4n+2}$, hence $a \in \bigcup_i S_i$ as desired. Conversely, by construction $\bigcup_i S_i \subset K_q \cap (T)^q$, and $S_i \cap (K_q)^q = \emptyset$ for all i.

(2) Let $a \in F^* \cdot (K_q)^q$. For all i sufficiently large, $a \in F^* \cdot (E_i)^q$ and hence $q|\nu(a)$ for all valuations ν trivial on F. By design of (♥), $a \notin F^* \cdot S_i$, hence $F^* \cdot (\bigcup_i S_i) \subseteq K_q \setminus (F^* \cdot (K_q)^q)$. Conversely, if $a \in K_q \setminus (F^* \cdot (K_q)^q)$, then by *Assumption* ($\otimes$)(5) there exists $b \in F^*$ with $ab \in (K_q \cap (T)^q) \setminus (K_q)^q = \bigcup_i S_i$ by (1).

(3) Let $a \in F$. Suppose for $b \in K_q \cap (T)^q \setminus \{0\}$, we have $1 + b, a^q + b^{-1} \in (K_q)^q$. Let i be sufficiently large such that $1 + b, a^q + b^{-1} \in (E_i)^q$. Notice that, for any valuation ν on E_i trivial on F, $q|\nu(b)$: indeed, if $\nu(b) < 0$ then $\nu(b) = \nu(1 + b)$, and if $\nu(b) > 0$ then $\nu(b) = \nu(a^q + b^{-1})$. By (♥) $b \notin S_i$ (for all subsequent i too), hence as $b \in K_q \cap (T)^q$, $b \in (K_q)^q$ by (1).

Conversely, if $a \in K_q \setminus F$, then for some n sufficiently large we may assume $a_n = a$ and $a \in E_{4n+2}$. By Case 3 of the construction, deliberately there exists $b \in S_{4n+3}$ such that $1 + b, a^q + b^{-1} \in (E_{4n+3})^q$ and $b \in K_q \cap (T)^q$. Therefore by (1),

$$\exists b \in K_q \cap (T)^q \setminus \{0\},\ (1 + b \in (K_q)^q \wedge a^q + b^{-1} \in (K_q)^q \wedge b \notin (K_q)^q),$$

as desired.

(4) Let $u \in \mathbb{Z}$ (resp. $\mathbb{F}_p[z]$), $u_1 \neq u_2 \in F$, and $u_1 + u_2 = u$. Assume for the purpose of contradiction both $t^q - u_1, t^q - u_2 \notin F^* \cdot (K_q)^q$. By the argument in Case 3 there exist d_1, d_2 such that $d_1(t^q - u_1), d_2(t^q - u_2) \in (K_q \cap (T)^q) \setminus (K_q)^q = \bigcup_i S_i$, by (1). We conclude for some sufficiently large i that $t^q - u_1, t^q - u_2 \in F^* \cdot S_i$, contradicting (♥).

Conversely, if $u \in F \setminus \mathbb{Z}$ (resp. $F \setminus \mathbb{F}_p[z]$), then for some n sufficiently large we may assume $a_n = u$ and $a_n \in E_{4n+3}$. By Case 4 of the construction, deliberately there exists $u_1 \neq u_2 \in F^*$ with $u_1 + u_2 = u$ and $t^q - u_1, t^q - u_2 \in S_{4n+4} \subset F^* \cdot S_{4n+4}$. Therefore by (2), $t^q - u_1, t^q - u_2 \notin F^* \cdot (K_q)^q$ as required for this argument. ■

Let us return to the case $(R, v_R) = (k(\Gamma), v_\Gamma|_{k(\Gamma)})$, $(T, v_T) = (k((\Gamma)), v_\Gamma)$, $F = k((\Gamma)) \cap (k(\Gamma)(t_1, \ldots, t_e))^s$. We have the following additional results:

Theorem 3.3.4. (Ax-Kochen-Ershov) [AK65, Ers65a]. *Let (K, v) and (L, w) be equicharacteristic 0 henselian valued fields. Then $K \equiv_{\mathcal{L}_{val}} L$ if and only if $Kv \equiv_{\mathcal{L}_r} Lw$ and $vK \equiv_{\mathcal{L}_{oag}} wL$.* ■

Consequently $(L, w) \equiv (Lw((wL)), v_{wL})$ if (L, w) is an equicharacteristic 0 henselian valued field.

Lemma 3.3.5. *Let $q > \mathrm{char}(k)$ be prime and v a henselian valuation on $k((\Gamma))$ which factors through v_Γ, where k and Γ are countable, and K_q as above. Then $K_q \cap (k((\Gamma)))^q$ is $\mathcal{L}_{val}$-definable in (K_q, w), where $w = v|_{K_q}$.*

Proof. Recall from *Lemma 3.3.1* that *Assumption* ($\otimes$) is satisfied. We claim that $c \in K_q \cap (k((\Gamma)))^q$ if and only if there exists $d \in K_q$ such that $w(c - d^q) > w(c)$. This suffices to prove the lemma.

Assume there exists $d \in K_q$ such that $w(c-d^q) > w(c)$; then (as elements of $k((\Gamma))$) we have $v(c - d^q) > v(c)$, hence $v(1 - \frac{d^q}{c}) > 0$, and thus $1 \equiv \frac{d^q}{c} \bmod \mathfrak{m}_v$. By Hensel's Lemma, there exists $e \in k((\Gamma))$ such that $e^q = \frac{d^q}{c}$; we conclude $c \in (k((\Gamma)))^q$.

Conversely, let $c \in K_q \cap (k((\Gamma)))^q$ and write $c = \widehat{d^q}$. Let $d \in k(\Gamma)$ be a sufficiently large finite truncation of $\widehat{d} \in k((\Gamma))$ such that $v_\Gamma(\widehat{d}-d) > v_\Gamma(\widehat{d})$ (and note $v_\Gamma(\widehat{d}) = v_\Gamma(d)$). Then

$$\begin{aligned} v_\Gamma(\widehat{d^q} - d^q) &= v_\Gamma(\widehat{d} - d) + v_\Gamma(\widehat{d}^{q-1} + \widehat{d}^{q-2}d + \cdots + \widehat{d}d^{q-2} + d^{q-1}) \\ &\geq v_\Gamma(\widehat{d} - d) + (q-1)v_\Gamma(\widehat{d}) > qv_\Gamma(\widehat{d}) = v_\Gamma(\widehat{d^q}), \quad \text{hence } v_\Gamma(\tfrac{\widehat{d^q} - d^q}{\widehat{d^q}}) > 0. \end{aligned}$$

Consequently $v(\frac{\widehat{d^q} - d^q}{\widehat{d^q}}) > 0$, i.e. $v(\widehat{d^q} - d^q) > v(\widehat{d^q})$; equivalently $v(c - d^q) > v(c)$ and hence $w(c - d^q) > w(c)$ as desired. ■

Theorem 3.3.6. *Let $q > \mathrm{char}(k)$ be prime, v a henselian valuation on $k((\Gamma))$ which factors through v_Γ (where k and Γ are countable), and K_q as above. Then:*

(1) $(K_q, v_\Gamma|_{K_q})$ is an immediate extension of $(k(\Gamma), v_\Gamma)$;

(2) $(K_q, v|_{K_q})$ is an immediate extension of $(k(\Gamma), v)$;

(3) $\mathbb{Z}$ (resp. $\mathbb{F}_p[z]$) is definable in K_q in the language $\{0, 1, +, \times, \mathcal{O}_{v|_{K_q}}\}$;

(4) If $a \in k((\Gamma)) \setminus K_q$ is separably algebraic over K_q, then $q|[K_q(a) : K_q]$.

Proof. *(1) & (2)* follow from the fact that $k(\Gamma) \subset K_q \subset k((\Gamma))$. For *(3)*, $\mathbb{Z}$ (resp. $\mathbb{F}_p[z]$) is $\mathcal{L}_{val}$-definable in K_q as $K_q \cap (k((\Gamma)))^q$ is $\mathcal{L}_{val}$-definable in K_q by *Lemma 3.3.5*, and this is sufficient to define $\mathbb{Z}$ (resp. $\mathbb{F}_p[z]$) by *Lemma 3.3.3*. Finally for *(4)*, note for some n sufficiently large, we have $a = a_n$ and $[E_{4n}(a_n) : E_{4n}] = [K_q(a) : K_q]$, as we assume $a \notin K_q$. By construction (Case 1), $q|[E_{4n}(a) : E_{4n}]$ as desired. ■

Remark 3.3.7. ([EP05, pp. 173–178].) Let S be an infinite set of indices and $\mathcal{U}$ a nonprincipal ultrafilter on S. For $s \in S$, let (K_s, v_s) be a valued field. One may take an ultraproduct $\prod_{s\in S}(K_s, v_s)/\mathcal{U}$ of valued fields, and obtain a valued field $\mathbb{K} = \prod_{s\in S} K_s/\mathcal{U}$ with value group $\prod_{s\in S} v_s K_s/\mathcal{U}$ and residue field $\prod_{s\in S} K_s v_s/\mathcal{U}$, under the valuation $\prod v_s$ defined by:

$$\prod v_s([(a_s)_{s\in S}]) = [(v_s(a_s))_{s\in S}], \quad \text{with residue}$$
$$res_{\prod v_s} : \mathcal{O}_{\prod v_s} \to \prod_{s\in S} K_s v_s/\mathcal{U}; \quad [(x_s)] \mapsto [(res_{v_s}(x_s))].$$

(Here $a_s \in K_s$ for $s \in S$, and $[\cdot]$ represents the equivalence class of tuples modulo $\mathcal{U}$.) □

Corollary 3.3.8. *Let (K, v) be an equicharacteristic 0 henselian nontrivially valued field. Then $\mathtt{Th}(K; \mathcal{L}_{val})$ is finitely undecidable.*

Proof. Writing $k = Kv$ and $\Gamma = vK$, by *Theorem 3.3.4* we have $(K, v) \equiv (k((\Gamma)), v_\Gamma)$. By the *Downwards Löwenheim-Skolem Theorem* we may also assume k, Γ are countable. Set v' (on k) to be the trivial valuation; in which case $v = v' \circ v_\Gamma = v_\Gamma$. By *Lemma 3.3.1*, $(R, v_R) = (k(\Gamma), v_\Gamma|_{k(\Gamma)}), (T, v_T) = (k((\Gamma)), v_\Gamma), F = k((\Gamma)) \cap \widetilde{k(\Gamma)}$ satisfy *Assumption* $(\otimes)$.

Let q be prime and consider $(K_q, w = v_\Gamma|_{K_q}) \subset (k((\Gamma)), v_\Gamma)$ arising from the Modified Construction; in particular K_q is an equicharacteristic 0 valued field with residue field k and value group Γ. We will verify the henselianity axioms $\varphi_1, \ldots, \varphi_{q-1}$ are satisfied, where φ_n is

$$\forall a_0, \ldots, a_{n-2} \left(\bigwedge_i a_i \in \mathfrak{m}_v \to \exists x \, [x^n + x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 = 0] \right).$$

Take $l \leq q-1$ and fix $a_0, \ldots, a_{l-2} \in \mathfrak{m}_w$. Suppose $X^l + X^{l-1} + a_{l-2}X^{l-2} + \cdots + a_0 = 0$ has no solution in K_q, and $\alpha \in k((\Gamma)) \setminus K_q$ satisfies this equation. Then $K_q(\alpha)/K_q$ is a finite proper extension. By *Theorem 3.3.6*, $q|[K_q(\alpha) : K_q]$, however $q > l$ and $[K_q(\alpha) : K_q] \leq l$; a contradiction. We conclude that $K_q \models \varphi_l$ for all $l \leq q - 1$; in particular for $n \geq 0$ fixed, $K_q \models \varphi_n$ for all primes $q > n$.

Let $\mathcal{U}$ be a nonprincipal ultrafilter on the set of primes, and let $\mathbb{K}$ be the ultraproduct $\prod_q K_q/\mathcal{U}$. By *Remark 3.3.7 & Łoś' Theorem*, $\mathbb{K}$ is an equicharacteristic 0 henselian valued field with residue field ($\mathcal{L}_r$-elementarily equivalent to) k, and value group ($\mathcal{L}_{oag}$-elementarily equivalent to) Γ. Hence by *Theorem 3.3.4*, $\mathbb{K} \equiv_{\mathcal{L}_{val}} k((\Gamma))$. Thus $\mathbb{K} \models T$ for any finite subtheory $T \subseteq \mathtt{Th}(k((\Gamma)); \mathcal{L}_{val})$, and hence for some prime q, $K_q \models T$. By *Theorem 3.3.6 & Corollary A.10*, $\mathtt{Th}(K_q; \mathcal{L}_{val})$ is hereditarily undecidable, making T undecidable as required. ■

Remark 3.3.9. By *Theorem 3.3.4* if k is a decidable field of characteristic 0, $\mathtt{Th}(k((t)); \mathcal{L}_{val})$ with valuation v_t is decidable. However the theory is *finitely undecidable* by *Corollary 3.3.8*. □

3.4 Henselian Valued Fields: Further Discourse

We may extend the results of the previous section from equicharacteristic 0 henselian valued fields, to mixed characteristic henselian valued fields, using the *standard decomposition*[5]:

Let (K, v) be a valued field of mixed characteristic $(0, p)$ with value group Γ. Define Δ_0 to be the minimal convex subgroup of Γ containing $v(p)$, and Δ_p to be the maximal convex subgroup of Γ not containing $v(p)$. We will consider the valuation(s) $v_0 : K \to \Gamma/\Delta_0$ (resp. $v_p : K \to \Gamma/\Delta_p$) corresponding to the coarsening(s) of v with respect to Δ_0 (resp. Δ_p), and the induced valuation(s) $\hat{v}_0 : Kv_0 \to \Delta_0$ (resp. $\hat{v}_p : Kv_p \to \Delta_p$) with residue field(s) Kv. Also consider $\overline{v_p} : Kv_0 \to \Delta_0/\Delta_p$ with residue field Kv_p; this arises as the coarsening of v_0 with respect to Δ_p (as $\Delta_p < \Delta_0 \leq \Gamma$). These fit together in the following way:

$$\begin{array}{ccccccc} K & \xrightarrow{res_{v_0}} & Kv_0 & \xrightarrow{res_{\overline{v_p}}} & Kv_p & \xrightarrow{res_{\hat{v}_p}} & Kv \\ \downarrow{\scriptstyle v_0} & & \downarrow{\scriptstyle \overline{v_p}} & & \downarrow{\scriptstyle \hat{v}_p} & & \\ \Gamma/\Delta_0 & & \Delta_0/\Delta_p & & \Delta_p & & \end{array}$$

[5]This is the terminology used by Anscombe & Jahnke [AJ19].

$$\begin{array}{ccccc} K & \xrightarrow{res_{v_0}} & Kv_0 & \xrightarrow{res_{\hat{v}_0}} & Kv \\ \downarrow{\scriptstyle v_0} & & \downarrow{\scriptstyle \hat{v}_0} & & \\ \Gamma/\Delta_0 & & \Delta_0 & & \end{array} \qquad \begin{array}{ccccc} K & \xrightarrow{res_{v_p}} & Kv_p & \xrightarrow{res_{\hat{v}_p}} & Kv \\ \downarrow{\scriptstyle v_p} & & \downarrow{\scriptstyle \hat{v}_p} & & \\ \Gamma/\Delta_p & & \Delta_p & & \end{array}$$

If $\Delta_0 = vK$ then by the *Compactness Theorem* there is an elementary extension $(K, v) \prec (K^\flat, v^\flat)$ containing an element $c^\flat$ such that $n \cdot v^\flat(p) < v^\flat(c^\flat) < \infty$ for all $n \geq 0$. Hence the minimal convex subgroup of $v^\flat K^\flat$ containing $v^\flat(p)$ does not contain $v^\flat(c^\flat)$, i.e. $\Delta_0 < v^\flat K^\flat$. As $(K, v) \equiv (K^\flat, v^\flat)$, for the purposes of proving finite undecidability we may assume WLOG $\Delta_0 < vK$. Consider:

Lemma 3.4.1. [AJ19, Lemma 6.5]. *Let T be a theory of bivalued fields (K, v', v) with v' an equicharacteristic 0 henselian coarsening of v, and suppose that T entails complete theories of valued fields (K, v') and $(Kv', \overline{v})$. Then T is complete.* ■

Corollary 3.4.2. *Let (K, v) be a mixed characteristic henselian nontrivially valued field, and v_0 as above. There exists a nontrivial ordered abelian group Ω such that $(K, v_0, v) \equiv (Kv_0((\Omega)), v_\Omega, \widehat{v}_0 \circ v_\Omega)$.*

Proof. Define $\Omega = vK/\Delta_0$. By *Theorem 3.3.4*, $(K, v_0) \equiv (Kv_0((\Omega)), v_\Omega)$. Since $v = \widehat{v}_0 \circ v_0$ in the standard decomposition of (K, v),

$$\begin{aligned} &(Kv_0, \widehat{v}_0) && \text{(residue field of } (K, v_0) \text{ with the induced valuation)} \\ = &(Kv_0, \widehat{v}_0) && \text{(residue field of } (Kv_0((\Omega)), v_\Omega) \text{ with the induced valuation).} \end{aligned}$$

By *Lemma 3.4.1*, we conclude $(K, v_0, v) \equiv (Kv_0((\Omega)), v_\Omega, \widehat{v}_0 \circ v_\Omega)$ as desired. ■

Theorem 3.4.3. *Let (K, v) be a mixed characteristic henselian nontrivially valued field. Then $\mathtt{Th}(K; \mathcal{L}_{val})$ is finitely undecidable.*

Proof. As finite undecidability is a property of $\mathtt{Th}(K; \mathcal{L}_{val})$, by *Corollary 3.4.2* we may assume WLOG $(K, v_0, v) = (Kv_0((\Omega)), v_\Omega, \widehat{v}_0 \circ v_\Omega)$ and furthermore (by the *Downwards Löwenheim-Skolem Theorem*) that Kv_0 and Ω are countable. Let $(T, v_T) =$

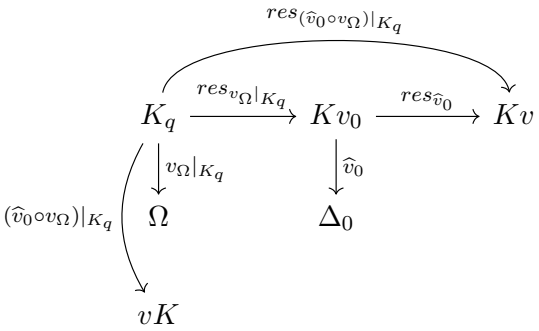
$(Kv_0((\Omega)), \widehat{v}_0 \circ v_\Omega)$, $(R, v_R) = (Kv_0(\Omega), \widehat{v}_0 \circ v_\Omega)$ and $F = T \cap \widetilde{R}$. By *Lemma 3.3.1*, *Assumption* $(\otimes)$ is satisfied: for $q > p$ prime, denote by K_q be the field given by the MODIFIED CONSTRUCTION, with valuation $(\widehat{v}_0 \circ v_\Omega)|_{K_q} = \widehat{v}_0 \circ v_\Omega|_{K_q}$. We have the following diagram of fields:

$$\begin{array}{ccccc}
Kv_0((\Omega)) & \xrightarrow{v_\Omega} & Kv_0 & \xrightarrow{\widehat{v}_0} & Kv \\
| & & \| & & \| \\
K_q & \xrightarrow{v_\Omega} & Kv_0 & \xrightarrow{\widehat{v}_0} & Kv \\
| & & \| & & \| \\
Kv_0(\Omega) & \xrightarrow{v_\Omega} & Kv_0 & \xrightarrow{\widehat{v}_0} & Kv
\end{array}$$

Consider K_q as a multisorted structure:

$$\mathcal{K}_q = (K_q,\, Kv_0,\, Kv,\, \Omega,\, \Delta_0,\, vK;\ res_{v_\Omega|_{K_q}},\, res_{\widehat{v}_0},\, res_{(\widehat{v}_0 \circ v_\Omega)|_{K_q}};\ v_\Omega|_{K_q},\, \widehat{v}_0,\, (\widehat{v}_0 \circ v_\Omega)|_{K_q}),$$

which encompasses the diagram



Let $\mathcal{U}$ be a nonprincipal ultrafilter on the set of primes larger than p, and let $\mathbb{K}$ be the ultraproduct $\prod_{q>p} \mathcal{K}_q/\mathcal{U}$. (We abuse notation to also denote the home sort of $\mathbb{K}$ by $\mathbb{K}$.) We have the following properties of $\mathbb{K}$:

- $\mathbb{K}$ has valuation $\mathfrak{v}_0 = \prod v_\Omega|_{K_q}$ with residue field $\prod_{q>p} Kv_0/\mathcal{U} = Kv_0^{\mathcal{U}}$ and value group $\prod_{q>p} \Omega/\mathcal{U} = \Omega^{\mathcal{U}}$. (This is *Remark 3.3.7.*) Furthermore, $(\mathbb{K}, \mathfrak{v}_0)$ is a *henselian* valued field. Indeed, we claim for $q > p$ prime the henselianity axioms $\varphi_1, \ldots, \varphi_{q-1}$ are satisfied in K_q:

  Let $l < q$ and fix $a_0, \ldots a_{l-2} \in \mathfrak{m}_{v_\Omega|_{K_q}}$. Suppose $X^l + X^{l-1} + a_{l-2}X^{l-2} + \cdots + a_0 = 0$

has no solution in K_q – though there exists a solution $\alpha \in K_q^h$, and $K_q^h \subseteq Kv_0((\Omega))$ by the universal property of henselisations [EP05, Theorem 5.2.2]. Then $K_q(\alpha)/K_q$ is a finite proper separable extension. By *Theorem 3.3.6*, $q|[K_q(\alpha) : K_q]$, however $q > l$ and $[K_q(\alpha) : K_q] \leq l$; a contradiction.

Therefore, by *Łoś' Theorem* (i.e. [CK12, Theorem 4.1.9]) $(\mathbb{K}, \mathfrak{v}_0)$ is a henselian valued field with $\mathfrak{v}_0\mathbb{K} \equiv_{\mathcal{L}_{oag}} \Omega$ and $\mathbb{K}\mathfrak{v}_0 \equiv_{\mathcal{L}_r} Kv_0$. By *Theorem 3.3.4* we conclude $(\mathbb{K}, \mathfrak{v}_0) \equiv (Kv_0((\Omega)), v_\Omega)$.

- $Kv_0^{\mathcal{U}}$ has valuation $\widehat{v}_0^{\mathcal{U}} = \prod \widehat{v}_0$ with residue field $vK^{\mathcal{U}}$ and value group $\Delta_0^{\mathcal{U}}$ (*Remark 3.3.7*). By [CK12, Theorem 4.1.9], $(Kv_0^{\mathcal{U}}, \widehat{v}_0^{\mathcal{U}}) \equiv (Kv_0, \widehat{v}_0)$.

- Hence $\mathbb{K}$ can be equipped with a valuation $\mathfrak{v}_1 := \widehat{v}_0^{\mathcal{U}} \circ \mathfrak{v}_0$, and $\mathfrak{v}_0$ is an equicharacteristic 0 henselian coarsening of $\mathfrak{v}_1$. $\mathbb{K}$ also has a valuation $\mathfrak{v}_2 = \prod(\widehat{v}_0 \circ v_\Omega)|_{K_q}$, and we claim $\mathcal{O}_{\mathfrak{v}_1} = \mathcal{O}_{\mathfrak{v}_2}$, so $(\mathbb{K}, \mathfrak{v}_1) \equiv (\mathbb{K}, \mathfrak{v}_2)$. Indeed,

$$\begin{aligned} x = [(x_q)] \in \mathcal{O}_{\mathfrak{v}_1} &\iff [(x_q)] \in res_{\mathfrak{v}_0}^{-1}(\mathcal{O}_{\widehat{v}_0^{\mathcal{U}}}) \\ &\iff res_{\mathfrak{v}_0}([(x_q)]) = [(res_{v_\Omega|_{K_q}}(x_q))] \in \mathcal{O}_{\widehat{v}_0^{\mathcal{U}}} \\ &\iff \{q : res_{v_\Omega|_{K_q}}(x_q) \in \mathcal{O}_{\widehat{v}_0}\} \in \mathcal{U} \\ &\iff \{q : x_q \in \mathcal{O}_{(\widehat{v}_0 \circ v_\Omega)|_{K_q}}\} \in \mathcal{U} \iff [(x_q)] \in \mathcal{O}_{\mathfrak{v}_2}. \end{aligned}$$

Considering $(\mathbb{K}, \mathfrak{v}_0, \mathfrak{v}_1)$ as a bivalued field, by *Lemma 3.4.1*

$$(\mathbb{K}, \mathfrak{v}_0, \mathfrak{v}_1) \equiv (Kv_0((\Omega)), v_\Omega, \widehat{v}_0 \circ v_\Omega) = (K, v_0, v).$$

Taking a reduct of the language, $(\mathbb{K}, \mathfrak{v}_2) \equiv (\mathbb{K}, \mathfrak{v}_1) \equiv (K, v)$. Therefore if Σ is a finite subtheory of $\mathtt{Th}(K; \mathcal{L}_{val})$, $(\mathbb{K}, \mathfrak{v}_2) \models \Sigma$, and hence for some q sufficiently large, $(K_q, \widehat{v}_0 \circ v_\Omega|_{K_q}) \models \Sigma$. By *Theorem 3.3.6 & Corollary A.10*, $\mathtt{Th}(K_q; \mathcal{L}_{val})$ is hereditarily undecidable, making Σ undecidable as required. ■

What remains is to handle the case of equicharacteristic $p > 0$ henselian nontrivially valued fields. We will show this gap can be eliminated for *NIP* henselian nontrivially

valued fields, as the work of Anscombe & Jahnke [AJ19] gives a useful algebraic classification of such fields ([AJ19, Theorem 5.1]). We will prove:

Theorem 3.4.4. *Let (K, v) be an equicharacteristic $p > 0$ NIP henselian nontrivially valued field. Then $\mathtt{Th}(K; \mathcal{L}_{val})$ is finitely undecidable.*

Corollary 3.4.5. *Assuming the NIP Fields Conjecture, every infinite NIP field is finitely undecidable.*

Proof. Recall *Theorem 3.2.11*, where assuming the *NIP Fields Conjecture* one can conclude every infinite NIP field K is either separably closed (hence finitely undecidable by *Corollaries 3.2.7 & 3.2.8*), real closed (hence finitely undecidable by [Zie82, Corollary 1]), or admits a nontrivial henselian valuation v definable in the language of rings. If K has characteristic 0, it is finitely undecidable by *Corollary 3.3.8* or *Theorem 3.4.3*; if K has positive characteristic, it is finitely undecidable by *Theorem 3.4.4*. ■

To use the classification of Anscombe & Jahnke, we require the following definitions.

Definition 3.4.6. A valued field (K, v) is said to be *(separably) defectless* if whenever L/K is a finite (separable) extension, $[L : K] = \sum_{w \supseteq v} e(w/v) f(w/v)$, where w ranges over all prolongations of v to L, $e(w/v) = (wL : vK)$ is the ramification degree and $f(w/v) = [Lw : Kv]$ is the inertia degree of the valued field extension $(L, w)/(K, v)$.

Definition 3.4.7. A valued field (K, v) of residue characteristic $p > 0$ is *Kaplansky*[6] if vK is p-divisible, and Kv is perfect and admits no proper separable algebraic extensions of degree divisible by p.

Theorem 3.4.8. *Let (K, v) be a positive equicharacteristic NIP henselian nontrivially valued field. Then (K, v) is separably defectless Kaplansky.*

Proof. An immediate consequence of [AJ19, Proposition 3.1]. ■

A corollary of this, noted by Anscombe & Jahnke, is that by [Del81, Théorème 3.1] there is exactly one complete $\mathcal{L}_{val}$-theory of equicharacteristic $p > 0$ henselian

[6] Equivalently ([AJ19, Remark 2.2]) (K, v) of residue characteristic $p > 0$ is Kaplansky if and only if vK is p-divisible and Kv admits no *finite* proper extensions of degree divisible by p.

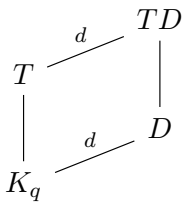
separably defectless valued fields (K, v) of imperfection degree e, with residue field $\mathcal{L}_r$-elementarily equivalent to Kv and value group $\mathcal{L}_{oag}$-elementarily equivalent to vK. (As we are concerned with *finitely axiomatised* subsets of $\mathtt{Th}(K; \mathcal{L}_{val})$, we will assume WLOG $e < \infty$.) The finite undecidability of $\mathtt{Th}(K; \mathcal{L}_{val})$ can be proven by combining ideas from §3.3, as we will see now.

For a valued field (B, v_B) to be separably defectless, it is sufficient for it to satisfy the first-order $\mathcal{L}_{val}$-statements[7] $(\blacklozenge_M)$ for all $M \geq 1$:

> For all finite separable extensions D/B of degree $\leq M$, the equality
>
> $$[D : B] = \sum_{w \supseteq v_B} e(w/v_B) f(w/v_B) \qquad (\blacklozenge_M)$$
>
> holds, where w ranges over all prolongations of v_B to D, $e(w/v_B)$ is the ramification index and $f(w/v_B)$ is the inertia degree.

Lemma 3.4.9. *Fix $M \in \mathbb{N}_{>0}$ and $q > M^M$ prime. Assume (R, v_R), (T, v_T), and F satisfy* Assumption $(\otimes)$ *and let K_q be the field resulting from the* Modified Construction. *If T is separably defectless Kaplansky, then $K_q \models (\blacklozenge_M)$.*

Proof. Let D/K_q be a separable extension of degree $\leq M$. By taking the normal closure may assume D/K_q is Galois and of degree $d \leq M^M$. If D/K_q is proper, by degree reasons $T \cap D = K_q$. Indeed, if $T \supset D' \supset K_q$ is a separable extension of degree $\leq M^M$, by the *Primitive Element Theorem* there exists $\alpha \in T \cap K_q^s$ such that $D' = K_q(\alpha)$. By *Theorem 3.3.6*, if $\alpha \notin K_q$ then $q | [K_q(\alpha) : K_q]$, however $q > M^M$ and $[K_q(\alpha) : K_q] \leq M^M$. This is a contradiction, hence $\alpha \in K_q$. Thus T and D are linearly disjoint over K_q. Consider the following tower of extensions:



[7] The argument of [AJ19, Lemma 2.4] confirms $(\blacklozenge_M)$ is a first-order $\mathcal{L}_{val}$-statement (with "defectless" replaced by "separably defectless", and field extensions made separable where appropriate).

By the tower property ([FJ08, Lemma 2.5.3]), D is linearly disjoint to K_q^h, a subfield of T by the universal property of henselisations. Thus $w = v_T|_{K_q}$ extends uniquely to (D, w'), by e.g. [BK17, Lemma 2.1]. As (T, v_T) is henselian, v_T extends uniquely to (TD, v'_T), and restricts to (D, w'). As T/K_q is immediate, as the valuation extensions are unique, and as T is linearly disjoint from D over K_q,

$$\begin{aligned} p^\nu e(w'/w)f(w'/w) &= [D : K_q] \qquad \text{where } \nu \geq 0, \text{ by [EP05, Theorem 3.3.3]}, \\ &= [TD : T] \qquad \text{by [FJ08, Corollary 2.5.2]}, \\ &= e(v'_T/v_T)f(v'_T/v_T) \qquad \text{as } T \text{ is separably defectless.} \end{aligned}$$

In addition, as T is Kaplansky, $p \nmid e(v'_T/v_T), f(v'_T/v_T)$. Hence

$$[D : K_q] = e(w'/w)f(w'/w) = \sum_{w' \supseteq w} e(w'/w)f(w'/w).$$

We conclude $K_q \models (\blacklozenge_M)$ as desired. ■

We are ready to prove:

Theorem 3.4.4. *Let (K, v) be an equicharacteristic $p > 0$ NIP henselian nontrivially valued field. Then $\mathtt{Th}(K; \mathcal{L}_{val})$ is finitely undecidable.*

Proof. Fix $e \in \mathbb{N}$, the imperfection degree of K. Let k, Γ be countable models of $\mathtt{Th}(Kv; \mathcal{L}_r)$, $\mathtt{Th}(vK; \mathcal{L}_{oag})$. By *Theorem 3.4.8* (K, v) is separably defectless Kaplansky, hence k is perfect and Γ is p-divisible, and thus $k(\Gamma)$ and $k((\Gamma))$ are perfect. By *Lemma 3.3.1* we may choose $t_1, \ldots, t_e \in k((\Gamma))$ transcendental and algebraically independent over $k(\Gamma)$ and consider the field $k(\Gamma)(t_1, \ldots, t_{e-1})$ – by [FJ08, Lemma 2.7.2] its imperfection degree is $e - 1$ exactly. Finally, set $F = k((\Gamma)) \cap (k(\Gamma)(t_1, \ldots, t_{e-1}))^s$. With $(R, v_R) = (k(\Gamma), v_\Gamma)$, $(T, v_T) = (k((\Gamma)), v_\Gamma)$, *Assumption* $(\otimes)$ is satisfied by *Lemma 3.3.1.* Note the imperfection degree of $F(t_e)$ is e exactly, and (T, v_T) is separably defectless Kaplansky.

By *Theorem 3.3.6* there exists a field $K_q \subset k((\Gamma))$ such that if $w = v_\Gamma|_{K_q}$, then

$K_q w = k$, $wK_q = \Gamma$, $\mathbb{F}_p[z]$ is $\mathcal{L}_{val}$-definable in K_q where $z \in k(\Gamma)$ is transcendental over $\mathbb{F}_p$, and if $a \in k((\Gamma))\backslash K_q$ is separably algebraic over K_q, then $q|[K_q(a) : K_q]$. In addition, by the construction of K_q as a union of separable extensions of $F(t_e)$, $[K_q : (K_q)^p] = p^e$. Hence K_q *is an equicharacteristic* p *nontrivially valued field of imperfection degree* e*, with residue field* k *and value group* Γ.

We will verify the henselianity axioms $\varphi_1, \ldots, \varphi_{q-1}$ are satisfied. Let $l < q$ and fix $a_0, \ldots a_{l-2} \in \mathfrak{m}_w$. Suppose $X^l + X^{l-1} + a_{l-2}X^{l-2} + \cdots + a_0 = 0$ has no solution in K_q – though there exists a solution $\alpha \in K_q^h$, and $K_q^h \subseteq k((\Gamma))$ by the universal property of henselisations [EP05, Theorem 5.2.2]. Then $K_q(\alpha)/K_q$ is a finite, proper separable ($K_q^h \subseteq K_q^s$) extension. By *Theorem 3.3.6*, $q|[K_q(\alpha) : K_q]$, however $q > l$ and $[K_q(\alpha) : K_q] \leq l$; a contradiction.

Let Q be the set of primes $q > p$ and $\mathcal{U}$ a nonprincipal ultrafilter on Q. Let $\mathbb{K} = \prod_{q \in Q} K_q/\mathcal{U}$; by *Łoś' Theorem*, $\mathbb{K}$ is an equicharacteristic p henselian nontrivially valued field, of imperfection degree e, and residue field $\mathcal{L}_r$-elementarily equivalent to Kv and value group $\mathcal{L}_{oag}$-elementarily equivalent to vK. Furthermore, $\mathbb{K}$ is separably defectless. Indeed, given $M \in \mathbb{N}_{>0}$, $K_q \models (\blacklozenge_M)$ for all primes $q > M^M$ by *Lemma 3.4.9*. Hence, by *Łoś' Theorem*, $\mathbb{K} \models (\blacklozenge_M)$ for all $M \geq 1$. By [Del81, Théorème 3.1], $\mathbb{K} \equiv_{\mathcal{L}_{val}} K$.

Let Σ be a finite subtheory of $\mathtt{Th}(K; \mathcal{L}_{val})$. As $\mathbb{K} \models \Sigma$, for some $q \in Q$ we have $K_q \models \Sigma$. By *Theorem 3.3.6 & Corollary A.10*, $\mathtt{Th}(K_q; \mathcal{L}_{val})$ is hereditarily undecidable, hence Σ is undecidable as required. ■

Altogether, this chapter shows:

Corollary 3.4.10. *Let* (K, v) *be an equicharacteristic* 0 *or mixed characteristic henselian nontrivially valued field. Then* $\mathtt{Th}(K; \mathcal{L}_{val})$ *is finitely undecidable.*

Let (K, v) *be an equicharacteristic* $p > 0$ *NIP henselian nontrivially valued field. Then* $\mathtt{Th}(K; \mathcal{L}_{val})$ *is finitely undecidable.*

Furthermore, assuming the NIP Fields Conjecture*, every infinite NIP field is finitely undecidable.* ■

3.5 Expansions of *Problem 1.2.5*

We remark briefly here that the pp. 44–46 CONSTRUCTION or the MODIFIED CONSTRUCTION of pp. 53–55 is eligible to be implemented in many 'standard' expansions of the language of rings, such as the language of rings with a derivation, or the languages one commonly considers for valued fields (with a cross section, residue map, etc.), or the language of rings with an automorphism or difference map, etc. Indeed, Ziegler considers this explicitly for the language of ordered rings and the language $\{0, 1, +, \times, \mathcal{O}\}$ of valued fields, in [Zie82]. We suspect the following is possible with Ziegler's construction:

Problem 3.5.1. *Prove the following (in their natural languages) are finitely undecidable:*

- $\mathtt{DCF}_p$*, where* $p = 0$ *or is prime*;
- $\mathtt{ACVF}$;
- $\mathtt{ACFA}$;
- $\mathbb{R}_{\exp}$ *and* $\mathbb{R}_{\mathrm{an}}$.

We could also expand our interest away from fields:

Problem 3.5.2. *Does there exist an infinite, finitely axiomatisable* ring*? Is every infinite* ring *finitely undecidable?*

For example, immediately from the interpretations of $\mathbb{N}$ in $\mathbb{Z}$ and $\mathbb{F}_p[t]$ (see *Appendix A*), $\mathtt{Th}(\mathbb{Z}; \mathcal{L}_r)$ and $\mathtt{Th}(\mathbb{F}_p[t]; \mathcal{L}_r(t))$ are finitely undecidable. (In fact, $\mathtt{Th}(\mathbb{F}_p[t]; \mathcal{L}_r)$ is finitely undecidable, by *Lemma A.9.*) Furthermore, $\mathtt{Th}(\mathcal{O}_k; \mathcal{L}_r)$ is finitely undecidable for any global field k. Indeed, when k is a number field, $\mathbb{Z}$ is $\mathcal{L}_r$-definable in $\mathcal{O}_k$ (due to J. Robinson [Rob59]) hence any finite subtheory of $\mathtt{Th}(\mathcal{O}_k; \mathcal{L}_r)$ is undecidable by a minor modification to *Corollary A.10.* When k is a global function field, arithmetic is interpretable in k (due to Rumely [Rum80]) and the same conclusion follows. To give another example: in [Rob62], J. Robinson proves $\mathbb{N}$ is $\mathcal{L}_r$-definable in $\mathcal{O}_{\mathbb{Q}^{tr}}$, where $\mathbb{Q}^{tr}$ is the theory of totally real algebraic numbers (see §4.2) – hence $\mathtt{Th}(\mathcal{O}_{\mathbb{Q}^{tr}}; \mathcal{L}_r)$ is finitely undecidable too.

One could also ask about the finite undecidability of structures equipped with reducts of the ring language – for example, Presburger arithmetic (namely $\mathtt{Th}(\mathbb{N}; 0, +)$, see e.g. [Haa18] and references therein) or Skolem arithmetic (namely $\mathtt{Th}(\mathbb{N}; 1, \times)$, see e.g. Cegielski [Ceg81] and Stonestrom [Sto21]). The author is unaware of finite (or hereditary) undecidability results for these theories.

Chapter 4

Finite Undecidability II: Pseudo-Closedness

The previous chapter discussed some fields that were "closed" in an algebraic or existential way, in some ring language. In this section we will tackle the corresponding more general "pseudo-closed" field structures, using a different method suggested by E. Hrushovski. Considering *pseudo-algebraically closed* (PAC) fields, as we do next, is quite natural from a classification theoretic standpoint. Indeed, recall the definition of a *simple* theory (introduced by Shelah [She80], expounded upon in [Wag00], defined in §1.3.1). We have the following folkloric conjecture:

Conjecture (Simple Fields). *Every infinite simple field is PAC.* ■

By 2019, according to Halevi et. al. [HHJ19, p. 182] "little (if any) progress has been made" on this conjecture, though Duret [Dur80] has shown that the *Simple Fields Conjecture* implies the *Stable Fields Conjecture* through the fact that a PAC field is stable if and only if it is separably closed (cf. [Dur80, Corollaire 6.5]). Therefore, moving out of the NIP field context, *PAC fields* are the next natural class of fields to tackle.

For the main undecidability results of this chapter, we assume the reader is familiar with *Appendix A*.

4.1 Pseudo-Algebraically Closed Fields

A field K is *pseudo-algebraically closed* if every geometrically irreducible variety over K has K-rational points. The idea behind this section is ultimately the adaptation of the undecidability of the theory of (perfect) PAC fields, due to Cherlin, van den Dries & Macintyre [CvdDM80] and independently Ershov [Ers81]. The key to this proof was, given an arbitrary nontrivial (by which we mean the vertex set is nonempty) graph Γ to construct a (perfect) PAC field interpreting Γ (in the sense of *Definition A.2*), as the theory of all such graphs is known to be hereditarily undecidable (see *Appendix A*). This construction was achieved by designing machinery to encode graphs into projective profinite groups, which are the absolute Galois groups of (perfect) PAC fields exactly.

Clearly we need apparatus to discuss profinite groups in a first-order setting. Simply considering them with the language of groups will not suffice; more information about the structure can be obtained by viewing a profinite group as an inverse limit of finite groups – and there is a "standard method... for making a (category-theoretic) diagram of first-order structures into a first-order structure" [CvdDM80, p. 14]. To this end (and following the presentation of [Cha02, §5.1]) for a profinite group G we consider a structure $S(G)$ whose underlying set is $\bigsqcup_{N\in\mathcal{N}} G/N$, where $\mathcal{N}$ is the family of open normal subgroups of G. The elements of G/N are denoted by gN, for $g \in G$. $S(G)$ is a structure in the ω-sorted language $\mathcal{L}_G = \{\leq, C, P\}$, whose sorts are indexed by positive natural numbers n and where $\leq, C$ are binary relations and P is a ternary relation, as follows: the elements of $S(G)$ of sort n are precisely those gN where $N \in \mathcal{N}$ and $[G : N] \leq n$. We say $gN \leq hM$ if and only if $N \subseteq M$, and $C(gN, hM)$ if and only if $N \subseteq M$ & $gM = hM$. Finally $P(g_1N_1, g_2N_2, g_3N_3)$ if and only if $N_1 = N_2 = N_3$ & $g_1g_2N_1 = g_3N_1$.

Clearly the sorts are nested with "$\leq$" indicating an order between the sorts. The relation "C" captures the projection maps $\pi_{N,M} : G/N \to G/M$ for $N, M \in \mathcal{N}$ with $N \subseteq M$, and "P" captures the group operation on G/N. The $\mathcal{L}_G$-structure $S(G)$ encodes the inverse system $\{(G/N, \pi_{N,M}) : N, M \in \mathcal{N},\ N \subseteq M\}$ precisely and hence determines G uniquely, as $G = \varprojlim G/N$. $S(G)$ is the *complete inverse system associated*

to G.

By [Cha02, pp. 979–980], the class of $\mathcal{L}_G$-structures of the form $S(G)$ for some profinite group G is axiomatisable in the class of all such structures. Suppose T_G denotes this collection of axioms. There is a duality between the category of profinite groups with continuous epimorphisms, and the category of $\mathcal{L}_G$-structures modelling T_G with $\mathcal{L}_G$-embeddings (*p. 980 ibid.*)

When $G = G_K = \mathrm{Gal}(K^s/K)$ is the absolute Galois group of a field K, this inverse system takes on a new light. Indeed, $S(G_K) = \bigsqcup \mathrm{Gal}(L/K)$ is the union over finite Galois extensions of K. The group epimorphisms encoded by C now correspond to the restriction maps $\mathrm{res} : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ (for when $K \subseteq L \subseteq M$). If K/E is *regular* (that is to say, E is separably algebraically closed in K and K/E is separable), then the corresponding map of absolute Galois groups $\pi : G_K \twoheadrightarrow G_E$ is surjective, hence $\iota : S(G_E) \hookrightarrow S(G_K)$ by $\iota(N) = \pi^{-1}(N)$, where N is an open normal subgroup of G_E.

In this language we will only consider *bounded* formulae and sentences, i.e. variables x have a prescribed sort, and quantification over x ranges over the variable's sort. E.g. if x is of sort n, "$\exists x$" is "there exists x of sort n". The theory $\mathtt{Th}(S(G); \mathcal{L}_G)$ is known as the *cotheory* of G. After reconstructing the basic tenants of model theory as "comodel theory" for profinite groups in this setting, Cherlin, van den Dries & Macintyre indicate the following results:

Theorem 4.1.1. *Let K, L be fields with common subfield E, such that K/E & L/E are regular. If $K \equiv_E L$ then $S(G_K) \equiv_{S(G_E)} S(G_L)$.*
There is a recursive *'translation' map $-^* : Sent(\mathcal{L}_G) \to Sent(\mathcal{L}_r)$ such that if φ is a $\mathcal{L}_G$-sentence, then $S(G_K) \models \varphi \iff K \models \varphi^*$, for any field K.*
Furthermore, let $\psi(\overline{x})$ be a $\mathcal{L}_G$-formula. Then there is a $\mathcal{L}_r$-formula $\psi^*(\overline{y})$ such that for a tuple $\overline{a}$ of the right sorts in $S(G_K)$, we have

$$(S(G_K), \overline{a}) \models \psi \quad \iff \quad (K, \overline{b}) \models \psi^*,$$

where $\overline{b} \in K$ encodes $\overline{a} \in S(G_K)$ in a suitable way.

Proof. For the former two, see [Cha02, Theorem 5.9 (1) & (2)] (though *loc. cit.* does not claim $-^*$ is *recursive*. This is clarified and proven in [Feh17, Appendix C]; see *Corollary C.10 ibid.* specifically).

For the latter, (whose phrasing is taken from [Dit18, Theorem 6.1.1], gathering all tuples into one), see [Cha02, Theorem 5.9 (3)] and [Feh17, Lemma C.8]. ■

Corollary 4.1.2. [CvdDM80]; [Cha02, Theorem 5.13]. *Let K_1, K_2 be PAC fields, separable over a common subfield E. Then $K_1 \equiv_E K_2$ if and only if K_1 and K_2 have the same degree of imperfection, there exists $\theta \in G_E$ such that $\theta(K_1 \cap E^s) = K_2 \cap E^s$, and if $S\Theta : S(G_{K_1 \cap E^s}) \to S(G_{K_2 \cap E^s})$ is the isomorphism induced by θ, then the partial map $S\Theta : S(G_{K_1}) \to S(G_{K_2})$ with domain $S(G_{K_1 \cap E^s})$ is $\mathcal{L}_G$-elementary.* ■

As Cherlin, van den Dries & Macintyre remark: the existence of such a map Θ is a *global* condition on the field, and can be replaced with suitable *local* satisfiability conditions ([CvdDM80, Corollary 37]).

Thus, the theory of a (perfect) PAC field K is completely determined by some 'algebraic part' of its theory and the 'cotheory' (with suitable constants) of its absolute Galois group G_K (which, by *Theorem 4.1.1*, is "seen" in K). This leads to a nice transfer of properties: if K is $\aleph_1$-saturated, so too is $S(G_K)$ ([Feh17, Corollary C.11]); if K is decidable, so too is $S(G_K)$; if K is stable, so too is $S(G_K)$ (both as consequences of *Theorem 4.1.1*). Note the important implications of the contrapositive of these statements.

Suppose K is a PAC field with prime subfield $\mathbb{F}$. Define $K_0 = K \cap \widetilde{\mathbb{F}}$; note K/K_0 is regular, hence there is an epimorphism $G_K \twoheadrightarrow G_{K_0}$ and thus an embedding $S(G_{K_0}) \hookrightarrow S(G_K)$. In the style of Koenigsmann [Koe16b], denote by $\mathtt{Th}^{alg}(K)$ the subset of $\mathtt{Th}(K; \mathcal{L}_r)$ given by dictating which monic irreducible one variable polynomials over $\mathbb{F}$ do and do not have a root in K (see [Koe16b, p. 935]; note $\mathtt{Th}^{alg}(K) \subseteq \mathtt{Th}(K_0; \mathcal{L}_r)$ but equality does not, in general, hold). We have the following corollary to *Corollary 4.1.2*:

Remark 4.1.3. By $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$ below we mean the set of $\mathcal{L}_r(K_0)$-sentences obtained from the recursive translation map $-^*$ of *Theorem 4.1.1.* Indeed, let $\varphi \in \mathrm{Form}(\mathcal{L}_G)$, $\overline{a} \in S(G_{K_0})$, and $S(G_K) \models \varphi(\overline{a})$. Let $\overline{b} \in K_0$ encode $\overline{a} \in S(G_{K_0})$ (by which we mean they are *compatible* in the sense of [Feh17, Definition C.5]); then $K \models \varphi^*(\overline{b})$ (this is [Feh17, Proposition C.9]) and $\varphi^*(\overline{b}) \in \mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$. □

Corollary 4.1.4. *A PAC field K is axiomatised by the following first-order $\mathcal{L}_r$-axiom scheme:*

(1) The characteristic and degree of imperfection of K;

(2) The PAC field axioms, denoted PAC*;*

(3) $\mathtt{Th}^{alg}(K)$*;*

(4) $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$. ■

A result of van den Dries & Lubotzky [vdDL81, §4.8, Proposition] describes a correspondence between projective profinite groups and (perfect) PAC fields, via their absolute Galois groups. We would like to use the following improvement:

Theorem 4.1.5. *Let L/K be a Galois extension, G a projective profinite group, and $\alpha : G \to \mathrm{Gal}(L/K)$ an epimorphism. Then K has an extension E with arbitrary degree of imperfection that is PAC, $E \cap L = K$, and there exists an isomorphism $\gamma : G_E \to G$ such that $\alpha \circ \gamma = res_L$.*

Proof. [FJ08, Theorem 23.1.1]; cf. [CvdDM80, Proposition 38]. ■

We will be able to use this theorem after the next definition, concerning families of finite groups. Such families are important to classify, as a sufficiently 'nice' family of groups will give rise to a 'nice' profinite group via an inverse limit, as we shall see in *Theorem 4.1.7.*

Definition 4.1.6. Let $\mathcal{C}$ be a family of finite groups containing the trivial group. We call $\mathcal{C}$ a *formation* if it satisfies the following two properties (see [FJ08, §17.3]):

(1) If $G \in \mathcal{C}$ and $\overline{G}$ is a homomorphic image of G, then $\overline{G} \in \mathcal{C}$.

(2) Let G be a finite group, $N_1, N_2 \triangleleft G$, $N_1 \cap N_2 = \{1\}$, and $G/N_1, G/N_2 \in \mathcal{C}$. Then $G \in \mathcal{C}$.

We call $\mathcal{C}$ a *full formation* if it satisfies the following properties:

(1*) Let $1 \to N \to G \to \overline{G} \to 1$ be a short exact sequence of finite groups. Then $G \in \mathcal{C}$ if and only if $N, \overline{G} \in \mathcal{C}$.

(2*) If $G \in \mathcal{C}$ and $H \leq G$, then $H \in \mathcal{C}$.

In particular, note that (1*) $\implies$ (1), (2) (and see [FJ08, §17.3]). Examples of full formations include the family of all finite groups, the family of all finite p-groups for any prime p, and the family of all solvable groups.

We now have the tools to complete the following, outlined to the author by E. Hrushovski:

Theorem 4.1.7. *No PAC field is finitely axiomatisable (even among the class of PAC fields of the same characteristic and degree of imperfection).*

This is to say that, given a PAC field L, there does not exist an $\mathcal{L}_r$-sentence γ such that for all PAC fields F of the same characteristic and degree of imperfection as L, $F \models \gamma \iff F \equiv_{\mathcal{L}_r} L$.

Proof. Assume for the purpose of contradiction there exists a finitely axiomatisable PAC field K; in particular, by *Corollary 4.1.4* to characterise K among all PAC fields of the same characteristic and degree of imperfection, we need only finite many axioms $\Sigma_1 \subset \mathtt{Th}^{alg}(K)$, $\Sigma_2^* \subset \mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$ (where $\Sigma_2 \subset \mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))$ is finite).

Let Λ be the set of universal sentences of Σ_1; Λ specifies the monic irreducible univariate polynomials over $\mathbb{F}$ (the prime subfield) in Σ_1 which *do not* have a root in K. Let K_{bad} be the join of minimal Galois extensions F/K with $F \models \neg\lambda$ for $\lambda \in \Lambda$. Then K_{bad}/K is finite, $K_{\text{bad}} \models \neg\Lambda$, and $\text{Gal}(K_{\text{bad}}/K)$ is a quotient of G_K. As

there is an epimorphism $G_K \twoheadrightarrow \mathrm{Gal}(K_{\mathrm{bad}}/K)$, there is an embedding of $\mathcal{L}_G$-structures $S(\mathrm{Gal}(K_{\mathrm{bad}}/K)) \hookrightarrow S(G_K)$.

Let $\overline{a} \in S(G_{K_0}) \subset S(G_K)$ be a finite tuple of elements such that Σ_2 is a set of (finitely many) $\mathcal{L}_G(\overline{a})$-sentences. Fix $n_k \in \mathbb{N}$ such that $S_1, \ldots, S_{n_k}$ is the smallest consecutive sequence of sorts involving the sentences of Σ_2. (Each sentence φ has finitely many occurrences of the symbols $\leq, C, P$, finitely many constant symbols, and finitely many bounded variables. Hence there exists $n_\varphi \in \mathbb{N}$ such that the $\mathcal{L}_G(\overline{a})$-symbols and variables occurring in φ occur at the sorts $S_1, \ldots, S_{n_\varphi}$.) Let $\widehat{p}$ be the smallest prime larger than $n_k + |\mathrm{Gal}(K_{\mathrm{bad}}/K)|$, P the set of primes $\{2, 3, \ldots, \widehat{p}\}$, and $\mathcal{C}$ the formation of finite groups whose order is necessarily a product of powers of primes of P (including trivial powers). As this formation is full, and G_K is projective, the maximal pro-$\mathcal{C}$ quotient of G_K (denoted G_P) is also projective ([FJ08, Proposition 22.4.8]).

Consider $S(G_P)$ as $\mathcal{L}_G$-structure: it may be expanded to an $\mathcal{L}_G(\overline{a})$-structure. Indeed, for $a_i \in \overline{a}$, let $g_i N_i$ be the interpretation of a_i in $S(G_K)$, where $g_i N_i \in G_K/N_i$ is of sort n_i, $N_i \triangleleft S(G_K)$. By design, $n_i \leq \widehat{p}$ and there exists $N_i' \triangleleft G_P$ with $\psi_i : G_K/N_i \xrightarrow{\cong} G_P/N_i'$ by the *Isomorphism Theorems for Compact Groups* [FJ08, p. 5]. Define the interpretation of a_i in $S(G_P)$ to be $\psi_i(g_i N_i)$.

In fact, there is a correspondence between closed $N_k \triangleleft G_K$ of index $k \leq \widehat{p}$, and closed $N_k' \triangleleft G_P$ of index $k \leq \widehat{p}$, with $G_K/N_k \cong G_P/N_k'$, by [Rot99, Theorem 2.28(ii)] (note the quotient map $G_K \twoheadrightarrow G_P$ is continuous, so Rotman's proof holds for *closed* subgroups). Therefore if φ is a sentence of Σ_2, $S(G_P) \models \varphi$, as $S(G_K) \models \varphi$ and the $\mathcal{L}_G(\overline{a})$-symbols and variables of φ occur in the sorts $S_1, \ldots, S_{\widehat{p}}$. Moreover, by construction $\mathrm{Gal}(K_{\mathrm{bad}}/K)$ is up to isomorphism a quotient of G_P, hence there is an epimorphism $G_P \twoheadrightarrow \mathrm{Gal}(K_{\mathrm{bad}}/K)$.

Let $\mathbb{F}_1(q)$ be the free pro-q group on one generator, where q is a prime larger than $\widehat{p}$. Finally, let $G_P \star \mathbb{F}_1(q)$ be the free product[1] of G_P and $\mathbb{F}_1(q)$. By [FJ08, Proposition 22.4.10], $G_P \star \mathbb{F}_1(q)$ is a projective profinite group. The $\mathcal{L}_G$-theories of $G_P \star \mathbb{F}_1(q)$ and G_P clearly differ; there is an epimorphism from $G_P \star \mathbb{F}_1(q)$ to $\mathbb{Z}/q\mathbb{Z}$, however no such epimorphism from G_P exists by construction. However $S(G_P \star \mathbb{F}_1(q)) \models \Sigma_2$: if

[1] The coproduct in the category of profinite groups. In [FJ08, Lemma 22.4.9] it is proven this is the profinite completion of the free product $\mathbb{G}$ of abstract groups $G_P, \mathbb{F}_1(q)$, with respect to the collection of $N \triangleleft \mathbb{G}$ of finite index, such that $N \cap G_P$ is open in G_P and $N \cap \mathbb{F}_1(q)$ is open in $\mathbb{F}_1(q)$.

$N_i \triangleleft G_P \star \mathbb{F}_1(q)$ is of index $\leq \widehat{p}$, under the projection $G_P \star \mathbb{F}_1(q) \twoheadrightarrow G_P \star \mathbb{F}_1(q)/N_i$ we must have $\mathbb{F}_1(q) \leq N_i$, as otherwise $\mathbb{F}_1(q)$ would have a proper normal subgroup of index $\leq \widehat{p}$. (This is a contradiction, as $\mathbb{F}_1(q)$ is pro-q and $\widehat{p} < q$.) By [Rot99, Theorem 2.28(ii)] there is a correspondence between closed $N_k \triangleleft G_P \star \mathbb{F}_1(q)$ of index $k \leq \widehat{p}$, and closed $N_k' \triangleleft G_P$ of index $k \leq \widehat{p}$, with $G_P \star \mathbb{F}_1(q)/N_k \cong G_P/N_k'$, (again note the quotient map[2] $G_P \star \mathbb{F}_1(q) \twoheadrightarrow G_P \star \mathbb{F}_1(q)/\langle \mathbb{F}_1(q) \rangle \cong G_P$ is continuous, so Rotman's proof holds for closed subgroups). Hence for any $\mathcal{L}_G(\overline{a})$-sentence φ with variables over the sorts $S_1, \ldots, S_{\widehat{p}}$, $S(G_P) \models \varphi \Leftrightarrow S(G_P \star \mathbb{F}_1(q)) \models \varphi$. We conclude $S(G_P), S(G_P \star \mathbb{F}_1(q)) \models \Sigma_2$.

By *Theorem 4.1.5* there exist PAC fields $F_1, F_2 \supseteq K$ such that $G_{F_1} \cong G_P$, $G_{F_2} \cong G_P \star \mathbb{F}_1(q)$, and $F_1 \cap K_{\text{bad}} = F_2 \cap K_{\text{bad}} = K$. We conclude that $F_1, F_2 \models \Sigma_1 \cup \Sigma_2^*$, however $F_1 \not\equiv F_2$ as $S(G_{F_1}) \not\equiv_{\mathcal{L}_G} S(G_{F_2})$; a contradiction as required. ■

Remark 4.1.8. *Cultural Remark.* As mentioned previously, the undecidability of the theory of PAC fields is due to Cherlin, van den Dries & Macintyre [CvdDM80] and, independently, Ershov [Ers81]. Ershov proved this result explicitly for characteristic 0 PAC fields (though was probably aware of its truth in more generality). Fried & Jarden [FJ08, Chapter 28] present these results for *perfect* PAC fields, as historically PAC fields were typically taken as perfect. Cherlin, van den Dries & Macintyre remark "[their undecidability statement] remains true if we prescribe characteristic and any degree of imperfectness compatible with the characteristic" [CvdDM80, p. 93]. Going forward, we will not assume perfectness. □

Both sets of mathematicians used the characterisation of the absolute Galois groups of (perfect) PAC fields as projective profinite groups to encode the theory of nontrivial graphs into the theory of such PAC field structures. Both proofs have been combined and presented by Fried & Jarden [FJ08, Chapter 28] and it is this proof we will reference. Note that, as Ershov remarks, this proof technique demonstrated already the hereditary undecidability of the theory of perfect PAC fields ([Ers81, p. 260]). We are

[2]For notation, recall §1.3.

aiming for something more general: that every finite subtheory of *any given* PAC field is undecidable.

As has already been mentioned, these proofs require a correspondence between graphs and profinite groups. In [FJ08, §28.6 – §28.8] it is outlined precisely how one can assign a graph Γ_G to every profinite group G using two finite groups as parameters (denoted D and W): we present this assignment now. This will be referenced in §4.2 & §4.3.

Construction 4.1.9. Given a profinite group G, define the graph $\Gamma_G = (A_G, R_G)$ where the set of vertices A_G is the set of open $N \triangleleft G$ such that $G/N \cong D$, and the edge relation R_G is the set of pairs $(N_1, N_2) \in A_G \times A_G$ such that $N_1 N_2 = G$ and there exists an open $M \triangleleft G$ such that $M \leq N_1 \cap N_2$ and $G/M \cong W$. Furthermore, there are conditions on the finite groups D and $W = U \rtimes (D \times D)$ that guarantee the surjectivity of the map $G \mapsto \Gamma_G$, known by Fried & Jarden as *the graph conditions*. They are (from [FJ08, Definition 28.7.2]):

(G1) D, U have no composition factors in common.

(G2) For each finite set I and epimorphism $\pi : D^I \to D$, there exists $i \in I$ such that $\ker(\pi) = \ker(\pi_i)$, where π_i is the projection map to the ith coordinate of D^I.

(G3) The intersection of all maximal subgroups of W is trivial, as is the intersection of all maximal subgroups of D.

(G4) For each embedding $\theta' : D \times D \to W$ as a semidirect complement (i.e. $U \cdot \theta'(D \times D) = W$, and $U \cap \theta'(D \times D) = 1$) and for each nontrivial $N \triangleleft U$, neither factor $D_1 = D \times \{1\}$, $D_2 = \{1\} \times D$ acts trivially via conjugation on N through θ'.[3]

Suppose D, W satisfy these conditions and are in a split short exact sequence:

$$1 \longrightarrow U \longrightarrow W \underset{\theta}{\overset{\lambda}{\rightleftarrows}} D \times D \longrightarrow 1.$$

[3]This is to say there exists $\eta \in N$, $d \in D_1 \cup D_2$ such that $\eta^{\theta'(d)} = \theta'(d) \cdot \eta \cdot \theta'(d)^{-1} \neq \eta$.

Following the notation of [FJ08, §28.8], let $\Gamma = (A, R)$ and consider the profinite group $D^A \times W^R$ and the canonical coordinate projections

$$\begin{aligned}
&\pi_A : D^A \times W^R \to D^A; && \pi_A(\overline{d}, \overline{w}) = \overline{d};\\
&\pi_a : D^A \times W^R \to D; && \pi_a(\overline{d}, \overline{w}) = d_a \quad \text{for } a \in A;\\
&\pi_r : D^A \times W^R \to W; && \pi_r(\overline{d}, \overline{w}) = w_r \quad \text{for } r \in R;
\end{aligned}$$

Define $G_\Gamma := \{(\overline{d}, \overline{w}) \in D^A \times W^R : r = (a, b) \in R \Rightarrow \lambda(w_r) = (d_a, d_b)\}$. This is a closed subgroup of $D^A \times W^R$, hence is profinite. The graphs Γ, Γ_{G_Γ} are indeed isomorphic ([FJ08, Proposition 28.8.3]), and

$$1 \longrightarrow U^R \longrightarrow G_\Gamma \xrightarrow{\pi_A|_{G_\Gamma}} D^A \longrightarrow 1$$

is a split short exact sequence ([FJ08, Lemmas 28.8.1 & 28.8.2]). ■

Definition 4.1.10. Let K be a field. Define the graph $\Gamma_K = (A_K, R_K)$ by

$$\begin{aligned}
A_K &= \{L : L/K \text{ is Galois and } \mathrm{Gal}(L/K) \cong D\},\\
R_K &= \{(L_1, L_2) \in A_K \times A_K : L_1 \cap L_2 = K \text{ and } \exists N/K \text{ Galois s.t.}\\
&\qquad\qquad L_1 L_2 \subseteq N \text{ and } \mathrm{Gal}(N/K) \cong W\}.
\end{aligned}$$

(Recall D, W are some fixed finite groups satisfying (G1)–(G4) of *Construction 4.1.9.*)

Through the map $L \mapsto G_L$ we see Γ_K and Γ_{G_K} are isomorphic. We will now argue that K can 'see' Γ_K, through encoding finite Galois extensions $K \subset L \subset K^s$, within a fixed separable closure K^s. We assume familiarity with *Appendix A.1.*

Construction 4.1.11. [FJ08, pp. 694–695]. For $l \in \mathbb{Z}_{>0}$ let $f_{\overline{x}}(T) = T^l + x_1 T^{l-1} + \cdots + x_l$, and if $\overline{a} \in K^l$, denote the splitting field of $f_{\overline{a}}(T)$ over K by $K_{\overline{a}}$. Let H be a finite group, and $\alpha_{l,H}(\overline{x})$ be an $\mathcal{L}_r$-formula such that, for $\overline{a} \in K^l$,

$$K \models \alpha_{l,H}(\overline{a}) \iff f_{\overline{a}}(T) \text{ is separable and } \mathrm{Gal}(K_{\overline{a}}/K) \cong H.$$

Using this and a finite group E, with $l = |H|$ one may construct an $\mathcal{L}_r$-formula $\rho_{H,E}$ such that for $\overline{b}, \overline{c} \in K^l$,

$$K \models \rho_{H,E}(\overline{b}, \overline{c}) \iff K_{\overline{b}} \cap K_{\overline{c}} = K,\ K \models \alpha_{|H|,H}(\overline{b}) \wedge \alpha_{|H|,H}(\overline{c}), \text{ and}$$
$$K \models \exists \overline{z}\,(\alpha_{|E|,E}(\overline{z}) \wedge \text{“}K_{\overline{b}} \subseteq K_{\overline{z}}\text{”} \wedge \text{“}K_{\overline{c}} \subseteq K_{\overline{z}}\text{”}).$$

We may then define a recursive translation map $-' : \mathrm{Form}(\mathcal{L}_{gr}) \to \mathrm{Form}(\mathcal{L}_r)$; $\phi \mapsto \phi'$ by the following rules:

- $R(X,Y) \mapsto (R(X,Y))' = \rho_{H,E}(\overline{x}, \overline{y})$;
- $\neg\varphi \mapsto \neg(\varphi')$;
- $\varphi_1 \wedge \varphi_2 \mapsto (\varphi_1') \wedge (\varphi_2')$;
- $\exists x(\varphi) \mapsto \exists \overline{x}\,(\alpha_{|H|,H}(\overline{x}) \wedge \varphi'(\overline{x}))$. □

Lemma 4.1.12. *Let K be a field; Γ_K is interpretable in K.*

Proof. Recalling *Definition A.2*, set $\mathcal{L}_1 = \mathcal{L}_r$, $\mathcal{L}_0 = \mathcal{L}_{gr}$, $n = |D|$, $\delta(\overline{x}) = \alpha_{n,D}(\overline{x})$, and $f : \alpha_{n,D}(K^n) \to \Gamma_K$; $\overline{a} \mapsto K_{\overline{a}}$. This is indeed surjective, as if L/K is Galois with $\mathrm{Gal}(L/K) \cong D$, it is the splitting field of a degree $n = |D|$ monic separable polynomial $f_{\overline{a}}(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ over K, and hence $K \models \alpha_{n,D}(\overline{a})$.

Note *Definition A.2 (2)* is satisfied by *Construction 4.1.11* with $E = W$, and condition (†) is confirmed in [FJ08, p. 695]. ■

Remark 4.1.13. Notice the above interpretation is *uniform* in the sense that the $\mathcal{L}_r$-formula $\alpha_{n,D}(\overline{x})$ and the map $-' : \mathrm{Form}(\mathcal{L}_{gr}) \to \mathrm{Form}(\mathcal{L}_r)$ of *Construction 4.1.11* do not depend on K or Γ_K. □

Now, let K be a PAC field and $\Sigma \subset \mathtt{Th}(K; \mathcal{L}_r)$ a finite subtheory. We shall eventually prove:

Theorem 4.1.14. *For any nontrivial graph* Γ *there exists a PAC field* $K_\Gamma \supseteq K$ *such that* $K_\Gamma \models \Sigma$ *and* $\Gamma_{K_\Gamma} \cong \Gamma$.

Before this, some definitions.

Definition 4.1.15. Let G be a profinite group. The intersection of all maximal open subgroups of G is a normal closed subgroup of G called the *Frattini group of* G and denoted $\Phi(G)$.

Fried & Jarden remark that under the operation $G \mapsto \Phi(G)$, there are "functorial properties" [FJ08, p. 498], e.g. if $N \lhd G$ is closed, $\Phi(N) \leq \Phi(G)$, or if $\theta : H \to G$ is an epimorphism of profinite groups, $\theta(\Phi(H)) \leq \Phi(G)$. See [FJ08, §22.1] for more information.

Definition 4.1.16. A homomorphism of profinite groups $\varphi : H \to G$ is a *Frattini cover*[4] if φ is surjective and $\ker(\varphi) \leq \Phi(H)$.

Note that as φ maps the set of all maximal open subgroups of H onto the set of all maximal open subgroups of G, $\varphi(\Phi(H)) = \Phi(G)$. There are various other properties of such maps, e.g. they preserve the rank of a group (see [FJ08, §22.5]).

Given a profinite group G, one can partially order the epimorphisms of profinite groups onto G: i.e. if $\theta_i : H_i \to G$ for $i = 1, 2$ are epimorphisms, θ_2 is *larger* than θ_1 if there is an epimorphism $\theta : H_2 \to H_1$ such that $\theta_1 \circ \theta = \theta_2$. As we will consider mainly projective groups, we shall be interested in *universal* Frattini covers that satisfy the following proposition:

Proposition 4.1.17. [FJ08, Proposition 22.6.1]. *Every profinite group* G *has an associated projective group*[5] $\widetilde{G}$ *and a Frattini cover* $\widetilde{\varphi} : \widetilde{G} \to G$*, unique up to isomorphism, called the* universal Frattini cover*, satisfying the following equivalent conditions:*

- $\widetilde{\varphi}$ *is the largest Frattini cover of* G*;*
- *if* $\widetilde{G}'$ *is a projective profinite group and* $\lambda : \widetilde{G}' \twoheadrightarrow G$ *is an epimorphism, then* λ *is larger than* $\widetilde{\varphi}$*.* ■

[4] Another name used for an epimorphism of profinite groups is a *cover*, hence the terminology.
[5] Sometimes known as the *Frattini hull of* G.

This concludes the pouring of the foundations; we are ready to begin construction. Recall K is a PAC field with Σ a finite subtheory of $\mathtt{Th}(K;\mathcal{L}_r)$. To prove *Theorem 4.1.14*, finding parameters $D_\Sigma, U_\Sigma, W_\Sigma$ such that the Fried-Jarden graph machinery still operates correctly, and does not 'interfere' with the part of the absolute Galois group of K axiomatised by Σ, will be the crucial step. Recall we require D_Σ and $W_\Sigma = U_\Sigma \rtimes (D_\Sigma \times D_\Sigma)$ to be finite groups with the following properties:

(G1) D_Σ, U_Σ have no composition factors in common.

(G2) For each finite set I and epimorphism $\pi : D_\Sigma^I \to D_\Sigma$, there exists $i \in I$ such that $\ker(\pi) = \ker(\pi_i)$, where π_i is the projection map to the ith coordinate of D_Σ^I.

(G3) $\Phi(W_\Sigma) = \Phi(D_\Sigma) = 1$.

(G4) For each embedding $\theta' : D_\Sigma \times D_\Sigma \to W_\Sigma$ as a semidirect complement (i.e. $U_\Sigma \cdot \theta'(D_\Sigma \times D_\Sigma) = W_\Sigma$, and $U_\Sigma \cap \theta'(D_\Sigma \times D_\Sigma) = 1$) and for each nontrivial $N \lhd U_\Sigma$, neither factor $D_1 = D_\Sigma \times \{1\}$, $D_2 = \{1\} \times D_\Sigma$ acts trivially via conjugation on N through θ'.

By the *Compactness Theorem*, there exists a finite set of $\mathcal{L}_r$-sentences Δ such that $\Delta \models \Sigma$ and $\Delta = \Delta_1 \cup \Delta_2 \cup \Delta_3 \cup \Delta_4^*$, where Δ_1 is a finite subset of $\mathcal{L}_r$-sentences specifying the characteristic and degree of imperfection of K (*Corollary 4.1.4 (1)*), Δ_2 is a finite subset of $\mathtt{PAC}$ (*Corollary 4.1.4 (2)*), Δ_3 is a finite subset of $\mathtt{Th}^{alg}(K)$ (*Corollary 4.1.4 (3)*), Δ_4^* is a finite subset of $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$ (*Corollary 4.1.4 (4)*), and Δ_4 is a finite subset of $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))$ with $\varphi \in \Delta_4 \Leftrightarrow \varphi^* \in \Delta_4^*$.

Let Λ be the set of universal sentences of Δ_3, and let K_{bad} be the join of minimal Galois extensions F/K with $F \models \neg\lambda$ for $\lambda \in \Lambda$. Let $\overline{a}_\Sigma \in S(G_{K_0}) \subset S(G_K)$ be a finite tuple of elements such that Δ_4 is a set of finitely many $\mathcal{L}_G(\overline{a}_\Sigma)$-sentences. Fix $n_\Sigma \in \mathbb{N}$ such that $S_1, \ldots, S_{n_\Sigma}$ is the smallest consecutive sequence of sorts involving the sentences of Δ_4. (Each sentence φ has finitely many occurrences of the symbols $\leq, C, P$, finitely many constant symbols, and finitely many bounded variables. Hence there exists $n_\varphi \in \mathbb{N}$ such that the $\mathcal{L}_G(\overline{a}_\Sigma)$-symbols and variables occurring in φ occur in the sorts $S_1, \ldots, S_{n_\varphi}$.) Let $\widehat{p}$ be the smallest prime larger than $n_\Sigma + |\operatorname{Gal}(K_{\text{bad}}/K)|$,

P_Σ the set of primes $\{2, 3, \ldots, \widehat{p}\}$, and $\mathcal{C}_\Sigma$ the formation of finite groups whose order is necessarily a product of powers of primes of P_Σ (including trivial powers). Define G_{P_Σ} to be the maximal pro-$\mathcal{C}_\Sigma$ quotient of G_K.

Construction 4.1.18. Choose primes t, r, s such that $t > r > s > \widehat{p}$, $r \equiv 1 \bmod s$, and $t \equiv 1 \bmod s$ (this can be done by *Dirichlet's Theorem on Arithmetic Progressions*). Let $U_\Sigma = C_t$ (the multiplicative cyclic group of order t) and $D_\Sigma = C_r \rtimes_\iota C_s$, where as $r \equiv 1 \bmod s$, there is an embedding $\iota : C_s \hookrightarrow C_{r-1} \cong \mathrm{Aut}(C_r)$ which determines the group operation:

$$(c_1, d_1) \cdot (c_2, d_2) := (c_1 \iota(d_1)(c_2), d_1 d_2).$$

Let γ be a generator of C_r and β be a generator of C_s, and consider these both as elements of D_Σ. (Abusing notation, write γ for $(\gamma, 1)$ and β for $(1, \beta)$.) Then calculation shows in $C_r \rtimes_\iota C_s$ we have the formula

$$\beta^a \cdot \gamma^b = \gamma^{bp(r)^{ak}} \cdot \beta^a,$$

where $r - 1 = ks$ and $p(r)$ is a primitive root modulo r (i.e. a generator of $(\mathbb{Z}/r\mathbb{Z})^*$, the multiplicative group of integers modulo r). One can check from this that elements of the form $\gamma^i \cdot \beta^j$ do not commute with one of γ or β when $0 \leq i < r, 0 \leq j < s$, and $i + j > 0$, hence D_Σ is centreless. As $t \equiv 1 \bmod s$, there is an embedding $C_s \hookrightarrow C_{t-1} \cong \mathrm{Aut}(C_t)$ which can be extended to a group homomorphism

$$t : D_\Sigma = C_r \rtimes C_s \twoheadrightarrow C_s \hookrightarrow \mathrm{Aut}(C_t) = \mathrm{Aut}(U_\Sigma).$$

Let $W_\Sigma = U_\Sigma \rtimes_\tau (D_\Sigma \times D_\Sigma)$ under the homomorphism $\tau : D_\Sigma \times D_\Sigma \to \mathrm{Aut}(U_\Sigma)$; $(x, y) \mapsto t(x)t(y)$, and note the following is a split exact sequence:

$$1 \longrightarrow U_\Sigma \longrightarrow W_\Sigma \underset{\theta}{\overset{\lambda}{\rightleftarrows}} D_\Sigma \times D_\Sigma \longrightarrow 1. \qquad \blacksquare$$

Lemma 4.1.19. *With $D_\Sigma, U_\Sigma, W_\Sigma$ from* Construction 4.1.18*, (G1)–(G4) are satisfied.*

Proof. We follow [FJ08, Example 28.7.4] as much as possible.

(G1) is satisfied: the composition factors of D_Σ are C_r and C_s, distinct to the (unique) composition factor C_t.

(G2) is satisfied: let I be a finite set and $\pi : D_\Sigma^I = \prod_{i\in I}(D_\Sigma)_i \to D_\Sigma$ an epimorphism. We may suppose $\ker(\pi) \cap (D_\Sigma)_i$ is a proper (normal) subgroup of D_Σ for each $i \in I$; otherwise if $(D_\Sigma)_j \leq \ker(\pi)$ for some $j \in I$ we may consider the epimorphism $\pi' : D_\Sigma^{I\setminus\{j\}} \to D_\Sigma$ and apply induction to find $i \in I \setminus \{j\}$ such that $\ker(\pi) = \ker(\pi_i)$.

For each $i \in I$, $\ker(\pi) \cap (D_\Sigma)_i$ is thus either 1 or a cyclic subgroup of $(D_\Sigma)_i$ of prime order. As $\ker(\pi) \cap (D_\Sigma)_i$ is normal, then $\ker(\pi) \cap (D_\Sigma)_i = 1$ or $\langle\gamma_i\rangle$ where $\gamma_i \in (D_\Sigma)_i$ is of order r. If $\ker(\pi) \cap (D_\Sigma)_i = \langle\gamma_i\rangle$ for all $i \in I$, then by the *First Isomorphism Theorem for Groups* the centre of D_Σ is nontrivial – a contradiction. WLOG suppose $\ker(\pi) \cap (D_\Sigma)_1 = 1$. By the *First Isomorphism Theorem for Groups*, $\pi((D_\Sigma)_1) = D_\Sigma$, and every element of $\pi((D_\Sigma)_i)$ for $i \neq 1$ commutes with every element of D_Σ. This is a contradiction unless $I = \{1\}$ (as we have assumed $\ker(\pi) \cap (D_\Sigma)_i$ is a *proper* subgroup of D_Σ for each $i \in I$).

(G3) is satisfied: from the formula $\beta^a \cdot \gamma^b = \gamma^{bp(r)^{ak}} \cdot \beta^a$ one can calculate

$$(\beta \cdot \gamma)^n = \gamma^{\sum_{i=1}^n p(r)^{ik}} \cdot \beta^n.$$

The order of $\beta\gamma$ is thus s, as s is the smallest power n for which $\beta^n = 1$, and recalling $sk = r - 1$, $p(r)^{r-1} \equiv 1 \bmod r$, note:

$$\sum_{i=1}^{s} p(r)^{ik} \equiv \sum_{i=0}^{s-1} (p(r)^k)^i \equiv \frac{(p(r)^k)^s - 1}{p(r)^k - 1} \equiv 0 \bmod r.$$

Hence $\langle\beta\gamma\rangle$ and $\langle\beta\rangle$ both have index r in D_Σ, and $\langle\beta\gamma\rangle \cap \langle\beta\rangle = 1$. By definition $\Phi(D_\Sigma) \leq \langle\beta\gamma\rangle \cap \langle\beta\rangle$, hence $\Phi(D_\Sigma) = 1$ and $\Phi(W_\Sigma) \leq U_\Sigma$. However $\theta(D_\Sigma \times D_\Sigma)$ has index t in W_Σ, thus $\Phi(W_\Sigma) \leq U_\Sigma \cap \theta(D_\Sigma \times D_\Sigma) = 1$.

Finally, (G4) is satisfied: let θ' be an embedding of $D_\Sigma \times D_\Sigma$ into W_Σ as a semidirect complement. Since the orders of U_Σ and $D_\Sigma \times D_\Sigma$ are relatively prime, $\theta'(D_\Sigma \times D_\Sigma)$ is conjugate to $\theta(D_\Sigma \times D_\Sigma)$ by the *Schur-Zassenhaus Lemma*[6]. By (G2), $D_\Sigma \times D_\Sigma$

[6]The formulation we use is [FJ08, Lemma 22.10.1].

has a unique factorisation as a direct product of two copies of D_Σ, meaning we may canonically write $D_\Sigma \times D_\Sigma = D_1 \times D_2$. We have, for $w \in W_\Sigma$, $v \in U_\Sigma$ (also denoted v as an element of W_Σ), and $d \in D_1 \cup D_2$:

$$\begin{aligned} v^{\theta'(d)} &= v^{\theta(d)^w} \\ &= \theta(d)^w \cdot v \cdot (\theta(d)^w)^{-1} = (w \cdot \theta(d) \cdot w^{-1}) \cdot v \cdot (w \cdot \theta(d) \cdot w^{-1})^{-1} \\ &= (w \cdot \theta(d) \cdot w^{-1}) \cdot v \cdot (w \cdot \theta(d)^{-1} \cdot w^{-1}) = w \cdot [\theta(d) \cdot [w^{-1} \cdot v \cdot w] \cdot \theta(d)^{-1}] \cdot w^{-1} \\ &= w \cdot \tau(d)(w^{-1} \cdot v \cdot w) \cdot w^{-1}. \end{aligned}$$

Note as U_Σ is normal, $\overline{v} := w^{-1} \cdot v \cdot w \in U_\Sigma$. If $w \cdot \tau(d)(w^{-1} \cdot v \cdot w) \cdot w^{-1} = v$, then $\tau(d)(\overline{v}) = \overline{v}$. However we may choose $v \in U_\Sigma$ and $d \in D_1 \cup D_2$ such that $\overline{v} \neq 1$ and $\tau(d) \in \mathrm{Aut}(U_\Sigma)$ has $\tau(d)(\overline{v}) \neq \overline{v}$. Hence neither of D_1 or D_2 act trivially via conjugation on U_Σ through θ', as desired. ■

Given a graph $\Gamma = (A, R)$, consider the profinite group G_Γ from *Construction 4.1.9* using D_Σ and W_Σ (we suppress the Σ notation in G_Γ). There is a split exact sequence

$$1 \longrightarrow U_\Sigma^R \longrightarrow G_\Gamma \longrightarrow D_\Sigma^A \longrightarrow 1.$$

Consider the cotheory of G_Γ: by design, there are no proper open normal subgroups $N \triangleleft G_\Gamma$ of index less than or equal to $\widehat{p}$. Hence the only element of $S(G_\Gamma)$ of sort $n \leq \widehat{p}$ is $1G_\Gamma$. Note also, $\Gamma \cong \Gamma_{G_\Gamma}$ from *Construction 4.1.9*. Let $\widetilde{G_\Gamma}$ be the universal Frattini cover of G_Γ with map $f : \widetilde{G_\Gamma} \to G_\Gamma$. By [CvdDM80, Corollary 54] the sorts $S_1, \ldots, S_{\widehat{p}}$ of $S(\widetilde{G_\Gamma})$ remain trivial, and $\Gamma_{\widetilde{G_\Gamma}} \cong \Gamma_{G_\Gamma}$ by [FJ08, Lemma 28.6.1]. Let $G_\Gamma^* = G_{P_\Sigma} \star \widetilde{G_\Gamma}$. Then G_Γ^* is projective ([FJ08, Proposition 22.4.10]) and $S(G_\Gamma^*) \models \Delta_4$. (Indeed, $S(G_\Gamma^*)$ is an $\mathcal{L}_G(\overline{a}_\Sigma)$-structure and $S(G_\Gamma^*) \models \Delta_4$; as the argument for this is pp. 75–76, with $\Delta_4 = \Sigma_2$ and $\mathbb{F}_p(q)$ replaced by $\widetilde{G_\Gamma}$, we do not repeat it here.) We claim $\Gamma_{G_\Gamma^*} \cong \Gamma_{\widetilde{G_\Gamma}}$, or more generally:

Lemma 4.1.20. *Let H be a pro-$\mathcal{C}_\Sigma$ group[7]; then $\Gamma_{H \star \widetilde{G_\Gamma}} \cong \Gamma_{\widetilde{G_\Gamma}}$.*

[7]Recall C_Σ is the full formation of finite groups whose order is a product or primes of P_Σ.

Proof. A minor adaptation of [FJ08, Lemma 28.6.1]. Consider the quotient map $\pi : H \star \widetilde{G_\Gamma} \to \widetilde{G_\Gamma}$, with kernel $\langle H \rangle$ the least closed normal subgroup of $H \star \widetilde{G_\Gamma}$ containing H. For open normal subgroups $N \triangleleft \widetilde{G_\Gamma}$, there is an isomorphism

$$\widetilde{G_\Gamma}/N \cong (H \star \widetilde{G_\Gamma})/\pi^{-1}(N).$$

This yields an embedding $\Gamma_{\widetilde{G_\Gamma}} \hookrightarrow \Gamma_{H \star \widetilde{G_\Gamma}}$ along π^{-1}.

Conversely, if $M \triangleleft H \star \widetilde{G_\Gamma}$ is open, and $H \star \widetilde{G_\Gamma}/M \cong D_\Sigma$ (resp. W_Σ), then consider $\rho : H \star \widetilde{G_\Gamma} \twoheadrightarrow D_\Sigma$ (resp. W_Σ) and notice $\rho(H) \leq D_\Sigma$ (resp. W_Σ). Since any quotient of H by an open normal subgroup of H is a P_Σ-group, there exists elements of $\rho(H)$ of the wrong order (by *Lagrange's Theorem*) unless $H \leq \ker(\rho)$. As $\ker(\rho)$ is a normal subgroup of $H \star \widetilde{G_\Gamma}$, $\ker(\pi) = \langle H \rangle \leq \ker(\rho) = M$. Therefore $M = \pi^{-1}(\pi(M))$ and thus π^{-1} induces an isomorphism of graphs $\Gamma_{H \star \widetilde{G_\Gamma}} \cong \Gamma_{\widetilde{G_\Gamma}}$ as required. ■

We are ready to prove:

Theorem 4.1.14. *For any nontrivial graph Γ there exists a PAC field $K_\Gamma \supseteq K$ such that $K_\Gamma \models \Sigma$ and $\Gamma_{K_\Gamma} \cong \Gamma$.*

Proof. Given Γ, Σ, construct the projective profinite group G^*_Γ. Note that $\mathrm{Gal}(K_{\mathrm{bad}}/K)$ is a quotient of G_{P_Σ}, which is a quotient of G^*_Γ, hence there is an epimorphism $G^*_\Gamma \twoheadrightarrow \mathrm{Gal}(K_{\mathrm{bad}}/K)$. By *Theorem 4.1.5* there is a PAC field K_Γ extending K, of the same degree of imperfection as K, such that $K_\Gamma \cap K_{\mathrm{bad}} = K$ and $G_{K_\Gamma} \cong G^*_\Gamma$. Therefore $K_\Gamma \models \Delta_1 \cup \Delta_2 \cup \Delta_3 \cup \Delta^*_4$ by construction, hence $K_\Gamma \models \Sigma$, and $\Gamma \cong \Gamma_{G_{K_\Gamma}} \cong \Gamma_{K_\Gamma}$ as required. ■

Corollary 4.1.21. *Every PAC field is finitely undecidable.*

Proof. Fix K a PAC field and $\Sigma \subset \mathtt{Th}(K; \mathcal{L}_r)$ a finite subtheory. Let Γ be a nontrivial graph; by *Lemma 4.1.12 & Theorem 4.1.14* there exists a PAC field $K_\Gamma \models \Sigma$ and Γ is interpretable in K_Γ. Furthermore, the interpretation of *Lemma 4.1.12* is uniform in the sense of *Definition A.6*; the class of nontrivial graphs is uniformly interpretable in

the class of PAC fields satisfying Σ. We conclude $\mathtt{PAC} \cup \Sigma$ is hereditarily undecidable by *Corollary A.15*, hence Σ is undecidable as required. ■

Example 4.1.22. Let $\mathbb{K}$ be a countable ω-free PAC field of characteristic 0 containing $\widetilde{\mathbb{Q}}$. By standard results (cf. [Koe16b, Proposition 9]) $\mathtt{Th}(\mathbb{K}; \mathcal{L}_r)$ is decidable, however by *Corollary 4.1.21*, $\mathtt{Th}(\mathbb{K}; \mathcal{L}_r)$ is finitely undecidable. □

As an undecidability result, *Corollary 4.1.21* is interesting in its own right. With *Theorem 4.1.7 & Corollary 4.1.21* there are connections back to *Problems 1.2.1 & 1.2.5*, modulo a classification-theoretic conjecture:

Corollary 4.1.23. *Assume the Simple Fields Conjecture. Then every infinite simple field is not finitely axiomatisable, and furthermore is finitely undecidable.* ■

4.2 Pseudo-Real Closed Fields

After considering PAC fields, the next natural step to take is to the *pseudo-real closed* fields; the PAC-analogue of an ordered field.

Remark 4.2.1. *Subtlety: uniqueness of real closure.* Recalling *§1.3*, $\mathbb{Q}$ as an ordered field has a unique ordering (the 'usual' one) and has a unique (up to order isomorphism) *real closure* $\mathbb{R}_{alg} := \mathbb{R} \cap \widetilde{\mathbb{Q}}$. By *real closure* of a field K with positive cone P, we mean a real closed algebraic extension of K whose order extends P. $\mathbb{R}_{alg}$ is real closed, and its order is necessarily unique as it is the set $(\mathbb{R}_{alg})^2$.

Clearly, as fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}_{alg}$, and $\mathbb{Q}(\sqrt{2})$ has two distinct orderings P_1, P_2 extending that of $\mathbb{Q}$. They are distinct, but order-isomorphic: $(\mathbb{Q}(\sqrt{2}), P_1)$ is isomorphic to $(\mathbb{Q}(\sqrt{2}), P_2)$. However, as $P_1 \neq P_2$, $\mathbb{Q}(\sqrt{2})$ has two nonisomorphic real closures R_1, R_2, i.e. (and this is the crucial point) there is no isomorphism $R_1 \to R_2$ *preserving the embedding of* $\mathbb{Q}(\sqrt{2})$ *in* R_1 *and* R_2. As fields, $\mathbb{R}_{alg}, R_1, R_2$ are all isomorphic; as ordered fields (WLOG) $\mathbb{R}_{alg} \cong R_1 \ncong R_2$ *over* $\mathbb{Q}(\sqrt{2})$; and $\mathbb{R}_{alg} \cong R_1 \cong R_2$ *over* $\mathbb{Q}$.

Therefore it very much matters over which field one takes the real closure. This contrasts with algebraically closed fields, where any two algebraic closures of $\mathbb{Q}(\sqrt{2})$ are isomorphic over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$. □

PRC fields were given their modern formulation by Prestel [Pre81, Theorem 1.2]:

Definition 4.2.2. A field K is *pseudo-real closed* (PRC) if every geometrically irreducible variety defined over K, which has a smooth $\overline{K}$-rational point in each real closure $\overline{K}$ of K, has a K-rational point.

We assume the reader is familiar with [HJ85]; if not, the notions relevant to this chapter are covered in *Appendix B*. The theory of formally real PRC fields is also undecidable[8] by the work of Haran:

Theorem 4.2.3. [Har84, Theorem 3.1]. *Let Ξ be a nonempty family of Boolean spaces, and* $\mathtt{PRC}(\Xi)$ *the elementary theory of the class of PRC fields K such that $X(K) \in \Xi$. Then* $\mathtt{PRC}(\Xi)$ *is undecidable.* ■

It is Haran's proof we will adapt to determine the following:

Corollary 4.2.16. *Every PRC field is finitely undecidable.*

Recall from [HJ85]/*Appendix B* the category of *Artin-Schreier structures*; this is the 'right' category to consider the Galois theory of PRC fields in, as evidenced by the main result of [HJ85]:

Theorem 4.2.4. [HJ85, Theorem 10.4]. *If K is a PRC field, then $\mathfrak{G}_K$ is projective. Conversely, if $\mathfrak{G}$ is a projective Artin-Schreier structure, there exists a PRC field K such that $\mathfrak{G} \cong \mathfrak{G}_K$.* ■

Haran & Jarden actually prove a theorem slightly more precise than this. They prove a corresponding *Theorem 4.1.5:* given a PRC field K, they produce a PRC field extension E whose algebraic part is governable relative to K, yet has an almost arbitrary absolute Artin-Schreier structure.

[8] In fact, *hereditarily* undecidable: Ershov's remark [Ers81, p. 260] on his proof of the hereditary undecidability of `PAC` applies here.

Theorem 4.2.5. [HJ85, Theorem 10.2]. *Let $\mathfrak{G}$ be a projective Artin-Schreier structure. Let L/K be a Galois extension such that $\sqrt{-1} \in L$ and let $\pi : \mathfrak{G} \to \mathfrak{Gal}(L/K)$ be an epimorphism. Then there exists a PRC extension E/K such that $\mathfrak{G} \cong \mathfrak{G}_E$, and*

$$\begin{array}{ccc} \mathfrak{G} & \xrightarrow{\cong} & \mathfrak{G}_E \\ & \searrow^{\pi} & \downarrow Res_L \\ & & \mathfrak{Gal}(L/K) \end{array}$$

is a commutative diagram. ■

Immediately, we obtain:

Corollary 4.2.6. *Let L/K be a Galois extension, $\mathfrak{G}$ a projective Artin-Schreier structure, and $\alpha : \mathfrak{G} \to \mathfrak{Gal}(L(\sqrt{-1})/K)$ an epimorphism. Then K has an extension E which is PRC, $E \cap L(\sqrt{-1}) = K$, and there exists an isomorphism $\gamma : \mathfrak{G}_E \to \mathfrak{G}$ such that $\alpha \circ \gamma = Res_L$.* ■

There is a rich theory of absolute Artin-Schreier structures one can develop alongside the theory of absolute Galois groups. As the absolute Galois group, plus some algebraic information, completely determines the first-order theory of a PAC field K, one would hope the same can be said for PRC fields. If two PRC fields K_1, K_2 are elementary equivalent, by interpreting finite Galois extensions of K_1 (resp. K_2) in K_1 (resp. K_2) we can draw some elementary equivalence between G_{K_1} and G_{K_2}. Of course, the algebraic information must also be equivalent. The difficulty is in saying whether this information is sufficient to force $K_1 \equiv K_2$. This can be done, however, using an adapted PAC lemma by Ershov [Ers84] and written explicitly by Jarden [Jar88].

Theorem 4.2.7. (cf. [Ers84, Theorem 2], [Jar88, Proposition 3].) *Let K_1, K_2 be PRC fields, separable over a common subfield E. Then $K_1 \equiv_E K_2$ if and only if K_1 & K_2 have the same degree of imperfection, there exists $\theta \in G_E$ such that $\theta(K_1 \cap E^s) = K_2 \cap E^s$, and if $S\Theta : S(G_{K_1 \cap E^s}) \to S(G_{K_2 \cap E^s})$ is the isomorphism induced by θ, then the partial map $S\Theta : S(G_{K_1}) \to S(G_{K_2})$ with domain $S(G_{K_1 \cap E^s})$ is $\mathcal{L}_G$-elementary.*

Proof. The following is Chatzidakis [Cha02, Theorem 5.13], mutatis mutandis. Assuming $K_1 \equiv_E K_2$, it is clear there exists $\theta \in G_E$ with $\theta(K_1 \cap E^s) = \theta(K_2 \cap E^s)$, and

the partial map $S\Theta : S(G_{K_1}) \to S(G_{K_2})$ induced by θ is $\mathcal{L}_G$-elementary on $S(G_{K_1 \cap E^s})$.

Conversely, assume we have the maps θ, $S\Theta$. Moving ${K_1}^s$ by an automorphism extending θ, we may assume WLOG $K_1 \cap E^s = K_2 \cap E^s$, then replace E by $K_1 \cap E^s$ and θ by the identity map. Note now K_1, K_2 are regular extensions of E, and $S\Theta$ is the identity on $S(G_E)$.

By an analogue of the *Keisler-Shelah Theorem*, there is a nonprincipal ultrafilter $\mathcal{U}$ on an index set I such that $S(G_{K_1^{\mathcal{U}}}) \cong_{S(G_E)} S(G_{K_2^{\mathcal{U}}})$ (see [Cha02, (5.12)] with *Remarks (2)*, §5.5 *ibid.*). Dualising, there is a group homeomorphism $\varphi : G_{K_1^{\mathcal{U}}} \to G_{K_2^{\mathcal{U}}}$ such that for every $\sigma \in G_{K_1^{\mathcal{U}}}$, $\varphi(\sigma)|_{E^s} = \sigma|_{E^s}$. By Cherlin, van den Dries & Macintyre [CvdDM80, §3][9] (for nonformally real PRC fields) and Jarden [Jar88, Proposition 3] (for formally real PRC fields), this forces $K_1^{\mathcal{U}} \equiv_E K_2^{\mathcal{U}}$, hence $K_1 \equiv_E K_2$ as required. ■

Note this is elementary equivalence in the language of rings (over a common subfield); *not* the language of *ordered* rings.

Corollary 4.2.8. *A PRC field K is axiomatised by the following first-order $\mathcal{L}_r$-axiom scheme:*

(1) The characteristic and degree of imperfection of K;

(2) The PRC field axioms, `PRC`*;*

(3) $\mathtt{Th}^{alg}(K)$*;*

(4) $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$. ■

(Recall *Remark 4.1.3*, and that $K_0 = K \cap \mathbb{F}^s$ where $\mathbb{F}$ is the prime subfield of K.)

Remark 4.2.9. We emphasise here that if K is a *formally real* PRC field (distinct to the nonformally real PRC fields; the PAC fields) then necessarily K has characteristic 0. In addition, the orders on K can in a way be 'seen' by $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))$. Indeed, the space of orders $X(K) = X(K(\sqrt{-1})/K) \cong X(K^s/K)/G_{K(\sqrt{-1})}$, which is homeomorphic to $\mathrm{Inv}(G_K)/G_{K(\sqrt{-1})}$ by *Theorem B.12*. □

[9] Presented also in Fried & Jarden [FJ08, Theorem 20.3.3].

Now that we have a solid description of the first-order theory of any given PRC field, we are almost ready to conclude its finite undecidability – what remains are category-theoretic tools, such as Haran's method of transferring the graph constructions in the category of profinite groups to the category of Artin-Schreier structures (in [Har84, §2]).

The following recalls [Har84, p. 102]: fix a Boolean space X. For a profinite group G, let $\mathbb{Z}/2\,\mathbb{Z}\times G$ act on the Boolean space $X \times G$ by:

$$(x,g)^{(1,h)} = (x,g)^{(\varepsilon,h)} = (x,gh), \qquad \text{for } x \in X \text{ and } g,h \in G,$$

where $\mathbb{Z}/2\,\mathbb{Z} = \langle\varepsilon\rangle$. Define $d : X \times G \to \mathbb{Z}/2\,\mathbb{Z}\times G$ by $d(x,g) = \varepsilon$. We have constructed an Artin-Schreier structure

$$F(X,G) = \langle \mathbb{Z}/2\,\mathbb{Z}\times G,\, G,\, d : X \times G \to \mathbb{Z}/2\,\mathbb{Z}\times G\rangle.$$

This describes a faithful functor $F(X,-)$ from the category of profinite groups to the category of Artin-Schreier structures (where we extend F to morphisms in the obvious way), with the additional property that the 'orbit space' $X(F(X,G))/G \cong X$. Moreover, if φ is an epimorphism of profinite groups, then $F(X,\varphi)$ is a cover of Artin-Schreier structures.

Remark 4.2.10. [Har84, Remark 2.2]. Let L/K be a Galois extension, G a profinite group, and X a Boolean space; then $\mathfrak{Gal}(L/K) \cong F(X,G)$ if and only if $\sqrt{-1} \in L \setminus K$, $X(K) \cong X$, and there exists a *totally real*[10] Galois extension $K \subseteq L_0 \subseteq L$ such that $\mathrm{Gal}(L_0/K) \cong G$ and $L = L_0(\sqrt{-1})$. □

We will also use the forgetful functor from the category of Artin-Schreier structures to the category of profinite groups:

$$\mathrm{Ft}(\mathfrak{G}) = \mathrm{Ft}(\langle G, G', X(\mathfrak{G}) \xrightarrow{d} G\rangle) = G.$$

(Morphisms are handled in the obvious way.)

[10] Each ordering $P \in X(K)$ extends to one on L_0.

Given an Artin-Schreier structure $\mathfrak{G} = \langle G, G', X(\mathfrak{G}) \xrightarrow{d} G\rangle$, we may perform an analogous graph construction for a fixed Boolean space X, and as before the groups D, W mentioned here satisfy conditions (G1)–(G4) of *Construction 4.1.9*. Let $A^X_{\mathfrak{G}}$ be the set of open normal subgroups of G such that $N \leq G'$, $\mathfrak{G}/N \cong F(X, D)$, and define the binary relation $R^X_{\mathfrak{G}}$ on $A^X_{\mathfrak{G}}$ to be the following set:

$$\{(N_1, N_2) \in A^X_{\mathfrak{G}} \times A^X_{\mathfrak{G}} : N_1 \neq N_2 \ \&\ \exists M \triangleleft G \text{ open s.t. } M \leq N_1 \cap N_2,\ \mathfrak{G}/M \cong F(X, W)\}.$$

The structure $\Gamma_{\mathfrak{G},X} = (A^X_{\mathfrak{G}}, R^X_{\mathfrak{G}})$ is a graph, and moreover to any graph Γ (and any Boolean space X) we may construct an Artin-Schreier structure $\mathfrak{G}_\Gamma$ such that $\Gamma_{\mathfrak{G}_\Gamma, X} \cong \Gamma$; namely $\mathfrak{G}_\Gamma = F(X, G_\Gamma)$ where G_Γ is the group from *Construction 4.1.9* (this is [Har84, p. 104, comment 1]). Similarly, if K is a field, define A^{rc}_K to be the set of Galois extensions L (contained in a fixed separable closure K^s of K) such that $\mathfrak{Gal}(L/K) \cong F(X(K), D)$. Define the binary relation R^{rc}_K on A^{rc}_K by:

$$R^{rc}_K = \{(L_1, L_2) \in A^{rc}_K \times A^{rc}_K : L_1 \neq L_2 \ \&\ \exists N/K \text{ Galois s.t. } L_1 L_2 \subseteq N \\ \&\ \mathfrak{Gal}(N/K) \cong F(X(K), W)\}.$$

This defines a graph Γ^{rc}_K. Finally, we define the *canonical graph structure for* $\mathfrak{G}$, denoted $\Gamma_{\mathfrak{G}}$, as $\Gamma_{\mathfrak{G}, X(\mathfrak{G})/G'}$. We have the following intuitive result:

Lemma 4.2.11. *Let G be a profinite group, X a Boolean space, and K a field. Then:*

- *There is a* natural *isomorphism $\Gamma_G \cong \Gamma_{F(X,G),X}$;*
- $\Gamma^{rc}_K \cong \Gamma_{\mathfrak{G}_K, X(K)} = \Gamma_{\mathfrak{G}_K, X(\mathfrak{G}_K)/G_{K(\sqrt{-1})}} = \Gamma_{\mathfrak{G}_K}$*;*
- *If $\phi : \mathfrak{H} \to \mathfrak{G}$ is a* Frattini cover *of Artin-Schreier structures, then $\Gamma_{\mathfrak{G},X} \cong \Gamma_{\mathfrak{H},X}$.*

Proof. *Comments 1, 2, & 3* of [Har84, p. 104]. *Frattini covers of Artin-Schreier structures* are introduced and their basic properties proven in [Har84, §1]. ■

One tool needed for the main proof not already introduced is some notion of "free product". In the category of Artin-Schreier structures, it is not immediately obvious

that this category admits a coproduct, and if it does, how that coproduct would behave. However examining *Theorem 4.1.7* we see that in fact we do not need a general coproduct – we shall see that the following construction will suffice[11].

Let $\mathfrak{G} = \langle G, G', X(\mathfrak{G}) \xrightarrow{d} G \rangle$ be an Artin-Schreier structure and E a profinite group. Define

$$\mathfrak{G} \diamond E = \langle G \star E,\, G'_\star,\, \mathrm{Inv}(G \star E) \xhookrightarrow{incl.} G \star E \rangle,$$

where "$\star$" is the coproduct in the category of profinite groups, $G'_\star := \ker(G \star E \to \mathbb{Z}/2\,\mathbb{Z})$ where $G \star E \to \mathbb{Z}/2\,\mathbb{Z}$ is uniquely determined by $E \to \{1\}$, $G \to G/G'$, where $G/G' \cong \mathbb{Z}/2\,\mathbb{Z}$ or $\{1\}$, and $\mathrm{Inv}(G \star E)$ is the set of involutions of $G \star E$. Note that a priori this is not necessarily even a weak Artin-Schreier structure. Though a posteriori, we have the following result.

Lemma 4.2.12. *Let $\mathfrak{G}$ be a projective Artin-Schreier structure, and E a projective profinite group. Then $\mathfrak{G} \diamond E$ is a projective Artin-Schreier structure.*

Proof. For exposition and clarity we shall prove this result 'manually', though there are alternative routes (cf. *Lemma 4.3.8*).

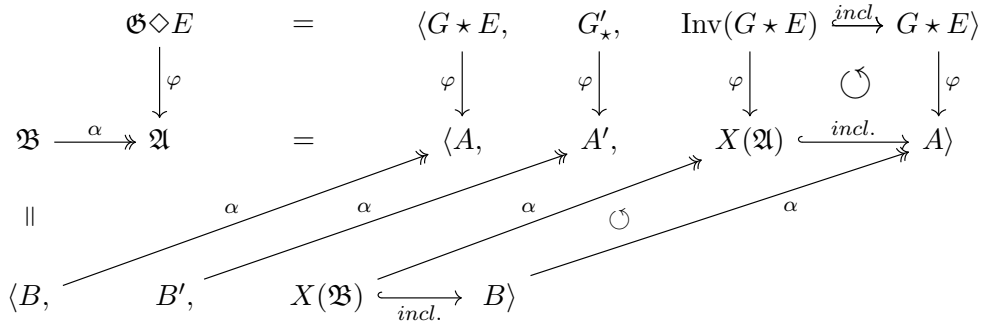
By *Theorem B.12*, G' is a projective profinite group and $X(\mathfrak{G}) \cong \mathrm{Inv}(G)$. Note that $G'_\star$ is open, normal, and of index ≤ 2 in $G \star E$. Therefore in order for $\mathfrak{G} \diamond E$ to be a weak Artin-Schreier structure, it is simply required that $\mathrm{Inv}(G \star E)$ be a closed subset of $G \star E$ (as then it is Boolean). Equivalently, by [HJ85, Remark 7.6] we wish there to exist an open $U \lhd G \star E$ such that $U \cap \mathrm{Inv}(G \star E) = \emptyset$. This is satisfied by $U = G'_\star$; indeed, if $\epsilon \in G \star E$ is an involution, by [HR85, Theorem A] it is conjugate to an involution σ of G or E. However $G' \leq G$ and E are projective, hence torsion free, so $\sigma \in G \setminus G'$. Therefore $\epsilon \notin \ker(G \star E \to \mathbb{Z}\,/2\,\mathbb{Z})$ above, thus $\epsilon \notin G'_\star$.

We shall show every finite embedding problem for $\mathfrak{G} \diamond E$ has a solution, which completes the proof by *Theorem B.11 (2)*. Consider the following embedding problem:

$$\begin{array}{ccc} & & \mathfrak{G} \diamond E \\ & & \downarrow \varphi \\ \mathfrak{B} & \xrightarrow{\alpha} \!\!\!\rightarrow & \mathfrak{A} \end{array}$$

[11] cf. [Feh10, §3.3] for a similar technique.

where φ is a morphism and α is an epimorphism of finite weak Artin-Schreier structures $\mathfrak{A}, \mathfrak{B}$. By *Theorem B.11 (3)*, as the forgetful map of $\mathfrak{G}\diamond E$ is injective it will suffice to assume $X(\mathfrak{A}) \subseteq A$, $X(\mathfrak{B}) \subseteq B$. Diagrammatically:



(Note the maps are indeed correctly labelled; each map is $\varphi : G \star E \to A$ or $\alpha : B \to A$, restricted to a subset of the relevant group.) This diagram gives rise to the following two:

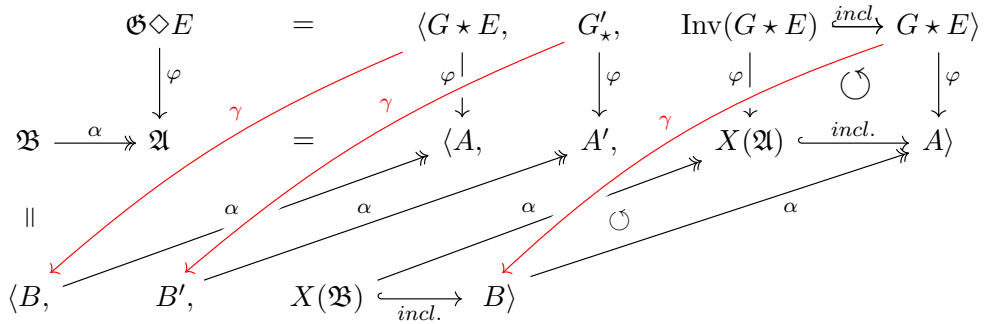
$$\begin{array}{ccc} & & G \\ & & \downarrow{\scriptstyle \varphi|_G} \\ B & \xrightarrow{\alpha} & A \end{array} \qquad\qquad \begin{array}{ccc} & & E \\ & & \downarrow{\scriptstyle \varphi|_E} \\ B & \xrightarrow{\alpha} & A \end{array}$$

where $\alpha : B' \twoheadrightarrow A'$. The former is solvable by $\gamma_G : G \to B$, as G is real projective (*Corollary B.15*, i.e. [HJ85, Proposition 7.7]) and this is a *real* embedding problem for G. Indeed (following the exposition of [HJ85, p. 474]) we may assume in addition that $X(\mathfrak{B}) = \mathrm{Inv}(B \setminus B')$, as by [HJ85, Corollary 6.2] there exists a finite group B_1 and epimorphism $\theta : B_1 \twoheadrightarrow B$ such that the image under θ of $\mathrm{Inv}(B_1 \setminus \ker(\theta))$ is exactly $X(\mathfrak{B})$, and we may replace $\mathfrak{B}$ with $\langle B_1, \theta^{-1}(B'), \mathrm{Inv}(B_1 \setminus \ker(\theta)) \hookrightarrow B_1\rangle$ if desired. Therefore if $\epsilon \in G$ is an involution with $\varphi|_G(\epsilon) \neq 1$, considering ϵ as an involution of $G \star E$, under $\alpha : X(\mathfrak{B}) \twoheadrightarrow X(\mathfrak{A})$ there exists an involution $b \in B \setminus B'$ with $\alpha(b) = \varphi(\epsilon) = \varphi|_G(\epsilon)$, as required.

The latter diagram is solvable by $\gamma_E : E \to B$ (as E is projective). By definition of the free product, there exists a morphism $\gamma : G \star E \to B$ uniquely extending $\varphi|_G$, $\varphi|_E$ such that $\alpha \circ \gamma = \varphi$.

Consider $\gamma|_{G'_\star} : G'_\star \to B$. We wish that $\gamma|_{G'_\star}(G'_\star) \subseteq B'$. This is indeed the case: by definition $\alpha(B') = A'$ (and moreover $\alpha(B \setminus B') \subseteq A \setminus A'$), so since $\alpha \circ \gamma = \varphi : G'_\star \to A'$

it must be the case $\gamma|_{G'_\star}(G'_\star) \subseteq B'$ as desired. We may update the main diagram to:



If it is the case that $\gamma(\mathrm{Inv}(G \star E)) \subseteq X(\mathfrak{B})$, then we are finished. Recall $X(\mathfrak{B}) = \mathrm{Inv}(B \setminus B')$; then for all $\varepsilon \in \mathrm{Inv}(G \star E)$, since $\alpha(\gamma(\varepsilon)) = \varphi(\varepsilon) \in X(\mathfrak{A})$, by the initial set up $\gamma(\varepsilon) \in B \setminus B'$ and hence $\gamma(\varepsilon) \in X(\mathfrak{B})$ as desired.

We conclude that $\gamma : \mathfrak{G}\diamond E \to \mathfrak{B}$ is a morphism of weak Artin-Schreier structures solving the initial finite real embedding problem. This completes the proof. ■

We will reference the following from the proof of [Har84, Theorem 3.1]:

Lemma 4.2.13. *Let K be a PRC field; Γ_K^{rc} is interpretable (in the sense of* Definition A.2*) in K.*

Proof. This is [Har84, pp. 106–107], which we elaborate on now. Let G be a finite group, and $\alpha_{r,G}(x_1, \ldots x_r)$ be an $\mathcal{L}_r$-formula such that

$$K \models \alpha_{r,G}(\overline{a}) \iff f_{\overline{a}}(T) = T^r + a_1 T^{r-1} + \cdots + a_r \text{ is irreducible over } K, \text{ and}$$
$$\mathfrak{Gal}(K_{\overline{a}}(\sqrt{-1})/K) \cong F(X(K), G),$$

where $\overline{a} \in K^r$. Indeed, $\alpha_{r,G}(\overline{a})$ can be given by the conjunction of the following statements:

- $f_{\overline{a}}$ is irreducible over K, $K_{\overline{a}}/K$ is Galois, and $\mathrm{Gal}(K_{\overline{a}}/K) \cong G$;
- $\sqrt{-1} \notin K$;
- $K_{\overline{a}}/K$ is totally real.

All but the last are standard to express in the language of rings, and the last is covered by Prestel in [Pre81, Theorem 4.1]. On *p. 154 ibid.*, Prestel shows an equivalent formulation of "$K_{\overline{a}}/K$ is totally real" is $\mathcal{L}_r$-axiomatisable, assuming K is PRC. He assumes (in our notation) that $f_{\overline{a}}$ is absolutely irreducible, though this is not used in this part of his proof.

Fix finite groups D, W satisfying the graph conditions (*Construction 4.1.9*), and define $l = |D|$, $m = |W|$. As in *Construction 4.1.11* one may construct an $\mathcal{L}_r$-formula $\rho_{D,W}$ such that for $\overline{b}, \overline{c} \in K^l$,

$$K \models \rho_{D,W}(\overline{b}, \overline{c}) \iff K_{\overline{b}} \not\subseteq K_{\overline{c}} \vee K_{\overline{c}} \not\subseteq K_{\overline{b}}, \quad K \models \alpha_{l,D}(\overline{b}) \wedge \alpha_{l,D}(\overline{c}), \quad \text{and}$$
$$K \models \exists \overline{z}\, (\alpha_{m,W}(\overline{z}) \wedge \text{“}K_{\overline{b}} \subseteq K_{\overline{z}}\text{”} \wedge \text{“}K_{\overline{c}} \subseteq K_{\overline{z}}\text{”}).$$

We may then define a recursive translation map $-' : \mathrm{Form}(\mathcal{L}_{gr}) \to \mathrm{Form}(\mathcal{L}_r)$; $\phi \mapsto \phi'$ by the following rules:

- $R(X, Y) \mapsto (R(X, Y))' = \rho_{D,W}(\overline{x}, \overline{y})$;
- $\neg\varphi \mapsto \neg(\varphi')$; $\qquad \varphi_1 \wedge \varphi_2 \mapsto (\varphi_1') \wedge (\varphi_2')$;
- $\exists x(\varphi) \mapsto \exists \overline{x}\, (\alpha_{l,D}(\overline{x}) \wedge \varphi'(\overline{x}))$.

Recalling *Definition A.2*, set $\mathcal{L}_1 = \mathcal{L}_r$, $\mathcal{L}_0 = \mathcal{L}_{gr}$, $n = l = |D|$, $\delta(\overline{x}) = \alpha_{n,D}(\overline{x})$, and $f : \alpha_{n,D}(K^n) \to \Gamma_K^{rc}$; $\overline{a} \mapsto K_{\overline{a}}(\sqrt{-1})$. This is indeed surjective: by *Remark 4.2.10* if $L \in A_K^{rc}$ there exists a totally real Galois extension L_0/K such that $L = L_0(\sqrt{-1})$ and $\mathrm{Gal}(L_0/K) \cong D$, hence L_0 is the splitting field of a degree $n = |D|$ monic separable irreducible polynomial $f_{\overline{a}}(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ over K. Therefore $K \models \alpha_{n,D}(\overline{a})$.

Note *Definition A.2 (2)* is satisfied by the above construction of $-'$, and condition (†) is confirmed in [Har84, Theorem 3.1]. ■

Remark 4.2.14. Notice the $\mathcal{L}_r$-formula $\alpha_{n,D}(\overline{x})$ and the map $-' : \mathrm{Form}(\mathcal{L}_{gr}) \to \mathrm{Form}(\mathcal{L}_r)$ of *Lemma 4.2.13* do not depend on K or Γ_K^{rc}; the interpretation is *uniform* across PRC fields K. □

Fix a PRC field K with a finite subtheory $\Sigma \subset \mathtt{Th}(K; \mathcal{L}_r)$. By the *Compactness Theorem*, there exists a finite set of $\mathcal{L}_r$-sentences Δ such that $\Delta \models \Sigma$ and $\Delta = \Delta_1 \cup \Delta_2 \cup \Delta_3 \cup \Delta_4^*$, where Δ_1 is a finite subset of $\mathcal{L}_r$-sentences specifying the characteristic and degree of imperfection of K (*Corollary 4.2.8 (1)*), Δ_2 is a finite subset of $\mathtt{PRC}$ (*Corollary 4.2.8 (2)*), Δ_3 is a finite subset of $\mathtt{Th}^{alg}(K)$ (*Corollary 4.2.8 (3)*), Δ_4^* is a finite subset of $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$ (*Corollary 4.2.8 (4)*), and Δ_4 is a finite subset of $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))$ with $\varphi \in \Delta_4 \Leftrightarrow \varphi^* \in \Delta_4^*$.

Let Λ be the set of universal sentences of Δ_3, and let K_{bad} be the join of $K(\sqrt{-1})$ and of minimal Galois extensions F/K within a fixed algebraic closure $\widetilde{K}$ of K, with $F \models \neg\lambda$ for $\lambda \in \Lambda$. Let $\overline{a}_\Sigma \in S(G_{K_0}) \subset S(G_K)$ be a finite tuple of elements such that Δ_4 is a set of finitely many $\mathcal{L}_G(\overline{a}_\Sigma)$-sentences. Fix $n_\Sigma \in \mathbb{N}$ such that $S_1, \ldots, S_{n_\Sigma}$ is the smallest consecutive sequence of sorts involving the sentences of Δ_4. Let $\widehat{p}$ be the smallest odd prime larger than $n_\Sigma + |\operatorname{Gal}(K_{\text{bad}}/K)|$, P_Σ the set of primes $\{2, 3, \ldots, \widehat{p}\}$, and $\mathcal{C}_\Sigma$ the formation of finite groups whose order is necessarily a product of powers of primes of P_Σ (including trivial powers). We have the following theorem:

Theorem 4.2.15. *Assume the above setup. For any nontrivial graph Γ, there exists a PRC field $K_\Gamma \supseteq K$ such that*

(1) $K_\Gamma \models \Sigma$;

(2) $\Gamma_{K_\Gamma}^{rc} \cong \Gamma$;

(3) $X(K_\Gamma) \cong X(K)$;

Proof. Assume K is formally real; if it is not the result is *Theorem 4.1.14*. We will mirror *Theorem 4.1.14–Lemma 4.1.20* closely to prove (1) & (2). We again assume familiarity with *Appendix B*.

Recall from *Construction 4.1.18* the groups D_Σ, W_Σ. Fix a nontrivial graph Γ, and consider the profinite group G_Γ from *Construction 4.1.9*. Let $\widetilde{G_\Gamma}$ be the universal Frattini cover of G_Γ with map $f : \widetilde{G_\Gamma} \to G_\Gamma$. By [CvdDM80, Corollary 54] the sorts $S_1, \ldots, S_{\widehat{p}}$ of $S(\widetilde{G}_\Gamma)$ are trivial (there is no proper normal subgroup $N \lhd \widetilde{G_\Gamma}$ with $[\widetilde{G_\Gamma} : N] \leq \widehat{p}$), and $\Gamma \cong \Gamma_{\widetilde{G_\Gamma}}$ by [FJ08, Lemma 28.6.1]. Consider further the diamond product

$\mathfrak{G}^* = \mathfrak{G}_{P_\Sigma} \diamond \widetilde{G_\Gamma}$, where $\mathfrak{G}_{P_\Sigma} = \langle G_{P_\Sigma}, G'_{P_\Sigma}, d : X(\mathfrak{G}_{P_\Sigma}) \to G_{P_\Sigma} \rangle$ is the maximal pro-$\mathcal{C}_\Sigma$ quotient of $\mathfrak{G}_K$ (*Lemma B.19*). $\mathfrak{G}^*$ is projective by *Lemma 4.2.12*, and $S(G_{P_\Sigma} \star \widetilde{G_\Gamma}) \models \Delta_4$ as previous. Indeed, if $N_i \lhd G_P \star \widetilde{G_\Gamma}$ is of index $\leq \widehat{p}$, under the projection $G_P \star \widetilde{G_\Gamma} \twoheadrightarrow G_P \star \widetilde{G_\Gamma}/N_i$ we must have $\widetilde{G_\Gamma} \leq N_i$, as otherwise $\widetilde{G_\Gamma}$ would have a proper normal subgroup of index $\leq \widehat{p}$, a contradiction to the above. By [Rot99, Theorem 2.28(ii)] there is a correspondence between closed $N_k \lhd G_P \star \widetilde{G_\Gamma}$ of index $k \leq \widehat{p}$, and closed $N'_k \lhd G_P$ of index $k \leq \widehat{p}$, with $G_P \star \widetilde{G_\Gamma}/N_k \cong G_P/N'_k$. Therefore for any $\mathcal{L}_G(\overline{a})$-sentence φ with variables over the sorts $S_1, \ldots, S_{\widehat{p}}$, $S(G_{P_\Sigma}) \models \varphi \Leftrightarrow S(G_{P_\Sigma} \star \widetilde{G_\Gamma}) \models \varphi$. That $S(G_{P_\Sigma}) \models \Delta_4$ is p. 75 exactly, with $\Sigma_2 = \Delta_4$.

We claim $\Gamma_{G'_\star} \cong \Gamma$. We (almost) repeat *Lemma 4.1.20:* note $\widetilde{G_\Gamma}, G'_{P_\Sigma} \leq G'_\star$, and

$$\widetilde{G_\Gamma} \cong (G_{P_\Sigma} \star \widetilde{G_\Gamma})/\langle G_{P_\Sigma} \rangle \cong G'_\star/(G'_\star \cap \langle G_{P_\Sigma} \rangle).$$

(The second isomorphism results from the *Second Isomorphism Theorem for Groups.*) Hence there is an epimorphism $\pi : G'_\star \to \widetilde{G_\Gamma}$ which yields an embedding $\Gamma_{\widetilde{G_\Gamma}} \hookrightarrow \Gamma_{G'_\star}$. Conversely, if $M \lhd G'_\star$ is open and $G'_\star/M \cong D_\Sigma$ (resp. W_Σ), under $\rho : G'_\star \twoheadrightarrow D_\Sigma$ (resp. W_Σ) we have $\rho(G'_{P_\Sigma}) \leq D_\Sigma$ (resp. W_Σ). As G'_{P_Σ} is pro-$\mathcal{C}_\Sigma$ ([FJ08, Lemma 17.3.1]), any quotient of G'_{P_Σ} is a P_Σ-group, hence there exists elements of $\rho(G'_{P_\Sigma})$ of the wrong order unless $G'_{P_\Sigma} \leq \ker(\rho)$. Hence $\ker(\pi) \leq \ker(\rho)$, thus $M = \pi^{-1}(\pi(M))$, and therefore π^{-1} induces an isomorphism of graphs $\Gamma_{G'_\star} \cong \Gamma$ as claimed.

The canonical graph structure for $\mathfrak{G}^*$ is also recovered correctly:

$$\begin{aligned}
\Gamma_{\mathfrak{G}^*} &= \Gamma_{\mathfrak{G}^*, X(\mathfrak{G}^*)/G'_\star} && \text{by definition,} \\
&\cong \Gamma_{F(X(\mathfrak{G}^*)/G'_\star, G'_\star), X(\mathfrak{G}^*)/G'_\star} && \text{by definition,} \\
&\cong \Gamma_{F(X(\mathfrak{G}_{P_\Sigma})/G'_{P_\Sigma}, G'_\star), X(\mathfrak{G}_{P_\Sigma})/G'_{P_\Sigma}} && \text{by } \textit{Lemma 4.2.11}, \\
&\cong \Gamma_{G'_\star} && \text{by } \textit{Lemma 4.2.11,} \\
&\cong \Gamma && \text{by the above.}
\end{aligned}$$

There is an epimorphism of Artin-Schreier structures $\mathfrak{G}_{P_\Sigma} \twoheadrightarrow \mathfrak{Gal}(K_{\mathrm{bad}}/K)$. Indeed, as $G_{P_\Sigma} = G_K/N_{\mathcal{C}_\Sigma}$, if $E_{\mathcal{C}_\Sigma}$ is the fixed field $(\widetilde{K})^{N_{\mathcal{C}_\Sigma}}$ then we have the tower

of fields $\widetilde{K}/E_{\mathcal{C}_\Sigma}/K_{\mathrm{bad}}/K$ by design. *Example B.8* ensures there is an epimorphism $\mathfrak{G}_{P_\Sigma} \twoheadrightarrow \mathfrak{Gal}(K_{\mathrm{bad}}/K)$. By *Corollary 4.2.6* there is an extension K_Γ of K that is PRC, $K_\Gamma \cap K_{\mathrm{bad}} = K$, and $\mathfrak{G}_{K_\Gamma} \cong \mathfrak{G}^*$. Thus, $S(G_{K_\Gamma}) \models \Delta_4$, and $K_\Gamma \models \Delta_3$. Therefore $K_\Gamma \models \Delta_1 \cup \Delta_2 \cup \Delta_3 \cup \Delta_4^*$ (implying $K_\Gamma \models \Sigma$), and from *Lemma 4.2.11*,

$$\Gamma_{K_\Gamma}^{rc} \cong \Gamma_{\mathfrak{G}_{K_\Gamma},\, X(K_\Gamma)} \cong \Gamma_{\mathfrak{G}^*,\, X(\mathfrak{G}^*)/G'_\star} \cong \Gamma,$$

This proves (1) & (2). The proof of (3) is a direct consequence of the above setup: $X(K_\Gamma) \cong X(\widetilde{K_\Gamma}/K_\Gamma)/G_{K_\Gamma(\sqrt{-1})} \cong X(\mathfrak{G}^*)/G'_\star$, as $\mathfrak{G}_{K_\Gamma} \cong \mathfrak{G}^*$. Furthermore:

$$\begin{aligned}
X(\mathfrak{G}^*)/G'_\star &= \mathrm{Inv}(G_{P_\Sigma} \star \widetilde{G_\Gamma})/G'_\star \\
&\cong \mathrm{Inv}(G_{P_\Sigma})/G'_{P_\Sigma} && \text{from}^{12}\ \text{[HR85, Theorem A]}, \\
&\cong X(\mathfrak{G}_{P_\Sigma})/G'_{P_\Sigma} && \text{as } \mathfrak{G}_{P_\Sigma} \text{ is projective; [HJ85, Proposition 7.4]}, \\
&= X(\mathfrak{G}_K/N_{\mathcal{C}_\Sigma})/(G'_K/N_{\mathcal{C}_\Sigma}) \\
&= (X(\mathfrak{G}_K)/N_{\mathcal{C}_\Sigma})/(G'_K/N_{\mathcal{C}_\Sigma}).
\end{aligned}$$

Notice $X(\mathfrak{G}_K)/G'_K \cong (X(\mathfrak{G}_K)/N_{\mathcal{C}_\Sigma})/(G'_K/N_{\mathcal{C}_\Sigma})$ as $\mathfrak{G}_K \twoheadrightarrow \mathfrak{G}_K/N_{\mathcal{C}_\Sigma}$ is a cover. Finally, $X(\mathfrak{G}_K)/G'_K \cong X(K)$ ensuring $X(K_\Gamma) \cong X(K)$; the order space of K_Γ is up to homeomorphism that of K. ■

Corollary 4.2.16. *Every PRC field is finitely undecidable.*

Proof. Fix K a PRC field and $\Sigma \subset \mathtt{Th}(K; \mathcal{L}_r)$ a finite subtheory. Assume K is formally real (otherwise the result is *Corollary 4.1.21*). Let Γ be a nontrivial graph; by *Lemma 4.2.13 & Theorem 4.2.15* there exists a PRC field $K_\Gamma \models \Sigma$ and Γ is interpretable in K_Γ. Furthermore, the interpretation of *Lemma 4.2.13* is uniform in the sense of *Definition A.6*; the class of nontrivial graphs is uniformly interpretable in the class of PRC fields satisfying Σ. We conclude $\mathtt{PRC} \cup \Sigma$ is hereditarily undecidable by *Corollary A.15*, hence Σ is undecidable as required. ■

[12] The involutions of $G_{P_\Sigma} \star \widetilde{G_\Gamma}$ are exactly the conjugates of $\mathrm{Inv}(G_{P_\Sigma})$ in $G_{P_\Sigma} \star \widetilde{G_\Gamma}$, by [HR85, Theorem A]. Therefore the morphism $\mathfrak{G}^* \to \mathfrak{G}_{P_\Sigma}$ induces a continuous *bijection* $\mathrm{Inv}(G_{P_\Sigma} \star \widetilde{G_\Gamma})/G'_\star \to \mathrm{Inv}(G_{P_\Sigma})/G'_{P_\Sigma}$.

Corollary 4.2.17. *No PRC field is finitely axiomatisable.* ■

Remark 4.2.18. In 2014, Shlapentokh & Videla [SV14, §6] posed three open questions about finite undecidability (recall their term is '*finite hereditary* undecidability'):

(1) *"It is known that the theory of the field of all totally real algebraic numbers is decidable ... Is this theory finitely hereditarily undecidable?"*

(2) *"Is the theory of pseudo real closed fields ... finitely hereditarily undecidable?"*

(3) *"In general, if $\mathfrak{T}$ is a theory of any subfield of $\widetilde{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$, is $\mathfrak{T}$ finitely hereditarily undecidable?"*

(Quotes from [SV14, p. 1262].) We may answer these as follows:

(1) By Pop [Pop90], the field $\mathbb{Q}^{tr}$ of totally real algebraic numbers is PRC, hence by *Corollary 4.2.16* the answer to (1) is *yes*.

(2) As posed, this is covered by Haran [Har84], however *Corollary 4.2.16* answers in the positive the more general subsequent question: *is the theory of any pseudo real closed field finitely undecidable?* (Equivalently: *is any completion of the theory of PRC fields finitely undecidable?*)

(3) We cannot answer this in full generality, though we make the following comment: as $\mathrm{Gal}(\widetilde{\mathbb{Q}}/\,\mathbb{Q})$ is profinite, it has a unique Haar measure μ [FJ08, Prop. 18.2.1]. By the PAC Nullstellensatz [Jar72, Theorem 2.5], the fixed field $\widetilde{\mathbb{Q}}(\sigma_1, \ldots, \sigma_n)$ is PAC for a μ-measure 1 subset of $\mathrm{Gal}(\widetilde{\mathbb{Q}}/\,\mathbb{Q})^n$. By *Corollary 4.1.21*, we conclude finite undecidability 'for almost all' fixed fields $\widetilde{\mathbb{Q}}(\sigma_1, \ldots, \sigma_n)$. Of course, with *Corollary 4.2.16*, we know there are even more infinite algebraic extensions $R/\mathbb{Q}$ with R finitely undecidable, namely the formally real PRC fields R. □

The move from PAC to PRC is also quite natural from the perspective of classification theory. Recall the definition of a (super)rosy theory from §1.3.1. The following is [Kru15, Conjecture 3]:

Conjecture (Superrosy Fields). *Every infinite superrosy field is perfect, bounded, and PRC.* ■

Corollary 4.2.19. *Assume the Superrosy Fields Conjecture. Then every infinite superrosy field is finitely undecidable.* ■

This conjecture arises from the supersimplicity context, and also the fact that a PRC field is superrosy if and only if it is perfect and bounded [Kru15, Fact 4.1]. Another result in this area is that any PRC field that is not algebraically nor real closed is not NIP [Mon17, Theorem 4.10], but not much more is known. As far as the author is aware, there are no classification-theoretic conjectures for infinite fields other than these; in particular there have been no conjectures on infinite rosy, NTP_2 or NSOP_1 fields. One would posit, however, given the few examples we have of these fields, an understanding of PAC, PRC and PpC[13] fields will be crucial. (For example, it is known that ω-free PAC fields of characteristic 0 are strictly NSOP_1 [CR16, Corollary 6.8], and a nontrivial ultraproduct of $\mathbb{Q}_p$ over primes p is strictly NTP_2 [Che14, Example 7.7 (2)].)

To conclude this section, we can recover the specific proof of *Theorem 4.1.7* in the PRC field context – that is, we do not need to conclude this using finite undecidability. The ingredients of this proof (and that of *Theorem 4.1.7*) are considerably more accessible than the ingredients of *Corollary 4.2.16* (resp. *Corollary 4.1.21*), hence we may speculate this argument could work in a considerably broader context – for example, in §4.3, where we do *not* have a finite undecidability result.

Theorem 4.2.20. *No PRC field is finitely axiomatisable (even among the class of PRC fields).*

This is to say that, given a PRC field L, there does not exist an $\mathcal{L}_r$-sentence γ such that for all PRC fields F of the same characteristic and degree of imperfection as L, $F \models \gamma \iff F \equiv_{\mathcal{L}_r} L$.

Proof. Assume for the purpose of contradiction that there is a formally real finitely axiomatisable PRC field K (see *Theorem 4.1.7* for when K is PRC but not formally

[13] *Pseudo-p-adically closed fields*, discussed in §4.3.

real). In order to characterise K among PRC fields, by *Corollary 4.2.8* we need only finitely many axioms $\Sigma_1 \subset \mathtt{Th}^{alg}(K)$ and $\Sigma_2^* \subset \mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$, where $\Sigma_2 \subset \mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))$ is finite.

Let Λ be the set of universal sentences of Σ_1, and let K_{bad} be the join of $K(\sqrt{-1})$ and of minimal Galois extensions F/K within a fixed algebraic closure $\widetilde{K}$ of K, with $F \models \neg\lambda$ for $\lambda \in \Lambda$. Then K_{bad}/K is finite, $K_{\mathrm{bad}} \models \neg\Lambda$, and $\mathrm{Res} : \mathfrak{G}_K \to \mathfrak{Gal}(K_{\mathrm{bad}}/K)$ is a cover (*Example B.8*). As there is an epimorphism $G_K \twoheadrightarrow \mathrm{Gal}(K_{\mathrm{bad}}/K)$ (apply the forgetful functor to Res) there is an embedding of $\mathcal{L}_G$-structures $S(\mathrm{Gal}(K_{\mathrm{bad}}/K)) \hookrightarrow S(G_K)$.

Let $\overline{a} \in S(G_{K_0}) \subset S(G_K)$ be a finite tuple of elements such that Σ_2 is a set of finitely many $\mathcal{L}_G(\overline{a})$-sentences. Fix $n_k \in \mathbb{N}$ such that $S_1, \ldots, S_{n_k}$ is the smallest consecutive sequence of sorts involving the sentences of Σ_2. Let $\widehat{p}$ be the smallest prime larger than $n_k + |\mathrm{Gal}(K_{\mathrm{bad}}/K)|$, P the set of primes $\{2, 3, \ldots, \widehat{p}\}$, and $\mathcal{C}$ the formation of finite groups whose order is necessarily a product of powers of primes of P (including trivial powers). As this formation is full, and $\mathfrak{G}_K$ is projective (*Theorem 4.2.4*), the maximal pro-$\mathcal{C}$ quotient of $\mathfrak{G}_K$, denoted $\mathfrak{G}_P$, is also projective (*Lemma B.19*). There is an epimorphism $\mathfrak{G}_P \twoheadrightarrow \mathfrak{Gal}(K_{\mathrm{bad}}/K)$ (*Example B.8*) and by construction $S(\mathrm{Ft}(\mathfrak{G}_P)) \models \Sigma_2$ (cf. p. 75).

Let $\mathbb{F}_1(q)$ be the free pro-q group on one generator, where q is a prime larger than $\widetilde{p}$. This is a projective profinite group. Consider $\mathfrak{G}_P \diamond \mathbb{F}_1(q)$; by *Lemma 4.2.12* this is a projective Artin-Schreier structure. The $\mathcal{L}_G$-theories of the profinite groups $\mathrm{Ft}(\mathfrak{G}_P \diamond \mathbb{F}_1(q))$ and $\mathrm{Ft}(\mathfrak{G}_P)$ differ: there are group epimorphisms from $\mathrm{Ft}(\mathfrak{G}_P \diamond \mathbb{F}_1(q))$ to finite groups of order q, arising from the forgetful functor, however there are no such epimorphisms for $\mathrm{Ft}(\mathfrak{G}_P)$ by construction. However $S(\mathrm{Ft}(\mathfrak{G}_P \diamond \mathbb{F}_1(q))) \models \Sigma_2$ (as on p. 76, from $S(\mathrm{Ft}(\mathfrak{G}_P)) \models \Sigma_2$).

There is an epimorphism $\mathfrak{G}_P \diamond \mathbb{F}_1(q) \twoheadrightarrow \mathfrak{G}_P$ as one might expect, hence by composition there is an epimorphism $\mathfrak{G}_P \diamond \mathbb{F}_1(q) \twoheadrightarrow \mathfrak{Gal}(K_{\mathrm{bad}}/K)$. By *Corollary 4.2.6* there exist PRC fields $E_1, E_2 \supseteq K$ such that $\mathfrak{G}_{E_1} \cong \mathfrak{G}_P$ and $\mathfrak{G}_{E_2} \cong \mathfrak{G}_P \diamond \mathbb{F}_1(q)$. Moreover, $E_1 \cap K_{\mathrm{bad}} = E_2 \cap K_{\mathrm{bad}} = K$, therefore $E_1, E_2 \models \Sigma_1$. We conclude $E_1, E_2 \models \Sigma_1 \cup \Sigma_2^*$ however $E_1 \not\equiv E_2$ as $S(\mathrm{Ft}(\mathfrak{G}_{E_1})) \not\equiv_{\mathcal{L}_G} S(\mathrm{Ft}(\mathfrak{G}_{E_2}))$; a contradiction, as required. ■

4.3 Pseudo-p-Adically Closed Fields

The definition of a *pseudo-p-adically closed field* is the natural step after that of PAC and PRC fields, from both an algebraic and model-theoretic standpoint. We shall assume the reader is familiar with these fields, and the paper [HJ88] – if not, see *Appendix C* for a brief introduction and important notation.

One might naturally expect the case of PpC fields to be more intricate than what followed previously; the approach of this thesis is through the absolute Galois group of such fields, and even for $\mathbb{Q}_p$, $\mathtt{Th}(S(G_{\mathbb{Q}_p}); \mathcal{L}_G)$ is monstrous compared to $\mathtt{Th}(S(G_K); \mathcal{L}_G)$ for K algebraically, real, or separably closed. A paper of Efrat recovers Haran's result:

Theorem 4.3.1. [Efr92, Corollary 4.3]. *The theory of formally p-adic PpC fields is undecidable*[14]. ■

We are unable to prove the finite undecidability of any PpC field (see *Remark 4.3.11*). In line with *Theorems 4.1.7 & 4.2.20*, we are able to show:

Theorem 4.3.9. *No bounded PpC field is finitely axiomatisable (even among the class of PpC fields).*

(Recall a field K is *bounded* if for every $n > 1$ there are finitely many Galois extensions L/K with $[L : K] = n$.) Before this, we have the following facts: recall from *Appendix C* the category of $G_{\mathbb{Q}_p}$-structures, and *Definition C.17 & Remark C.18.*

Theorem 4.3.2. ([HJ88, Theorems 15.1 & 15.3]; cf. *Theorem 15.4 ibid.*) *If K is a PpC field, then $\mathfrak{G}_K$ is projective (as a $G_{\mathbb{Q}_p}$-structure). Conversely, if $\mathfrak{G}$ is a projective $G_{\mathbb{Q}_p}$-structure, there exists a PpC field K such that $\mathfrak{G} \cong \mathfrak{G}_K$.* ■

Furthermore, we have a corresponding *Theorem 4.1.5/Theorem 4.2.5:*

Definition 4.3.3. A field extension L/K is *totally p-adic* if the restriction map[15] $\mathrm{Res} : X(L) \to X(K)$ is surjective.

[14] In fact, *hereditarily* undecidable: Ershov's remark [Ers81, p. 260] on his proof of the hereditary undecidability of `PAC` applies here.

[15] See *Definition C.16* for the *space of sites* $X(F)$ of a field F.

Theorem 4.3.4. [HJ88, Theorem 15.3]. *Let $\mathfrak{G}$ be a projective $G_{\mathbb{Q}_p}$-structure. Let L/K be a Galois extension and $\pi : \mathfrak{G} \to \mathfrak{Gal}(L/K)$ be an epimorphism. Then there exists a totally p-adic PpC extension E/K such that $\mathfrak{G} \cong \mathfrak{G}_E$, and*

$$\begin{array}{ccc} \mathfrak{G} & \xrightarrow{\cong} & \mathfrak{G}_E \\ & \searrow^{\pi} & \downarrow Res_L \\ & & \mathfrak{Gal}(L/K) \end{array}$$

is a commutative diagram. ■

This is to say we have 'correctly' extended all the p-adic valuation data from K to L. In the PRC setting we used *totally real extensions* (on p. 94) via a similar characterisation. Also note that *Theorem 4.3.4* has the corollary:

Corollary 4.3.5. (cf. *Corollary 4.2.6.*) *Let L/K be a Galois extension, $\mathfrak{G}$ a projective $G_{\mathbb{Q}_p}$-structure, and $\alpha : \mathfrak{G} \to \mathfrak{Gal}(L/K)$ an epimorphism. Then K has a totally p-adic extension E which is PpC, $E \cap L = K$, and there exists an isomorphism $\gamma : \mathfrak{G}_E \to \mathfrak{G}$ such that $\alpha \circ \gamma = Res_L$.* ■

As before, the Galois-theoretic information of a PpC field, along with some arithmetic information, completely determines that field's ($\mathcal{L}_r$-)theory:

Theorem 4.3.6. *Let K_1, K_2 be PpC fields, separable over a common subfield E. Then $K_1 \equiv_E K_2$ if and only if K_1 & K_2 have the same degree of imperfection, there exists $\theta \in G_E$ such that $\theta(K_1 \cap E^s) = K_2 \cap E^s$, and if $S\Theta : S(G_{K_1 \cap E^s}) \to S(G_{K_2 \cap E^s})$ is the isomorphism induced by θ, then the partial map $S\Theta : S(G_{K_1}) \to S(G_{K_2})$ with domain $S(G_{K_1 \cap E^s})$ is $\mathcal{L}_G$-elementary.*

Proof (Sketch). As in *Theorem 4.2.7.* Note this now requires a "PpC embedding lemma", i.e. *if K_1 and K_2 are formally p-adic PpC fields that contain a common field E, and supposing that there exists a homeomorphism $\varphi : G_{K_1} \to G_{K_2}$ such that for every $\sigma \in G_{K_1}$, $\varphi(\sigma)|_{E^s} = \sigma|_{E^s}$; then $K_1 \equiv_E K_2$.* Such a lemma is provided by [Kün89, Lemma 5 & Proposition 6]. ■

Corollary 4.3.7. *A PpC field K is axiomatised by the following first-order $\mathcal{L}_r$-axiom scheme:*

(1) The characteristic and degree of imperfection of K;

(2) The PpC field axioms, $\mathtt{PpC}$;

(3) $\mathtt{Th}^{alg}(K)$;

(4) $\mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$. ■

(Recall *Remark 4.1.3*, and that $K_0 = K \cap \mathbb{F}^s$ where $\mathbb{F}$ is the prime subfield of K.)

Let us repeat *Lemma 4.2.12* and prove there is a 'counterfeit' coproduct in the category of $G_{\mathbb{Q}_p}$-structures, sufficiently similar to the real thing:

Lemma 4.3.8. *Let G be a $G_{\mathbb{Q}_p}$-projective group, and E a projective profinite group. Then $G \star E$ is a $G_{\mathbb{Q}_p}$-projective group.*

Proof. (cf. the 'manual' proof of *Lemma 4.2.12*.) Let the following be a finite $G_{\mathbb{Q}_p}$-embedding problem (recall *Definition C.9*) for G:

$$\begin{array}{ccc} & & G \star E \\ & & \downarrow \varphi \\ B & \xrightarrow{\alpha} \!\!\!\rightarrow & A \end{array} \tag{4.1}$$

This diagram gives rise to the following two:

$$\begin{array}{ccc} & & G \\ & & \downarrow \varphi|_G \\ B & \xrightarrow{\alpha} \!\!\!\rightarrow & A \end{array} \qquad\qquad \begin{array}{ccc} & & E \\ & & \downarrow \varphi|_E \\ B & \xrightarrow{\alpha} \!\!\!\rightarrow & A \end{array}$$

The latter is solvable, as E is projective. We claim the former is in fact a $G_{\mathbb{Q}_p}$-embedding problem. Indeed[16], $\mathcal{D}(G) \hookrightarrow \mathcal{D}(G \star E)$ as $G \leq G \star E$, so if $H \in \mathcal{D}(G)$ there exists $\gamma_H : H \to B$ with $\alpha \circ \gamma_H = \varphi|_H = (\varphi|_G)|_H$. Therefore, as G is $G_{\mathbb{Q}_p}$-projective, we conclude the former diagram is solvable:

[16]Recall from *Appendix C* the notation $\mathcal{D}(G) = \{H \leq G : H \cong G_{\mathbb{Q}_p}\}$ for a profinite group G.

By definition of the free product, there exists a morphism $\gamma : G \star E \to A$ uniquely extending $\varphi|_G$, $\varphi|_E$, and making (4.1) commute. Finally, we must show $\mathcal{D}(G \star E) = \{H \leq G \star E : H \cong G_{\mathbb{Q}_p}\}$ is (topologically) closed in $\mathrm{Subg}(G \star E)$ – however this is always the case for $G_{\mathbb{Q}_p}$-structures by a minor adaptation of [Feh10, Lemma 3.5.1]:

Claim. *Let G be a profinite group. Then $\mathcal{D}(G)$ is closed in* $\mathrm{Subg}(G)$.

Proof. Cf. [Feh10, Lemma 3.5.1]. Consider $H \in \mathrm{Subg}(G)$ such that $H \ncong G_{\mathbb{Q}_p}$. As $G_{\mathbb{Q}_p}$ is finitely generated, by [Feh10, Lemma 1.3.2 (1)] there exists $H_0 \triangleleft H$ open such that H/H_0 is not a quotient of $G_{\mathbb{Q}_p}$. Fix $N \triangleleft G$ open with $N \cap H \leq H_0$ (which exists by [FJ08, Lemma 1.2.5 (a)]). As $H/(N \cap H) \supseteq H/H_0$, $H/(N \cap H)$ is also not a quotient of $G_{\mathbb{Q}_p}$. If $H' \leq G$ and $H'N = HN$, then $H'/(N \cap H') \cong H'N/N \cong HN/N \cong H/(N \cap H)$. Hence $H'/(N \cap H')$ is also not a quotient of $G_{\mathbb{Q}_p}$, meaning $H' \ncong G_{\mathbb{Q}_p}$. We have shown the "strict" neighbourhood $v(H, N) \subseteq \mathrm{Subg}(G) \setminus \mathcal{D}(G)$ (see *Remark C.7*), hence $\mathcal{D}(G)$ is closed, as desired. ♦

This also concludes the proof of the lemma. ■

Theorem 4.3.9. *No bounded PpC field is finitely axiomatisable (even among the class of PpC fields).*

This is to say that, given a bounded PpC field L, there does not exist an $\mathcal{L}_r$-sentence γ such that for all PpC fields F of the same characteristic and degree of imperfection as L, $F \models \gamma \iff F \equiv_{\mathcal{L}_r} L$.

Proof. Assume for the purpose of contradiction that there is a formally p-adic finitely axiomatisable bounded PpC field K (see *Theorem 4.1.7* for when K is PpC but not formally p-adic). In order to characterise K among PpC fields, by *Corollary 4.3.7* we need only finitely many axioms $\Sigma_1 \subset \mathtt{Th}^{alg}(K)$ and $\Sigma_2^* \subset \mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))^*$,

where $\Sigma_2 \subset \mathtt{Th}(S(G_K); \mathcal{L}_G(S(G_{K_0})))$ is finite.

Let Λ be the set of universal sentences of Σ_1, and let K_{bad} be the join of minimal Galois extensions F/K within a fixed algebraic closure $\widetilde{K}$ of K, with $F \models \neg\lambda$ for $\lambda \in \Lambda$. Then K_{bad}/K is finite, $K_{\mathrm{bad}} \models \neg\Lambda$, and $\mathrm{Res} : \mathfrak{G}_K \to \mathfrak{Gal}(K_{\mathrm{bad}}/K)$ is a cover (*Remark C.18*). As there is an epimorphism $G_K \twoheadrightarrow \mathrm{Gal}(K_{\mathrm{bad}}/K)$ – apply the forgetful functor to Res – there is an embedding of $\mathcal{L}_G$-structures $S(\mathrm{Gal}(K_{\mathrm{bad}}/K)) \hookrightarrow S(G_K)$.

Let $\overline{a} \in S(G_{K_0}) \subset S(G_K)$ be a finite tuple of elements such that Σ_2 is a set of finitely many $\mathcal{L}_G(\overline{a})$-sentences. Fix $n_k \in \mathbb{N}$ such that $S_1, \ldots, S_{n_k}$ is the smallest consecutive sequence of sorts involving the sentences of Σ_2. Let $\widehat{p}$ be the smallest prime larger than $n_k + |\mathrm{Gal}(K_{\mathrm{bad}}/K)|$ and $\mathbb{F}_1(q)$ be the free pro-q group on one generator, where q is a prime larger than $\widetilde{p}$. This is a projective profinite group. Consider $G_K \star \mathbb{F}_1(q)$; by *Lemma 4.3.8* this is a $G_{\mathbb{Q}_p}$-projective group, and $S(G_K \star \mathbb{F}_1(q)) \models \Sigma_2$ (as on p. 76, from $S(G_K) \models \Sigma_2$). However the $\mathcal{L}_G$-theories of $S(G_K \star \mathbb{F}_1(q))$ and $S(G_K)$ differ: indeed, as K is bounded, G_K is small (as a profinite group) hence there are $1 \leq n_q < \infty$ many open normal subgroups of G_K of index $\leq q$. Consider the sentence

$$\varphi_{n_q} : \qquad \exists N_0, \ldots, N_{n_q} \in S_q \left(\bigwedge_{\substack{i \neq j \\ 0 \leq i,j \leq n_q}} \neg(N_i \leq N_j \wedge N_j \leq N_i) \right),$$

where S_q denotes sort q, $N_i = g_i M_i$ is a coset of an open $M_i \triangleleft G_K$ of index $\leq q$, and recall $N_i \leq N_j \iff M_i \subseteq M_j$. This sentence expresses "there are $n_q + 1$ distinct open normal subgroups of index $\leq q$", and clearly $S(G_K) \not\models \varphi_{n_q}$ while $S(G_K \star \mathbb{F}_1(q)) \models \varphi_{n_q}$.

Let $\mathfrak{G}_K \diamond \mathbb{F}_1(q)$ be a projective $G_{\mathbb{Q}_p}$-structure with underlying group $G_K \star \widetilde{G_\Gamma}$, from *Theorem C.11*. By *Theorem 4.3.4* (setting $L = K$) there exist totally p-adic PpC fields $E_1, E_2 \supseteq K$ such that $\mathfrak{G}_{E_1} \cong \mathfrak{G}_K$ and $\mathfrak{G}_{E_2} \cong \mathfrak{G}_K \diamond \mathbb{F}_1(q)$. As there are epimorphisms $G_{E_1} \cong G_K \twoheadrightarrow \mathrm{Gal}(K_{\mathrm{bad}}/K)$, $G_{E_2} \cong G_K \star \widetilde{G_\Gamma} \twoheadrightarrow G_K \twoheadrightarrow \mathrm{Gal}(K_{\mathrm{bad}}/K)$, $E_1 \cap K_{\mathrm{bad}} = E_2 \cap K_{\mathrm{bad}} = K$, therefore $E_1, E_2 \models \Sigma_1$. We conclude $E_1, E_2 \models \Sigma_1 \cup \Sigma_2^*$ however $E_1 \not\equiv E_2$ as $S(G_{E_1}) \not\equiv_{\mathcal{L}_G} S(G_{E_2})$; a contradiction, as required. ■

Remark 4.3.10. Again, there is a classification-theoretic connection: every bounded

PpC field has an NTP$_2$ $\mathcal{L}_r$-theory [Mon17, Corollary 8.6], and it is conjectured ([CKS15, Conjecture 5.1]) that NTP$_2$ PpC fields are bounded. □

Remark 4.3.11. We are unable to prove formally p-adic PpC fields are finitely undecidable – indeed, difficulties arise adapting the previous proofs to the p-adic context, simply because $G_{\mathbb{Q}_p}$ has a more complicated $\mathcal{L}_G$-structure theory than $\mathbb{Z}/2\,\mathbb{Z}$ $(= G_{\mathbb{R}})$ or $\{1\}$ $(= G_{\mathbb{C}})$.

The first fundamental issue is that, if $\mathcal{C}$ is a full formation of finite P-groups where P is a finite set of consecutive primes $\{2, 3, \ldots, \widehat{p}\}$, it is not true that the maximal pro-$\mathcal{C}$ quotient of a $G_{\mathbb{Q}_p}$-projective group remains $G_{\mathbb{Q}_p}$-projective. Indeed, the absolute Galois group of a formally p-adic PpC field K admits embeddings $G_{\mathbb{Q}_p} \hookrightarrow G_K$ by [HJ88, Lemma 5.3]; impossible if G_K is pro-$\mathcal{C}$.

The second fundamental issue is the following: let K be a PAC (resp. PRC) field, $\Sigma \subset \mathtt{Th}(K; \mathcal{L}_r)$ a finite subtheory, and Γ be a nontrivial graph. In *Theorem 4.1.14* (resp. *Theorem 4.2.15*), the field K_Γ constructed has absolute Galois group $H \star \widetilde{G_\Gamma}$ where H is projective (resp. real projective) and has no open normal subgroups of index $n_\Sigma = |D_\Sigma|$ or $|W_\Sigma|$. If H is the absolute Galois group of a formally p-adic PpC field, we cannot be guaranteed that any index n_Σ open normal subgroup of $H \star \widetilde{G_\Gamma}$ contains H. Consequently, although $\Gamma \hookrightarrow \Gamma_{H \star \widetilde{G_\Gamma}}$ $(= \Gamma_{G_{K_\Gamma}}$, interpretable in K_Γ by [Efr92, Lemma 4.1]) we cannot guarantee these graphs are isomorphic. □

Appendices

A Two Key Hereditary Undecidability Results

In *Chapters 3 & 4* we require specific pieces of 20^{th} century computability (whose exposition in the least is) due to Tarski, Mostowski, R. Robinson, and Ershov, Lavrov, Taimanov & Taitslin.

Let $\mathcal{L}$ be a language. Recall an $\mathcal{L}$-theory T is *essentially undecidable* if T and every consistent extension of T in the same language is undecidable, i.e. every model of T has an undecidable theory. The prototypical example is *Robinson arithmetic*; denoted Q, this is a finitely axiomatised essentially undecidable fragment of $\mathtt{Th}(\mathbb{N};\mathcal{L}_r)$, due to R. Robinson [Rob50]. A theory T is *hereditarily undecidable* if T and every nonempty subtheory of T in the same language is undecidable. By Tarski et al. [TMR53, I] (and explicitly stated by Ershov et al. [ELTT65, Corollary 3.4.1]), every finitely axiomatised undecidable theory is hereditarily undecidable – hence Robinson's Q is hereditarily undecidable. As is e.g. $\mathtt{Th}(\mathbb{N};\mathcal{L}_r)$, as a consequence of *Theorem A.8*.

A.1 Interpretations

Definition A.1. [Hod93, p. 58]. Let $\mathcal{L}$ be a language. Denoting variables as $x_1, x_2, \ldots$, by an *unnested atomic $\mathcal{L}$-formula* we mean an atomic $\mathcal{L}$-formula of one of the following forms:

- $x_i = x_j$;
- $x_i = c$ for some constant $c \in \mathcal{L}$;

- $f(x_{i_1}, \ldots, x_{i_n}) = x_j$ for some arity n function symbol $f \in \mathcal{L}$;
- $R(x_{i_1}, \ldots, x_{i_n})$ for some arity n relation symbol $R \in \mathcal{L}$.

Definition A.2. [Hod93, p. 212]. Let $\mathcal{L}_0$, $\mathcal{L}_1$ be languages, A an $\mathcal{L}_1$-structure and B an $\mathcal{L}_0$-structure. We define an *interpretation of B in A* to be:

(1) An $\mathcal{L}_1$-formula $\delta(x_1, \ldots, x_n)$;

(2) For every unnested atomic $\mathcal{L}_0$-formula $\phi(y_1, \ldots, y_m)$, an $\mathcal{L}_1$-formula $\phi'(\overline{x}_1, \ldots, \overline{x}_m)$ in which the $\overline{x}_i$ are disjoint n-tuples of distinct variables;

(3) A surjective function $f : \delta(A^n) \to B$,

such that for all unnested atomic $\mathcal{L}_0$-formulae ϕ and $\overline{a}_i \in \delta(A^n)$,

$$B \models \phi(f(\overline{a}_1), \ldots, f(\overline{a}_m)) \iff A \models \phi'(\overline{a}_1, \ldots, \overline{a}_m). \qquad (\dagger)$$

We say B *is interpretable in* A if there exists a interpretation of B in A. We say B is interpretable in A *with parameters* if there exists a set $S \subset A$ such that B is interpretable in the $\mathcal{L}_1(S)$-structure A.

Definition A.3. [Hod93, §5.3, Remark 4]. Let $\mathcal{L}_0$, $\mathcal{L}_1$ be recursively presented languages, A an $\mathcal{L}_1$-structure and B an $\mathcal{L}_0$-structure. We define a *recursive* interpretation of B in A to be an interpretation where the map $\phi \mapsto \phi'$ of *Definition A.2 (2)* is recursive.

E.g. if $\mathcal{L}_0$, $\mathcal{L}_1$ are finite, they are recursively presented, and an interpretation of (an $\mathcal{L}_0$-structure) B in (an $\mathcal{L}_1$-structure) A is automatically a recursive interpretation.

Remark A.4. Suppose an $\mathcal{L}_0$-structure B is interpretable in an $\mathcal{L}_1$-structure A; the map $\phi \mapsto \phi'$ on unnested atomic $\mathcal{L}_0$-formulae in *Definition A.2 (2)* may be extended to a map $-' : \mathrm{Form}(\mathcal{L}_0) \to \mathrm{Form}(\mathcal{L}_1)$, satisfying the equivalence (†); this is [Hod93, Theorem 5.3.2]. Furthermore, this map is recursive if B is recursively interpretable in A. The map $-'$ is known as the *reduction map of the interpretation.* □

Remark A.5. Let $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2$ be languages, and let A be an $\mathcal{L}_0$-structure, B an $\mathcal{L}_1$-structure, and C an $\mathcal{L}_2$-structure. If C is interpretable in B, and B is interpretable in A, then C is interpretable in A. Assuming $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2$ are recursively presented, this statement remains true if we replace "interpretable" by "recursively interpretable". □

We will also require a notion of an interpretation being 'uniform' across a class of structures.

Definition A.6. Let $\mathcal{L}_0, \mathcal{L}_1$ be finite languages, K_0 a class of $\mathcal{L}_0$-structures and K_1 a class of $\mathcal{L}_1$-structures. We say K_0 *is uniformly interpretable in* K_1 if there exists:

(1) An $\mathcal{L}_1$-formula $\delta(x_1, \ldots, x_n)$;

(2) For every unnested atomic $\mathcal{L}_0$-formula $\phi(y_1, \ldots, y_m)$, an $\mathcal{L}_1$-formula $\phi'(\overline{x}_1, \ldots, \overline{x}_m)$ in which the $\overline{x}_i$ are disjoint n-tuples of distinct variables;

such that for any $B \in K_0$ there exists:

- $A \in K_1$;
- A surjective function $f_{AB} : \delta(A^n) \to B$ such that for all unnested atomic $\mathcal{L}_0$-formulae ϕ and $\overline{a}_i \in \delta(A^n)$, $B \models \phi(f_{AB}(\overline{a}_1), \ldots, f_{AB}(\overline{a}_m)) \Leftrightarrow A \models \phi'(\overline{a}_1, \ldots, \overline{a}_m)$.

We say K_0 is *uniformly interpretable with parameters* in K_1 if there exists a finite expansion $\mathcal{L}_1'$ of $\mathcal{L}_1$ by constant symbols such that K_0 is uniformly interpretable in K_1 as a class of $\mathcal{L}_1'$-structures.

Remark A.7. A class K_0 of $\mathcal{L}_0$-structures being uniformly interpretable with parameters in a class K_1 of $\mathcal{L}_1$-structures is what Ershov refers to as 'K_0 being *relatively elementarily definable* in K_1', in [Eršo80, pp. 271–272]. Ershov notes if K_1^* is a class of $\mathcal{L}_1$-structures containing the class K_1, and K_0 is uniformly interpretable with parameters in K_1, then K_0 is uniformly interpretable with parameters in K_1^* ([Eršo80, p. 272]). □

A.2 Undecidability

All of the undecidability results of *Chapter 3* rely on the following theorem of Tarski. General references for this material are [TMR53, ELTT65, Sho93].

Theorem A.8. (Tarski). *Let $\mathcal{L}_1$, $\mathcal{L}_2$ be finite languages. The $\mathcal{L}_2$-theory T_2 is hereditarily undecidable if there exists a finitely axiomatised essentially undecidable $\mathcal{L}_1$-theory T_1 and models $M_1 \models T_1$, $M_2 \models T_2$ such that M_1 is interpretable in M_2.*

Proof. This is [ELTT65, pp. 87–89], using different (but equivalent) terminology. Results such as this originate in [TMR53, §I.3 & §I.4]; cf. *Theorems 6, 7 & 8 ibid.* ■

We will use this as follows:

Lemma A.9. [Sho93, Proposition 11.2]. *Let $\mathcal{L}$ be a finite language and $a_1, \ldots, a_n$ constant symbols not in $\mathcal{L}$. Let M be an $\mathcal{L}(a_1, \ldots, a_n)$-structure and $M|_{\mathcal{L}}$ the reduct of M to $\mathcal{L}$. If $\mathtt{Th}(M; \mathcal{L}(a_1, \ldots, a_n))$ is hereditarily undecidable, so too is $\mathtt{Th}(M|_{\mathcal{L}}; \mathcal{L})$.* ■

Corollary A.10. *Let K be a field of characteristic 0, and L a field of characteristic $p > 0$ such that there exists $t \in L$ transcendental over $\mathbb{F}_p$. Let $\mathcal{L}$ be a finite expansion of the language of rings. Suppose $\mathbb{Z}$ is $\mathcal{L}$-definable with parameters in K and $\mathbb{F}_p[t]$ is $\mathcal{L}$-definable with parameters in L. Then $\mathtt{Th}(K; \mathcal{L})$ and $\mathtt{Th}(L; \mathcal{L})$ are hereditarily undecidable.*

Proof. This is an application of *Theorem A.8* with $\mathcal{L}_2$ an expansion of $\mathcal{L}$ by constant symbols, $\mathcal{L}_1 = \mathcal{L}_r$, $T_1 = Q$ (*Robinson arithmetic*) and $M_1 = \mathbb{N}$. Notice $\mathbb{N}$ is $\emptyset$-$\mathcal{L}_r$-definable in $\mathbb{Z}$ (e.g. $\mathbb{N} = \{n \in \mathbb{Z} : \exists x_1, x_2, x_3, x_4 \, (n = x_1^2 + x_2^2 + x_3^2 + x_4^2)\}$ by *Lagrange's Four Square Theorem*) hence interpretable in $\mathbb{Z}$. By [Rob51, §4a–4b], $\mathbb{N}$ is interpretable in the $\mathcal{L}_r(t)$-structure $\mathbb{F}_p[t]$. Thus, by assumption $\mathbb{N}$ is interpretable in K (with, say, parameters $\overline{c} = \{c_1, \ldots, c_k\}$) and $\mathbb{N}$ is interpretable in L (with, say, parameters $\overline{d} = \{d_1, \ldots, d_l\}$). By *Theorem A.8*, $\mathtt{Th}(K; \mathcal{L}(\overline{c}))$ and $\mathtt{Th}(L; \mathcal{L}(\overline{d}))$ are hereditarily undecidable. The hereditary undecidability of $\mathtt{Th}(K; \mathcal{L})$ and $\mathtt{Th}(L; \mathcal{L})$ follows from *Lemma A.9* exactly. ■

In *Chapter 4* the theory we work with is the theory of nontrivial (by which we mean the vertex set is nonempty) graphs; known to be undecidable (e.g. [FJ08, Corollary 28.5.3], which uses a key result of Lavrov [ELTT65, Theorem 3.3.3]. In [CQ52, Theorem III] Church & Quine note the theory of a binary symmetric predicate is undecidable). The theory of nontrivial graphs is *hereditarily* undecidable as it is finitely axiomatised (this is [ELTT65, Corollary 3.4.1]). It is *not* essentially undecidable, as it has decidable models (e.g. a nontrivial finite graph), however when its models are interpreted in a uniform way, the interpreting theory is forced to be hereditarily undecidable too. This is the result *Chapter 4* rests on, and what we shall prove next. (A general reference for this material is [Erš80, Chapter 5, §1].)

For the remainder of this section, all languages will be finite, hence all interpretations recursive. The following definitions were suggested to the author by E. Hrushovski (see [Hod93, pp. 221–222] for discussion):

Definition A.11. Let $\mathcal{L}_0, \mathcal{L}_1$ be finite languages, K_0 a class of $\mathcal{L}_0$-structures and K_1 a class of $\mathcal{L}_1$-structures. We say K_0 is uniformly interpretable *in the strict sense* in K_1 if K_0 is uniformly interpretable in K_1, and (following the notation of *Definition A.6*) for every $A \in K_1$ there exists $B \in K_0$ and a surjective function $f_{AB} : \delta(A^n) \to B$ such that for all unnested atomic $\mathcal{L}_0$-formulae ϕ and $\overline{a}_i \in \delta(A^n)$, $B \models \phi(f_{AB}(\overline{a}_1), \ldots, f_{AB}(\overline{a}_m)) \iff A \models \phi'(\overline{a}_1, \ldots, \overline{a}_m)$.

Let T be a theory in a language $\mathcal{L}$. Denote by $\mathbb{K}_T$ the class of all $\mathcal{L}$-structures satisfying T, and if $\mathbb{K}$ is a class of $\mathcal{L}$-structures, denote by $\mathtt{Th}(\mathbb{K}; \mathcal{L})$ the common $\mathcal{L}$-theory of $M \in \mathbb{K}$.

Definition A.12. Let $\mathcal{L}_0, \mathcal{L}_1$ be finite languages, T_0 an $\mathcal{L}_0$-theory and T_1 an $\mathcal{L}_1$-theory. We say T_0 *is interpretable* (resp. *interpretable with parameters*, resp. *interpretable in the strict sense*) *in* T_1 if $\mathbb{K}_{T_0}$ is uniformly interpretable (resp. uniformly interpretable with parameters, resp. uniformly interpretable in the strict sense) in $\mathbb{K}_{T_1}$.

This definition leads to a nice transfer of undecidability from T_0 to T_1:

Lemma A.13. *Let $\mathcal{L}_0, \mathcal{L}_1$ be finite languages, T_0 an $\mathcal{L}_0$-theory and T_1 an $\mathcal{L}_1$-theory. Suppose T_0 is interpretable in the strict sense in T_1. If T_0 is undecidable, then T_1 is undecidable.*

Proof. We will argue that if T_1 is decidable, so too is T_0. For $\varphi \in \mathrm{Sent}(\mathcal{L}_0)$, $\varphi \in T_0$ if and only if for all $M \in \mathbb{K}_{T_0}$, $M \models \varphi$. By assumption (and a consequence of *Remark A.4*), for $M \in \mathbb{K}_{T_0}$ there exists $N \in \mathbb{K}_{T_1}$ such that $N \models \varphi'$. Furthermore, for all $N \in \mathbb{K}_{T_1}$, $N \models \varphi'$: otherwise $N \models \neg\varphi'$, and as $\neg\varphi' = (\neg\varphi)'$, by *Remark A.4 & Definition A.12* there exists $M \in \mathbb{K}_{T_0}$ with $M \models \neg\varphi$, a contradiction. We conclude $\varphi \in T_0 \iff \varphi' \in T_1$. As the reduction map $-'$ is recursive and T_1 is decidable, so too is T_0. ■

Theorem A.14. (Ershov). *Let $\mathcal{L}_0, \mathcal{L}_1$ be finite languages, T_0 an $\mathcal{L}_0$-theory and T_1 an $\mathcal{L}_1$-theory. Suppose T_0 is interpretable with parameters in T_1; if T_0 is hereditarily undecidable, then T_1 is hereditarily undecidable.*

This result is originally due to Ershov ([Erš80, Chapter 5, §1.4, Theorem 2]; cf. *Remark A.7* for the terminology "relatively elementarily definable").

Proof. By *Definitions A.6 & A.12*, for some finite expansion by constants $\mathcal{L}_1^\flat \supseteq \mathcal{L}_1$, T_0 is interpretable in T_1 as an $\mathcal{L}_1^\flat$-theory. Consider the reduction map $-' : \mathrm{Form}(\mathcal{L}_0) \to \mathrm{Form}(\mathcal{L}_1^\flat)$ from *Remark A.4*. We claim $T^\circ = \{\varphi \in \mathrm{Sent}(\mathcal{L}_0) : \varphi' \in T_1\}$ is a subtheory of T_0. Indeed, define $\mathbb{K}_{T_0}^\circ$ to be the class of $\mathcal{L}_0$-structures M° such that there exists $N \in \mathbb{K}_{T_1}$ and a surjective function $f_{NM^\circ} : \delta(N^n) \to M^\circ$ such that for all unnested atomic $\mathcal{L}_0$-formulae $\phi(x_1, \ldots, x_m)$ and $\overline{a}_i \in \delta(N^n)$,

$$M^\circ \models \phi(f_{NM^\circ}(\overline{a}_1), \ldots, f_{NM^\circ}(\overline{a}_m)) \iff N \models \phi'(\overline{a}_1, \ldots, \overline{a}_m).$$

By assumption, $\mathbb{K}_{T_0} \subseteq \mathbb{K}_{T_0}^\circ$, hence $\mathtt{Th}(\mathbb{K}_{T_0}^\circ; \mathcal{L}_0) \subseteq T_0$, and $\mathbb{K}_{T_0}^\circ$ is uniformly interpretable in the strict sense in (the class of $\mathcal{L}_1^\flat$-structures) $\mathbb{K}_{T_1}$. By definition, for $\varphi \in \mathrm{Sent}(\mathcal{L}_0)$, $\varphi \in \mathtt{Th}(\mathbb{K}_{T_0}^\circ; \mathcal{L}_0) \iff \varphi' \in T_1$ and $T^\circ = \mathtt{Th}(\mathbb{K}_{T_0}^\circ; \mathcal{L}_0)$ is uniformly interpretable in the strict sense in T_1. We conclude the undecidability of T_1 from *Lemma*

A.13.

If S is a subtheory of T_1, $\mathbb{K}_{T_1} \subseteq \mathbb{K}_S$. By *Remark A.7*, T_0 is interpretable with parameters in S, hence the above proof applies. We conclude T_1 is *hereditarily* undecidable.

Finally, we claim that T_1 is hereditarily undecidable as an $\mathcal{L}_1$-theory. (We will follow [Sho93, Proposition 11.2] for this.) First note that if $\phi \in \mathrm{Sent}(\mathcal{L}_1^\flat)$, there exists $\phi_\flat(x_1, \ldots, x_k) \in \mathrm{Form}(\mathcal{L}_1)$ such that ϕ is obtained from $\phi_\flat$ by replacing the free occurrences of $x_1, \ldots, x_k$ by constants $c_1, \ldots, c_k \in \mathcal{L}_1^\flat \setminus \mathcal{L}_1$. Now, let S be an $\mathcal{L}_1$-subtheory of T_1; i.e. S is a subtheory of $\mathtt{Th}(\mathbb{K}_{T_1}|_{\mathcal{L}_1}; \mathcal{L}_1)$, where $\mathbb{K}_{T_1}|_{\mathcal{L}_1}$ is the class of $\mathcal{L}_1$-structures M such that $M \in \mathbb{K}_{T_1}|_{\mathcal{L}_1} \iff M^+ \in \mathbb{K}_{T_1}$, where M^+ is an expansion of M to $\mathcal{L}_1^\flat$. Let $S^\flat = \mathrm{Cons}(S)$ as a subtheory of the $\mathcal{L}_1^\flat$-theory T_1. We claim $\phi \in S^\flat \iff \forall x_1, \ldots, x_k\, \phi_\flat(x_1, \ldots, x_k) \in S$.

Indeed, $\forall x_1, \ldots, x_k\, \phi_\flat(x_1, \ldots, x_k) \in S \implies \phi \in S^\flat$ is immediate. Suppose $\phi \in S^\flat$, and consider $N \in \mathbb{K}_S$ with $n_1, \ldots, n_k \in N$. Expand N to an $\mathcal{L}_1^\flat$-structure N^+ by setting $c_1^{N^+} = n_1, \ldots, c_k^{N^+} = n_k$. As $N \models S$, $N^+ \models S^\flat$, hence $N^+ \models \phi$ and thus $N \models \phi_\flat(n_1, \ldots, n_k)$. As $N \in \mathbb{K}_S$, $n_1, \ldots, n_k \in N$ were arbitrary, $\forall x_1, \ldots, x_k\, \phi_\flat(x_1, \ldots, x_k) \in \mathtt{Th}(\mathbb{K}_S; \mathcal{L}_1) = S$ as claimed.

As $S^\flat$ is undecidable, S is undecidable. We conclude $\mathtt{Th}(\mathbb{K}_{T_1}|_{\mathcal{L}_1}; \mathcal{L}_1)$ – namely, T_1 as an $\mathcal{L}_1$-theory – is hereditarily undecidable, as required. ■

Corollary A.15. *Let $\mathbb{G}$ be the class of nontrivial graphs, and let $\mathbb{K}$ be a class of fields. Suppose $\mathbb{G}$ is uniformly interpretable with parameters in $\mathbb{K}$; then $\mathtt{Th}(\mathbb{K}; \mathcal{L}_r)$ is hereditarily undecidable.* ■

B Background on PRC fields & Artin-Schreier structures

This appendix serves as a brief overview of the parts of [HJ85] relevant to *Chapter 4*. First, a definition:

Definition B.1. [Pre81, Theorem 1.2]. A field K is *pseudo-real closed* (PRC) if every geometrically irreducible variety defined over K, which has a smooth $\overline{K}$-rational point in each real closure $\overline{K}$ of K, has a K-rational point. (If $\mathscr{V}$ is a K-variety, the $\overline{K}$-variety $\overline{\mathscr{V}} = \mathscr{V} \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{K})$ has a *smooth* $\overline{K}$-rational point $x \in \overline{\mathscr{V}}$ if $\dim \mathcal{O}_{\overline{\mathscr{V}},x} = \dim \mathfrak{m}_x/\mathfrak{m}_x^2$.)

Equivalently, a characteristic 0 field K is PRC if it is existentially closed in every field extension L to which all orderings of K extend, in which K is algebraically closed. Defining the PRC property in this manner ensures these fields enjoy the intuitive property that every algebraic extension of a PRC field is itself PRC [Pre81, Theorem 3.1]. In addition, PAC fields K can be characterised as exactly those PRC fields that are not formally real, i.e. if $X(K)$ denotes the space of orderings of K (recall §1.3), $X(K) = \emptyset$. In first-order terms, if $\mathtt{PRC}$ denotes the common $\mathcal{L}_r$-theory of PRC fields[17], then

$$\mathtt{PAC} = \mathtt{PRC} \cup \{\exists x, y\,(x^2 + y^2 = -1)\}.$$

As $\mathtt{PAC}$ is finitely undecidable (by [CvdDM80, Ers81]), so too is $\mathtt{PRC}$. Of course, we could also ask about the decidability of the theory of *formally real* PRC fields; those PRC fields that are ordered (hence are not PAC). An example of such a field to keep in mind is the field of totally real numbers $\mathbb{Q}^{tr}$ (PRC due to Pop [Pop90]). This is the maximal Galois extension of $\mathbb{Q}$ in $\mathbb{R}$; equivalently $\mathbb{Q}^{tr} = \bigcap_{\sigma \in G_{\mathbb{Q}}} \sigma(\mathbb{R} \cap \widetilde{\mathbb{Q}})$. For a class of examples, see [HJ85, §5]; in particular Proposition 5.6 *ibid.* The theory of formally real PRC fields is also undecidable:

Theorem B.2. [Har84, Theorem 3.1]. *Let Ξ be a nonempty family of Boolean spaces*[18]*, and $\mathtt{PRC}(\Xi)$ the elementary theory of the class of PRC fields K such that $X(K) \in \Xi$. Then $\mathtt{PRC}(\Xi)$ is undecidable.* ■

[17] This is first-order $\mathcal{L}_r$-axiomatisable by [Pre81, Theorem 4.1].
[18] Defined below in *Definition B.3.*

Haran's proof is quite beautiful, and is achieved by realising two clever ideas: the first is that, as the absolute Galois groups of PAC fields are exactly the projective profinite groups, a matching structure theory can and should be developed for the absolute Galois groups of PRC fields K – structures that can 'see' to some extent the orderings on K. The second clever idea is to construct a functor that allows one to pass the relevant graph constructions from the category of profinite groups to this new PRC field context. We will outline the new 'absolute structures' for PRC fields, first fashioned in [HJ85].

Definition B.3. A *Boolean space* is a totally disconnected compact Hausdorff space (equivalently, the inverse limit of finite discrete spaces, or a set homeomorphic to a closed subset of $\{-1,1\}^I$ for some set I).

Example B.4. The set of orderings of a PRC field K with the Harrison topology (§1.3) is an example of a Boolean space – as is any profinite group viewed topologically. □

Definition B.5. An *Artin-Schreier structure* is a system $\mathfrak{G} = \langle G, G', X(\mathfrak{G}) \xrightarrow{d} G \rangle$, where G is a profinite group, G' is an open subgroup of G of index ≤ 2, $X(\mathfrak{G})$ is a Boolean space[19] on which G acts continuously, and d is a continuous map (known as the *forgetful map*) such that for every $x \in X(\mathfrak{G})$:

(1) $d(x)$ is an involution, $d(x) \notin G'$, and $d(x^\sigma) = (d(x))^\sigma$ for every $\sigma \in G$;

(2) $\{\sigma \in G : x^\sigma = x\} = \{1, d(x)\}$.

If $\mathfrak{G}$ satisfies only (1) it is a *weak Artin-Schreier structure.*

Example B.6. A reference for this example is [HJ85, §2 & Example 3.2]. Suppose L/K is a Galois extension, and $\sqrt{-1} \in L$. Let $X(L/K)$ be the space of maximal ordered subfields of L; the set of pairs (E, Q) where $K \leq E \leq L$, and Q is an ordering of E extending one from K, and there is no proper subfield $E \lneq E' \lneq L$ with an ordering Q' extending one from K. In fact, such maximal ordered subfields are the fixed fields $L^{\langle\varepsilon\rangle}$ of involutions $\varepsilon \in \mathrm{Gal}(L/K)$ such that $L^{\langle\varepsilon\rangle}$ is formally real, by [HJ85,

[19] $X(\mathfrak{G}) = \emptyset$ is permitted.

Proposition 2.1]. Equip $X(L/K)$ with the Harrison topology, given by the subbase $\{\{(E,Q) : a \in Q\} : a \in L^*\}$. $X(L/K)$ is a Boolean space, acted on by $\mathrm{Gal}(L/K)$. Furthermore if $x = (E,Q) = (L^{\langle\varepsilon\rangle}, Q) \in X(L/K)$, define the map $d(x) := \varepsilon$. Then

$$\mathfrak{Gal}(L/K) := \langle \mathrm{Gal}(L/K),\ \mathrm{Gal}(L/K(\sqrt{-1})),\ d : X(L/K) \to \mathrm{Gal}(L/K) \rangle$$

forms an Artin-Schreier structure by definition. Define an involution $\varepsilon \in \mathrm{Gal}(L/K)$ to be *real* if $L^{\langle\varepsilon\rangle}$ is formally real, and let $I(L/K)$ be the set of *real* involutions in $\mathrm{Gal}(L/K)$. Then $\langle \mathrm{Gal}(L/K),\ \mathrm{Gal}(L/K(\sqrt{-1})),\ I(L/K) \xhookrightarrow{incl.} \mathrm{Gal}(L/K) \rangle$ is a weak Artin-Schreier structure by definition. □

When $L = K^s$, $\mathfrak{Gal}(K^s/K) = \mathfrak{G}_K$ is the *absolute Artin-Schreier structure of* K. So in a sense it is the involutions of the absolute Galois group of K that 'see' the orders on K, and this is highlighted by the absolute Artin-Schreier structure.

Definition B.7. A *morphism* of Artin-Schreier structures $\varphi : \mathfrak{H} \to \mathfrak{G}$, where $\mathfrak{H} = \langle H, H', d_H : X(\mathfrak{H}) \to H \rangle$, $\mathfrak{G} = \langle G, G', d_G : X(\mathfrak{G}) \to G \rangle$, is a pair of maps (φ_1, φ_2) consisting of a continuous homomorphism $\varphi_1 : H \to G$ and a continuous map $\varphi_2 : X(\mathfrak{H}) \to X(\mathfrak{G})$ such that:

(1) $\varphi_1 \circ d_H = d_G \circ \varphi_2$;

(2) $\varphi_2(x^\sigma) = \varphi_2(x)^{\varphi_1(\sigma)}$, for all $x \in X(\mathfrak{H})$ and[20] $\sigma \in H$;

(3) $\varphi_1^{-1}(G') = H'$.

It is an *epimorphism* if both φ_1, φ_2 are onto. It is a *cover* if it is an epimorphism and, for all $x, y \in X(\mathfrak{H})$ such that $\varphi_2(x) = \varphi_2(y)$, there exists $\sigma \in H$ such that $x^\sigma = y$.

Often the notation is abused and the subscripts $1, 2, G, H$ are dropped. Note that (3) is equivalent to "$\varphi_1(H') \subseteq G'$ & $\varphi_1(H \setminus H') \subseteq G \setminus G'$", which forces $\mathrm{Ker}(\varphi_1) \subseteq H'$.

[20] If (1) holds, $\sigma \in H'$ suffices.

Example B.8. [HJ85, Example 3.4 (a)]. If L/K, F/K are Galois extensions with $\sqrt{-1} \in F \subseteq L$, then the canonical restriction map $\mathrm{Res} : \mathfrak{Gal}(L/K) \to \mathfrak{Gal}(F/K)$ is a cover. □

Remark B.9. A *Frattini cover* $\phi : \mathfrak{H} \to \mathfrak{G}$ of Artin-Schreier structures $\mathfrak{H}$, $\mathfrak{G}$ is a cover such that for every Artin-Schreier *substructure* $\mathfrak{H}_0 \leq \mathfrak{H}$, $\phi|_{\mathfrak{H}_0} : \mathfrak{H}_0 \to \mathfrak{G}$ is *not* a cover. (An Artin-Schreier *substructure* $\mathfrak{M} \leq \mathfrak{N}$ is one where $M \subseteq N$, $X(\mathfrak{M}) \subseteq X(\mathfrak{N})$, and the inclusions $M \hookrightarrow N$, $X(\mathfrak{M}) \hookrightarrow X(\mathfrak{N})$ define a morphism $\mathfrak{M} \to \mathfrak{N}$.)

The properties such a cover enjoys are analogous to that of profinite groups (p. 80), and are elaborated on in [Har84, §1]. In particular, given *any* cover $\varphi : \mathfrak{H} \to \mathfrak{G}$ there exists an Artin-Schreier substructure $\mathfrak{F} \leq \mathfrak{H}$ such that $\varphi|_{\mathfrak{F}} : \mathfrak{F} \to \mathfrak{G}$ is a Frattini cover. This is [Har84, Lemma 1.6]. □

Consider the category of Artin-Schreier structures with morphisms between them. An Artin-Schreier structure should be *projective* if it is a *projective object* ([Mac98, p. 118]) in this category. A central result of Haran & Jarden's work is a characterisation of this projectivity in terms of *embedding problems:*

Definition B.10. [HJ85, p. 468]. Let $\mathfrak{G}$ be a (weak) Artin-Schreier structure. A diagram

$$\begin{array}{ccc} & & \mathfrak{G} \\ & & \downarrow{\scriptstyle \varphi} \\ \mathfrak{B} & \xrightarrow{\alpha} & \mathfrak{A} \end{array}$$

where φ is a morphism and α an epimorphism of <u>weak</u> Artin-Schreier structures is called a *<u>weak</u> embedding problem for* $\mathfrak{G}$. If $\mathfrak{A}, \mathfrak{B}$ are Artin-Schreier structures, and α is a cover, this is an *embedding problem for* $\mathfrak{G}$. The problem is *finite* if both $\mathfrak{A}, \mathfrak{B}$ are finite. A *solution* to a problem is a morphism $\gamma : \mathfrak{G} \to \mathfrak{B}$ such that $\alpha \circ \gamma = \varphi$. An Artin-Schreier structure $\mathfrak{G}$ is *projective (in the sense of Haran & Jarden)* if every embedding problem for $\mathfrak{G}$ has a solution.

Theorem B.11. *Let $\mathfrak{G}$ be a (weak) Artin-Schreier structure. TFAE:*

(1) $\mathfrak{G}$ *is a projective (in the sense of Haran & Jarden) Artin-Schreier structure;*

(2) $\mathfrak{G}$ *is a projective object in the category of Artin-Schreier structures;*

(3) Every finite weak embedding problem for $\mathfrak{G}$ *has a solution;*

(4) The forgetful map of $\mathfrak{G}$ *is injective, and every finite weak embedding problem for* $\mathfrak{G}$*, in which the forgetful maps of* $\mathfrak{A}, \mathfrak{B}$ *are inclusions, has a solution.*

Proof. The equivalence of *(1), (3) & (4)* is [HJ85, Lemma 7.5] exactly. By definition, (2) $\Rightarrow$ (3). For (1) $\Rightarrow$ (2), we indicate [HJ85, p. 471]: consider the embedding problem:

$$\begin{array}{ccc} & & \mathfrak{G} \\ & & \downarrow \varphi \\ \mathfrak{B} & \xrightarrow{\alpha} & \mathfrak{A} \end{array}$$

where $\mathfrak{A}$, $\mathfrak{B} = \langle B, B', X(\mathfrak{B}) \to B \rangle$ are Artin-Schreier structures, and α is an epimorphism. Let $\mathfrak{B}^\sharp = \langle B, B', X(\mathfrak{B})^\sharp \to B \rangle$ be an Artin-Schreier substructure of $\mathfrak{B}$ such that $X(\mathfrak{B})^\sharp \subseteq X(\mathfrak{B})$ is minimal while being closed under the action of B and $\alpha(X(\mathfrak{B})^\sharp) = X(\mathfrak{A})$ still. Now consider the embedding problem:

$$\begin{array}{ccccc} & & & & \mathfrak{G} \\ & & \overset{\alpha^\sharp}{\frown} & & \downarrow \varphi \\ \mathfrak{B}^\sharp & \xhookrightarrow{\iota} & \mathfrak{B} & \xrightarrow{\alpha} & \mathfrak{A} \end{array}$$

Note (by design) $\alpha^\sharp$ is a cover, as $X(\mathfrak{B}^\sharp)/B'$ is homeomorphic to $X(\mathfrak{A})/A'$. Assuming (1), there is a solution $\gamma : \mathfrak{G} \to \mathfrak{B}^\sharp$, which gives a solution $\iota \circ \gamma$ to the original embedding problem, proving (2). ∎

Going forward, we will shorten *projective (in the sense of Haran & Jarden)* to *projective*, owing to *Theorem B.11.* Later, Haran developed a cohomology theory of Artin-Schreier structures [Har90, Har93], which provided a characterisation of projectivity in the Artin-Schreier structure category in terms of projectivity of the underlying group-theoretic data.

Theorem B.12. [Har93, Theorem 2.1]. *An Artin-Schreier structure* $\mathfrak{G} = \langle G, G', X(\mathfrak{G}) \to G \rangle$ *is projective if and only if* G' *is projective and* $X(\mathfrak{G}) =^{21} \mathrm{Inv}(G)$*, the set of involutions of* G*.* ■

Haran also produced a characterisation of projective Artin-Schreier structures in terms of the cohomological dimension of such a structure (see [Har90, Har93]). One can also phrase the projectivity of an Artin-Schreier structure $\mathfrak{G} = \langle G, G', X(\mathfrak{G}) \to G \rangle$ purely in terms of a group-theoretic property of G:

Definition B.13. Let G be a profinite group. A diagram

$$\begin{array}{ccc} & & G \\ & & \downarrow \varphi \\ B & \xrightarrow{\alpha} \!\!\!\rightarrow & A \end{array}$$

where φ is a homomorphism and α is an epimorphism of (finite) groups, is called a (finite) *real* embedding problem for G if, for every involution $\epsilon \in G$ with $\varphi(\epsilon) \neq 1$, there exists an involution $b \in B$ with $\alpha(b) = \varphi(\epsilon)$. The group G is *real* projective if $\mathrm{Inv}(G)$ is closed in G, and every finite real embedding problem has a solution.

Theorem B.14. [HJ85, Proposition 7.7]. *Let* G *be a profinite group and* $\mathrm{Inv}(G)$ *the set of involutions of* G *Denote*

$$\mathcal{G}' = \{G' \lhd G : G' \text{ is open, } (G : G') \leq 2, \text{ and } G' \cap \mathrm{Inv}(G) = \emptyset\}.$$

TFAE:

(1) G *is real projective;*

(2) $\mathcal{G}' \neq \emptyset$ *and for every (equivalently, for some)* $G' \in \mathcal{G}'$*,* $\mathfrak{G} = \langle G, G', \mathrm{Inv}(G) \xhookrightarrow{incl.} G \rangle$ *is a projective Artin-Schreier structure.* ■

Corollary B.15. *An Artin-Schreier structure* $\mathfrak{G} = \langle G, G', X(\mathfrak{G}) \xrightarrow{d} G \rangle$ *is projective if and only if* G *is real projective.*

[21] By which we mean there is a continuous bijection $d : X \to \mathrm{Inv}(G)$ such that $d(x^\sigma) = \sigma d(x) \sigma^{-1}$. Haran notes in [Har93, p. 232], "[w]e have not put it this way merely to avoid ambiguity in notation".

Proof. A consequence of *Theorem B.14*, noting that if $\mathfrak{G}$ is a projective Artin-Schreier structure, WLOG $X(\mathfrak{G}) = \mathrm{Inv}(G)$ by *Theorem B.11 (4).* ■

With these ideas, one can prove a result analogous to van den Dries-Lubotzky's [vdDL81, §4.8, Proposition]:

Theorem B.16. *If K is a PRC field, then $\mathfrak{G}_K$ is projective. Conversely, if $\mathfrak{G}$ is a projective Artin-Schreier structure, there exists a PRC field K such that $\mathfrak{G} \cong \mathfrak{G}_K$.*

Proof. This is equivalent to the statement of [HJ85, Theorem 10.4], and follows from [HJ85, Theorems 10.1 & 10.2]. ■

Haran & Jarden actually prove a theorem slightly more precise than this. They prove a corresponding *Theorem 4.1.5:* given a PRC field K, they produce a PRC field extension E whose algebraic part is governable relative to K, yet has an almost arbitrary absolute Artin-Schreier structure.

Theorem B.17. [HJ85, Theorem 10.2]. *Let $\mathfrak{G}$ be a projective Artin-Schreier structure. Let L/K be a Galois extension such that $\sqrt{-1} \in L$ and let $\pi : \mathfrak{G} \to \mathfrak{Gal}(L/K)$ be an epimorphism. Then there exists a PRC extension E/K such that $\mathfrak{G} \cong \mathfrak{G}_E$, and*

$$\begin{array}{ccc} \mathfrak{G} & \xrightarrow{\cong} & \mathfrak{G}_E \\ & \searrow^{\pi} & \downarrow Res_L \\ & & \mathfrak{Gal}(L/K) \end{array}$$

is a commutative diagram. ■

Finally, in our constructions we will require the use of quotient Artin-Schreier structures, which we define now:

Definition B.18. [HJ85, §4.1]. Let $\mathfrak{G} = \langle G, G', X(\mathfrak{G}) \xrightarrow{d} G \rangle$ be a (weak) Artin-Schreier structure, and $N \leq G'$ a closed normal subgroup of G. Define the *quotient (weak) Artin-Schreier structure* $\mathfrak{G}/N$ to be

$$\langle G/N,\, G'/N,\, X(\mathfrak{G})/N \xrightarrow{\overline{d}} G/N \rangle,$$

where $X(\mathfrak{G})/N$ is the quotient Boolean space of $X(\mathfrak{G})$ under the relation $x_1 \sim x_2 \iff \exists \sigma \in N\ (x_1^\sigma = x_2)$ for all $x_1, x_2 \in X(\mathfrak{G})$, and $\overline{d} : X(\mathfrak{G})/N \to G/N$ is the forgetful map induced by $d : X(\mathfrak{G}) \to G$.

The following is likely known, but unavailable in the literature, so we prove it ourselves: let $\mathcal{C}$ be a full formation of finite groups (recall *Definition 4.1.6*) containing the family of finite 2-groups, fix $\mathfrak{G} = \langle G, G', X(\mathfrak{G}) \xrightarrow{d} G \rangle$, define $\mathcal{N}$ to be the family of closed normal subgroups $N \triangleleft G$ such that $G/N \in \mathcal{C}$, and let $N_{\mathcal{C}} = \bigcap \mathcal{N}$. Then $G/N_{\mathcal{C}}$ is the maximal pro-$\mathcal{C}$ quotient of G. As $G' \leq G$ is open and of index ≤ 2, $N_{\mathcal{C}} \leq G'$, hence we may form the (well-defined) quotient Artin-Schreier structure

$$\mathfrak{G}_{\mathcal{C}} := \mathfrak{G}/N_{\mathcal{C}} = \langle G/N_{\mathcal{C}},\ G'/N_{\mathcal{C}},\ X(\mathfrak{G})/N_{\mathcal{C}} \xrightarrow{\overline{d}} G/N_{\mathcal{C}} \rangle.$$

This Artin-Schreier structure is defined to be the *maximal pro-$\mathcal{C}$ quotient of $\mathfrak{G}$*. Notice as $\mathcal{C}$ is a full formation, $G'/N_{\mathcal{C}}$ is pro-$\mathcal{C}$ ([FJ08, Lemma 17.3.1]).

Lemma B.19. *Suppose $\mathcal{C}$ is a full formation of finite groups containing the family of finite 2-groups, and $\mathfrak{G}$ is a projective Artin-Schreier structure. Then the maximal pro-$\mathcal{C}$ quotient $\mathfrak{G}_{\mathcal{C}}$ is also a projective Artin-Schreier structure.*

Proof. We will first show $\mathfrak{G}_{\mathcal{C}}$ is $\mathcal{C}$-projective[22]. Let $\mathfrak{A}, \mathfrak{B}$ be finite Artin-Schreier structures whose underlying groups A, B are elements of $\mathcal{C}$ (immediately this implies $A', B' \in \mathcal{C}$). Consider the embedding problem

$$\begin{array}{ccc} & & \mathfrak{G}_{\mathcal{C}} = \mathfrak{G}/N_{\mathcal{C}} \\ & & \big\downarrow \phi \\ \mathfrak{B} & \xrightarrow{\quad\alpha\quad} \!\!\!\rightarrow & \mathfrak{A} \end{array}$$

where α is an epimorphism and ϕ a morphism. Recall the cover that is the quotient morphism $\pi : \mathfrak{G} \twoheadrightarrow \mathfrak{G}/N_{\mathcal{C}}$ (cf. [HJ85, pp. 458–459]); as $\mathfrak{G}$ is projective there exists a morphism $\gamma : \mathfrak{G} \to \mathfrak{B}$ such that $\alpha \circ \gamma = \phi \circ \pi$, by *Theorem B.11.*

We claim γ factors through $N_{\mathcal{C}}$. Indeed, γ consists of the continuous morphisms $\gamma_1 : G \to B$ (which has the property $\gamma_1^{-1}(B') = G'$) and $\gamma_2 : X(\mathfrak{G}) \to X(\mathfrak{B})$ mak-

[22] Projective relative to $\mathcal{C}$-groups; see [FJ08, Definition 22.3.1].

ing the relevant diagrams commute. By the *First Isomorphism Theorem for groups*, $G/\ker(\gamma_1) \cong \gamma_1(G) \leq B$, hence as $\mathcal{C}$ is a full formation, by definition $\ker(\gamma_1) \in \mathcal{N}$. Therefore $N_{\mathcal{C}} \subseteq \ker(\gamma_1)$, and thus the map γ_1 factors through $N_{\mathcal{C}}$.

For $\gamma_2 : X(\mathfrak{G}) \to X(\mathfrak{B})$, notice that:

$$x_1 \sim x_2 \implies \gamma_2(x_2) = \gamma_2(x_1^{\sigma}) = \gamma_2(x_1)^{\gamma_1(\sigma)} = \gamma_2(x_1),$$

as $\sigma \in N_{\mathcal{C}} \subseteq \ker(\gamma_1)$. Thus, γ_2 factors through the equivalence relation $\sim$, and gives rise to a natural map $X(\mathfrak{G})/N_{\mathcal{C}} \to X(\mathfrak{B})$. Therefore the morphism $\gamma : \mathfrak{G} \to \mathfrak{B}$ factors through a morphism $\overline{\gamma} : \mathfrak{G}/N_{\mathcal{C}} \to \mathfrak{B}$, i.e. $\overline{\gamma} \circ \pi = \gamma$. We conclude $\alpha \circ \overline{\gamma} = \phi$ as required to prove $\mathfrak{G}_{\mathcal{C}}$ is $\mathcal{C}$-projective.

Now consider the general embedding problem

$$\begin{array}{ccc} & & \mathfrak{G}_{\mathcal{C}} \\ & & \downarrow \phi \\ \mathfrak{B} & \xrightarrow{\alpha} & \mathfrak{A} \end{array}$$

where $\mathfrak{A}, \mathfrak{B}$ are arbitrary finite Artin-Schreier structures, and α is an epimorphism. We may assume WLOG ϕ is an epimorphism (as Haran & Jarden note in [HJ85, pp. 471–472], we may replace $\mathfrak{A}$ with an epimorphic image $\mathfrak{A}_0$ of $\mathfrak{G}_{\mathcal{C}}$, and $\mathfrak{B}$ with the fibred product of $\mathfrak{B}$ with $\mathfrak{A}_0$ over $\mathfrak{A}$. For more details on fibred products of Artin-Schreier structures, see [HJ85, p. 460 & Lemma 4.6]). Hence $A, A' \in \mathcal{C}$. By[23] [RZ00, Lemma 7.6.6] there exists $M \leq B$ such that $B = \ker(\alpha)M$, $M \in \mathcal{C}$, and $\alpha(M) = A$. Let $M' = B' \cap M$. We may further assume $\mathrm{Inv}(B) = \{\epsilon_1, \ldots, \epsilon_n\} \subset M$, as if not the group $M\langle\epsilon_1\rangle \ldots \langle\epsilon_n\rangle$ has these properties (note we assumed $\mathcal{C}$ contains the family of finite 2-groups). Clearly $M' \leq M$ (and thus $M' \in \mathcal{C}$), but also $\alpha(M') = A'$.

Indeed, $\alpha(M') \subseteq A'$, and furthermore given $a' \in A'$ we may find $b' \in B'$ such that $\alpha(b') = a'$. M is constructed ([RZ00, Lemma 7.6.6]) so that $\ker(\alpha)M = B$, hence $b' = km$ for some $k \in \ker(\alpha)$ and $m \in M$. By definition of α, $\ker(\alpha) \subseteq B'$, hence

[23] Ribes & Zalesskii prove this for $\mathcal{C}$ a *saturated variety of finite groups*; terminology found in [RZ00, pp. 19–20 & Definition 7.6.4]. We note a full formation of finite groups *is* a 'saturated variety', by definition [RZ00, pp. 19–20] and [RZ00, Example 7.6.5 (1)].

$m = k^{-1}b' \in B' \cap M$. Then $A' \subseteq \alpha(M')$ as desired. Note $M' \neq M \iff B' \neq B$, as $\ker(\alpha)M = B$ whereas $\ker(\alpha)M' \leq \ker(\alpha)B' = B'$. Finally, $(M : M') \leq (B : B') \leq 2$ as required to define the Artin-Schreier substructure

$$\mathfrak{M} = \langle M,\, M',\, X(\mathfrak{M}) \xrightarrow{d_M} M \rangle \quad \leq \quad \mathfrak{B} = \langle B,\, B',\, X(\mathfrak{B}) \xrightarrow{d_B} B \rangle,$$

where $X(\mathfrak{M}) := d_B^{-1}(M)$ and $d_M = d_B|_{X(\mathfrak{M})}$. Note that as B is finite, M is closed, hence as d_B is continuous the space $X(\mathfrak{M}) \subseteq X(\mathfrak{B})$ is Boolean. Therefore $\mathfrak{M}$ indeed satisfies the definition of an Artin-Schreier structure. It is furthermore a *substructure* of $\mathfrak{B}$, as the canonical inclusion map $\mathfrak{M} \hookrightarrow \mathfrak{B}$ is a morphism, and by construction $\alpha : \mathfrak{M} \twoheadrightarrow \mathfrak{A}$ is an epimorphism.

As $\mathfrak{G}_{\mathcal{C}}$ is $\mathcal{C}$-projective, there exists a morphism $\gamma : \mathfrak{G}_{\mathcal{C}} \to \mathfrak{M}$ which solves the embedding problem. Solving finite embedding problems is sufficient by *Theorem B.11* to ensure $\mathfrak{G}_{\mathcal{C}}$ is projective in the category of Artin-Schreier structures, as required. ■

C Background on PpC fields and $G_{\mathbb{Q}_p}$-structures

After the algebra and model theory of PAC and PRC fields, *pseudo-p-adically closed fields* are a reasonable subsequent consideration. First, some terminology:

Definition C.1. Let K be a field, and p prime. A valuation v is *p-adic* if its residue field is $\mathbb{F}_p$ and $v(p)$ is the minimal positive element of the value group $v(K^*)$. A field K that admits a p-adic valuation is *formally p-adic*.

Formally p-adic fields necessarily have characteristic 0. A p-adically valued field (K, v) which has no proper p-adically valued algebraic extension is *p-adically closed*. For every p-adically valued field (K, v) there exists an algebraic extension $(\overline{K}, \overline{v})$ which is p-adically closed: this is known as a[24] *p-adic closure* of (K, v).

Definition C.2. A field K is *pseudo-p-adically closed* (PpC) if every geometrically irreducible variety defined over K, which has a smooth $\overline{K}$-rational point in each p-adic closure $\overline{K}$ of K, has a K-rational point. (If $\mathscr{V}$ is a K-variety, the $\overline{K}$-variety $\overline{\mathscr{V}} = \mathscr{V} \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{K})$ has a *smooth* $\overline{K}$-rational point $x \in \overline{\mathscr{V}}$ if $\dim \mathcal{O}_{\overline{\mathscr{V}}, x} = \dim \mathfrak{m}_x/\mathfrak{m}_x^2$.)

Note that we do not assume that K has a p-adic valuation; a PpC field with no p-adic valuation is PAC. See [HJ88, Lemma 12.5] for an example class of formally p-adic PpC fields. For a specific example, take $\mathbb{Q}^{tp}$, the "totally p-adic" algebraic numbers (for a fixed prime p). This is analogous to $\mathbb{Q}^{tr}$; for example, $\mathbb{Q}^{tp} = \bigcap_{\sigma \in G_\mathbb{Q}} \sigma(\mathbb{Q}_p \cap \widetilde{\mathbb{Q}})$ and (equivalently) this field is the maximal Galois extension of $\mathbb{Q}$ in $\mathbb{Q}_p$. This field is PpC by Pop [Pop90].

Remark C.3. If a field is formally real, this can be expressed through $\mathcal{L}_r$ in the field structure (namely "-1 is not a sum of squares"). The same is true of formally p-adic fields: defining the *Kochen operator*

$$\gamma(x) = \frac{1}{p} \frac{x^p - x}{(x^p - x)^2 - 1},$$

it is a result of Prestel & Roquette (stated in [HJ88, Lemma 6.1], which references [PR84,

[24] Uniqueness (or lack thereof) is discussed after *Definition C.12*.

Theorem 6.4]) that if $\mathrm{char}(K) = 0$ and $p \cdot f(\gamma(x_1), \ldots, \gamma(x_n)) \neq a$ for each nonzero $a \in \mathbb{Z}$ relatively prime to p, $f \in \mathbb{Z}[\overline{x}]$ and $\overline{x} \in K$, then K is formally p-adic. □

Through the same style of arguments as Haran, Efrat [Efr92] proves:

Theorem C.4. [Efr92, Corollary 4.3]. *The theory of formally p-adic PpC fields is undecidable.* ■

The undecidability of the theory of *all* PpC fields, $\mathtt{P}\boldsymbol{p}\mathtt{C}$, follows from the undecidability of PAC. This is [Efr92, Remark 4.4]: let $\theta(x, y, z)$ be the numerator of the rational function $\gamma(x) + \gamma(y) + \gamma(z) - \frac{1}{p}$. Then $\mathtt{PAC} = \mathtt{P}\boldsymbol{p}\mathtt{C} \cup \{\exists x, y, z\,(\theta(x, y, z) = 0)\}$. Indeed, $\theta(x, y, z)$ is absolutely irreducible by Schinzel [Sch85, Corollaries 1, 2] (and independently Fried [Fri87, Main Theorem] in characteristic 0), thus any PAC field L satisfies $\mathtt{P}\boldsymbol{p}\mathtt{C}$ and $L \models \exists x, y, z\,(\theta(x, y, z) = 0)$. Conversely, if L is PpC and $L \models \exists x, y, z\,(\theta(x, y, z) = 0)$, then L is not formally p-adic by *Remark C.3* – hence is PAC by definition. $\mathtt{P}\boldsymbol{p}\mathtt{C}$ is first-order $\mathcal{L}_r$-axiomatisable by [Jar91, Lemma 10.1].

In this appendix we will follow Haran & Jarden's adaptation [HJ88] of their previous PRC field paper [HJ85] by introducing Γ-*structures* as a generalisation of Artin-Schreier structures. The remainder of this appendix is an overview of[25] [HJ88] for §4.3.

Definition C.5. Let Γ be a finitely generated profinite group. A Γ-*structure* is a system $\mathfrak{G} = \langle G, X(\mathfrak{G}) \xrightarrow{d} \mathrm{Hom}(\Gamma, G)\rangle$, where G is a profinite group acting continuously on the Boolean space $X(\mathfrak{G})$, and d is a continuous map (known as the *forgetful map*), such that for every $x \in X(\mathfrak{G})$:

(1) $d(x^\sigma) = (d(x))^\sigma$ for every $\sigma \in G$;

(2) $\{\sigma \in G : x^\sigma = x\} = \{1\}$ (we say the action of G on $X(\mathfrak{G})$ is *regular*).

If $\mathfrak{G}$ satisfies only (1) it is a *weak* Γ-*structure*.

[25] The author also found the copy of [HJ88] located at www.tau.ac.il/∼jarden/Articles/paper43.pdf quite helpful.

Remark C.6. Compare this definition to *Definition B.5* to see that $\mathbb{Z}/2\,\mathbb{Z}$-structures carry near identical information as Artin-Schreier structures. It is not a perfect match, as the prototypical example for Γ (namely $G_{\mathbb{Q}_p}$, the absolute Galois group of $\mathbb{Q}_p$) is very different to $\mathbb{Z}/2\,\mathbb{Z}$. So, for example, while in *Definition B.5* we asked $\{\sigma \in G : x^\sigma = x\}$ $= \{1, d(x)\}$ for all $x \in X(\mathfrak{G})$, as $G_{\mathbb{Q}_p}$ is torsion free (explicitly given by [HJP05, Lemma 8.3]) here we have $\{\sigma \in G : x^\sigma = x\} = \{1\}$. □

Remark C.7. [HJ88, p. 150]. Let $\mathfrak{G} = \langle G, X(\mathfrak{G}) \xrightarrow{d} \mathrm{Hom}(\Gamma, G)\rangle$ be a (weak) Γ-structure. Denote the set of closed subgroups of G by $\mathrm{Subg}(G)$. Notice that $\mathrm{Subg}(G)$ can be viewed as a Boolean space: for open normal subgroups of G, equip $\mathrm{Subg}(G/N)$ with the discrete topology. By the compactness of G, $\mathrm{Subg}(G) \cong \varprojlim \mathrm{Subg}(G/N)$, hence $\mathrm{Subg}(G)$ is a profinite space under this topology. Furthermore, the map

$$\Im : \mathrm{Hom}(\Gamma, G) \to \mathrm{Subg}(G); \qquad \Im(\psi) = \psi(\Gamma),$$

is continuous, as it is the inverse limit of the continuous maps $\Im_N : \mathrm{Hom}(\Gamma, G/N) \to \mathrm{Subg}(G/N)$ of finite discrete spaces. This topology may be equivalently characterised as follows: called the *strict topology*, it has basis

$$v(\Delta, N) = \{H \in \mathrm{Subg}(G) : HN = \Delta N\}, \quad \text{where } \Delta \in \mathrm{Subg}(G) \text{ and } N \lhd G \text{ open.}$$

One may also equip $\mathrm{Subg}(G)$ with the *étale topology*, with basis $\{\mathrm{Subg}(U)\}_{U \leq G \text{ open}}$. This is coarser than the strict topology ([HJ21, Lemma 1.2.2]). Both topologies have a number of useful properties, including:

- If $\varphi : H \to G$ is a homomorphism of profinite groups, the induced map $\varphi^* :$ $\mathrm{Subg}(H) \to \mathrm{Subg}(G)$ is étale continuous. If φ is an epimorphism, φ^* is strictly continuous.
- If H is open (resp. closed) in G, $\mathrm{Subg}(H)$ is strictly open (resp. closed) in $\mathrm{Subg}(G)$.
- If H is closed in G, the induced inclusion $\mathrm{Subg}(H) \hookrightarrow \mathrm{Subg}(G)$ is étale continuous,

as is the restriction $\mathrm{Subg}(G) \to \mathrm{Subg}(H)$ induced from $J \mapsto J \cap H$.

- Let $\mathcal{D}$ be a subset of $\mathrm{Subg}(G)$. If $\mathcal{D}$ is étale closed, it is strictly closed, equivalently strictly compact, which implies $\mathcal{D}$ is étale compact, and thus $\bigcup_{H\in\mathcal{D}} H$ is closed in G.

These properties arise from [HJ21, pp. 8–10]. Going forward, unless otherwise stated we shall take $\mathrm{Subg}(G)$ with the strict topology. □

The category we consider in the PpC context is the *category of* Γ*-structures*. The definition of *morphism, epimorphism, (universal Frattini*[26]*) cover, (weak/finite/solution to an) embedding problem,* and *(maximal pro-*$\mathcal{C}$*) quotient structure* are exactly as in *Appendix B*; cf. *Definitions B.7, B.10 & B.18, and Remark B.9*. We have the following definitions:

Definition C.8. [HJ88, Definition 5.1]. A Γ-structure is *projective* if every finite weak embedding problem has a solution.

Definition C.9. [HJ88, Definition 4.1]. A profinite group G is $G_{\mathbb{Q}_p}$*-projective* if $\mathcal{D}(G) = \{H \leq G : H \cong G_{\mathbb{Q}_p}\}$ is closed[27] in $\mathrm{Subg}(G)$, and for every diagram

$$\begin{array}{ccc} & & G \\ & & \downarrow{\scriptstyle \varphi} \\ B & \xrightarrow{\alpha} & A \end{array}$$

where φ is a homomorphism and α is an epimorphism, such that for each $H \in \mathcal{D}(G)$ there exists $\gamma_H : H \to B$ with $\alpha \circ \gamma_H = \varphi|_H$ (i.e. "for every $G_{\mathbb{Q}_p}$*-embedding problem*"), there is a *solution* $\gamma : G \to B$; a morphism such that $\alpha \circ \gamma = \varphi$.

We recover parts of *Theorems B.11 & B.12*, when assumptions[28] on Γ are made:

[26] See [Efr91, §4] as reference.

[27] In fact this is *always* satisfied; see the proof of *Lemma 4.3.8*, cf. [Feh10, Lemma 3.5.1].

[28] Results that follow can be true in more generality, under [HJ88, Assumption 3.1 or 8.1] or the starting paragraph of §7 *ibid*. However for simplicity we will restrict to the groups and fields we are most interested in – those for which Haran, Jarden & Efrat's main results hold.

Theorem C.10. *Let $\mathfrak{G}$ be a $G_{\mathbb{Q}_p}$-structure, projective (in the sense of* Definition C.8*). Then $\mathfrak{G}$ is a projective object in the category of $G_{\mathbb{Q}_p}$-structures, and the underlying group G is $G_{\mathbb{Q}_p}$-projective.*

Furthermore, the forgetful map is injective, for each $x \in X(\mathfrak{G})$ the map $d(x) : G_{\mathbb{Q}_p} \to G$ is injective, and the space of orbits $X(\mathfrak{G})/G$ is homeomorphic to $\mathcal{D}(G)$.

Proof. That G is $G_{\mathbb{Q}_p}$-projective is [HJ88, Proposition 5.4 (a)]. The "Furthermore..." is [HJ88, Lemma 5.3]. It remains to show that, if $\mathfrak{G}$ is projective (in the sense of *Definition C.8*), the embedding problem

$$\begin{array}{ccc} & & \mathfrak{G} \\ & & \downarrow \varphi \\ \mathfrak{B} & \xrightarrow{\alpha} & \mathfrak{A} \end{array}$$

has a solution, where $\mathfrak{A}$, $\mathfrak{B} = \langle B, X(\mathfrak{B}) \xrightarrow{d} \mathrm{Hom}(G_{\mathbb{Q}_p}, B)\rangle$ are $G_{\mathbb{Q}_p}$-structures, and α is an epimorphism. Let $\mathfrak{B}^\sharp = \langle B, X(\mathfrak{B})^\sharp \xrightarrow{d} \mathrm{Hom}(G_{\mathbb{Q}_p}, B)\rangle$ be a $G_{\mathbb{Q}_p}$-substructure of $\mathfrak{B}$ where $X(\mathfrak{B})^\sharp \subseteq X(\mathfrak{B})$ is a (minimal) closed system of representatives for the B-orbits of the elements of $X(\mathfrak{B})$, such that $\alpha(X(\mathfrak{B})^\sharp)$ is a system of representatives for the A-orbits of elements of $X(\mathfrak{A})$; $X(\mathfrak{B})^\sharp$ exists by [HJ88, Lemma 2.4]. The composed map $\mathfrak{B}^\sharp \xhookrightarrow{\iota} \mathfrak{B} \xrightarrow{\alpha} \mathfrak{A}$ is a cover by [HJ88, Lemma 2.7].

By *Definition C.8*, there is a solution $\gamma : \mathfrak{G} \to \mathfrak{B}^\sharp$ such that $\alpha \circ (\iota \circ \gamma) = \varphi$, hence $\iota \circ \gamma$ solves the required embedding problem. ∎

Theorem C.11. [HJ88, Proposition 5.4]. *If G is Γ-projective, then there exists $X \subseteq \mathrm{Hom}(\Gamma, G)$, closed topologically and closed under the action of G, such that $\mathcal{D}(G) = \{\psi(\Gamma) : \psi \in X\}$ and $\langle G, X \xrightarrow{incl.} \mathrm{Hom}(\Gamma, G)\rangle$ is a projective Γ-structure.* ∎

We will now describe the Galois structures $\mathfrak{Gal}(L/K)$ ascribed to formally p-adic fields K with algebraic extensions L. This ultimately requires a 'natural' Boolean space $X(L/K) := X(\mathfrak{Gal}(L/K))$ carrying valuation-theoretic data. In the case of PRC fields, recall from *Example B.6* that the underlying space of $X(L/K)$ was the set of pairs (E, Q) where $K \leq E \leq L$ and Q is an ordering of E, extending one from K, and E

was 'maximal' in a sense. Here, Haran & Jarden do something similar, where instead of *orderings* they consider *the p-adic valuations*, or more conveniently the coarsened place corresponding to a p-adic valuation.

Indeed (following the exposition of [HJ88, p. 168]) let (K, v) be formally p-adic. Each element of $\mathcal{O}_v$ can be 'approximated' by $\mathbb{Z}_p$, in the sense that for $a \in \mathcal{O}_v$ and $n \in \mathbb{N}$ there exists unique integers $a_0, \ldots, a_n \in [0, p-1]$ with $a \equiv a_0 + a_1 p + \cdots + a_n p^n \bmod p^{n+1}\mathcal{O}_v$. Therefore, there is a canonical homomorphism

$$\pi_v : \mathcal{O}_v \to \mathbb{Z}_p; \qquad a \mapsto \sum_{n=0}^{\infty} a_n p^n,$$

with $\mathrm{Ker}(\pi_v) = \cap_n p^n \mathcal{O}_v$. The coarsening $\mathcal{O}_{\dot{v}} = (\mathcal{O}_v)_{\mathrm{Ker}(\pi_v)}$ is a valuation ring corresponding to a place $\pi_{\dot{v}} : K \to \mathbb{Q}_p \cup \{\infty\}$ extending π_v. One may check (viz. [HJ88, Lemma 6.7]) the operation $v \mapsto \pi_{\dot{v}}$ is a bijection between p-adic valuations of K and places $K \to \mathbb{Q}_p \cup \{\infty\}$.

By valuation-theoretic algebra (i.a. [HJ88, §6–8]), fixing a p-adic closure $\overline{K}$ of K, there is a sequence of isomorphisms

$$\overline{K}^*/(\overline{K}^*)^n \cong (\overline{K}^* \cap \widetilde{\mathbb{Q}})/(\overline{K}^* \cap \widetilde{\mathbb{Q}})^n \cong (\mathbb{Q}_p^* \cap \widetilde{\mathbb{Q}})/(\mathbb{Q}_p^* \cap \widetilde{\mathbb{Q}})^n \cong \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n,$$

hence the canonical homomorphism $K^* \to \overline{K}^*/(\overline{K}^*)^n$ induces a homomorphism $K^* \to \varprojlim \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n$ of K^* with the profinite completion of $\mathbb{Q}_p^*$ ([HJ88, p. 173]). Denote the set-theoretic union "$\mathbb{Q}_p \cup \{\infty\} \cup \varprojlim \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n$" by Θ. We now define:

Definition C.12. ([HJ88, Definition 8.2] with $F = \mathbb{Q}_p$.) Let K be a field of characteristic 0, $\pi : K \to \mathbb{Q}_p \cup \{\infty\}$ a place, and $\varphi : K^* \to \varprojlim \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n$ a homomorphism. The pair (π, φ) is a Θ-*site of* K if π and φ agree[29] on units in the valuation ring induced by π.

The motivation for this definition is as follows ([HJ88, p. 148]): given a formally p-adic field K, two p-adic closures E, F of K are *not necessarily isomorphic*. This is

[29] Implicitly we identify $\mathbb{Q}_p^*$ as a subgroup of $\varprojlim \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n$; a nontrivial remark but possible by [HJ88, Lemma 6.8 (a)].

a new difficulty – two algebraic or real closures of a field *are* isomorphic (though see *Remark 4.2.1*). In the p-adic case, there is a criterion for two p-adic closures to be isomorphic: by Macintyre[30], $E \cong_K F$ if and only if $K \cap (E)^n = K \cap (F)^n$ for all $n \in \mathbb{N}$ (explicitly this is a consequence of [PR84, Corollary 3.11]). Thus a p-adic closure $\overline{K}$ is characterised by the homomorphism $K^* \to \varprojlim \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n$ arising from the canonical $K^* \to \overline{K}^*/(\overline{K}^*)^n$ with kernel $K \cap (\overline{K})^n$. Therefore a Θ-site (π, φ) may be thought of as the data ('p-adic valuation', 'p-adic closure'). For every place $\pi : K \to \mathbb{Q}_p \cup \{\infty\}$, there exists a homomorphism $\varphi : K^* \to \varprojlim \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n$ making (π, φ) a Θ-site (take a p-adic closure with respect to π; cf. [HJ88, Corollary 8.10]), and φ is unique in that if (π', φ') is a Θ-site of K such that $\varphi = \varphi'$, then $\pi = \pi'$ [HJ88, Lemma 8.8].

Remark C.13. (from [Efr92, p. 447].) The set of Θ-sites of K, denoted $X(K)$, 'is' the set of K-isomorphism classes of p-adic closures of K. Furthermore, if K is PpC then any two p-adic closures of K with respect to a fixed p-adic valuation are K isomorphic ([Gro87, Proposition 3.06]; [Jar91, Theorem 10.8 (b)] as well), hence the Θ-sites of such K 'are' the p-adic valuations of K.

In comparison, for a formally real field F, the space $X(F)$ was the set of orderings of F (recall *Remark 4.2.9*). We can recover the formally real setting from *Definition C.12* too (this is [HJ88, Remark 8.3]): in place of $\mathbb{Q}_p$, we have $\mathbb{R}$; in place of $\varprojlim \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n$, we have $\{\pm 1\}$. Then for $(K, <)$ an ordered field, define

$$\pi : K \to \mathbb{R} \cup \{\infty\}; \quad x \mapsto \sup\{r \in \mathbb{Q} \,:\, r < x\} \text{ if the supremum exists, } \infty \text{ otherwise.}$$

This place gives rise to a valuation ring $\mathcal{O}_\pi$. Along with

$$\varphi : K^* \to \{\pm 1\}; \qquad x \mapsto 1 \text{ if and only if } x > 0,$$

this defines a "Θ-*site of* K" (where instead of identifying $\mathbb{Q}_p^*$ as a subgroup of $\varprojlim \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^n$, we have the homomorphism $\text{sign} : \mathbb{R}^* \to \{\pm 1\}$, and the units of $\mathcal{O}_\pi$ agree under φ and $\text{sign} \circ \pi$). Conversely, if (π, φ) is a "Θ-site of K", the rule $\varphi = \text{sign} \circ \pi$

[30] [Mac76, Theorem 1] proves the first order theory of p-adically closed fields has quantifier elimination in the language of rings plus (for each $n \in \mathbb{N}$) a predicate interpreted as the set of n-th powers.

on units $\mathcal{O}_\pi^\times$ defines a prepositive cone (a *positive* cone P on K is a *prepositive* cone such that $K = P \cup -P$), which by $\varphi : K^* \to \{\pm 1\}$ is indeed an ordering. $\square$

This is the picture for a single formally p-adic field K; now we extend our definitions to algebraic field extensions L/K. To carry the p-adic closure information, define

$$\Phi_L := (L^* \times \varprojlim \mathbb{Q}_p^* / (\mathbb{Q}_p^*)^n) / \{(a^{-1}, a) : a \in \mathbb{Q}_p^*\}.$$

By definition $\Phi_{\mathbb{Q}_p} \cong \varprojlim \mathbb{Q}_p^* / (\mathbb{Q}_p^*)^n$, as one might expect, and $\widetilde{\Phi} := \Phi_{\widetilde{\mathbb{Q}_p}} = \bigcup_E \Phi_E$ where the union ranges over the finite extensions $E/\mathbb{Q}_p$. Topologically, $\widetilde{\Phi}$ has the quotient topology of the product topology. As $G_{\mathbb{Q}_p}$ acts continuously on $\widetilde{\mathbb{Q}_p}$, and $\widetilde{\mathbb{Q}_p}$ can be continuously embedded in $\widetilde{\Phi}$, we see $G_{\mathbb{Q}_p}$ acts continuously on $\widetilde{\Phi}$ too.

Denoting the set theoretic union "$E \cup \{\infty\} \cup \Phi_E$" as Θ_E, with $\widetilde{\Theta} := \Theta_{\widetilde{\mathbb{Q}_p}}$, we have:

Definition C.14. ([HJ88, p. 177] with $F = \mathbb{Q}_p$.) Let L be a field of characteristic 0, $\pi : L \to \widetilde{\mathbb{Q}_p} \cup \{\infty\}$ a place, and $\varphi : L^* \to \widetilde{\Phi}$ a homomorphism. The pair (π, φ) is a $\widetilde{\Theta}$-*site of* L if π and φ agree[31] on units in the valuation ring induced by π.

What is the connection between Θ-sites and $\widetilde{\Theta}$-sites? If $\theta = (\pi, \varphi)$ is a $\widetilde{\Theta}$-site of L, where L/K is Galois, then $Res_K(\theta) = (\pi|_K, \varphi|_{K^*})$ is a $\widetilde{\Theta}$-site of K. Furthermore, if θ is a Θ-site of K, it may be extended to a $\widetilde{\Theta}$-site θ' of L in such a way that if θ'' is another extension, there exists a unique $\sigma \in \mathrm{Gal}(L/K)$ with $\theta' = \theta'' \circ \sigma$ ([HJ88, Proposition 9.3]).

Definition C.15. Define the σ with this property as *the orbitiser with respect to* θ' *and* θ''.

We shall be interested in those $\widetilde{\Theta}$-site extensions 'which are actually Θ-sites' – by which we mean those $\widetilde{\Theta}$-sites of a formally p-adic field F, $\theta = (\pi, \varphi)$, such that $\pi(F) \subseteq \mathbb{Q}_p \cup \{\infty\}$ and $\varphi(F^*) \subseteq \Phi$. This condition will be denoted "$\theta(F) \in \Theta$". Informally, such $\widetilde{\Theta}$-sites 'are' Θ-sites which have p-adic valuation & p-adic closure information compatible in a manner with Galois extensions.

[31] $\widetilde{\mathbb{Q}_p}^*$ can again be identified as a subgroup of $\widetilde{\Phi}$, by [HJ88, Lemma 9.2].

Definition C.16. ([HJ88, p. 180].) Let L/K be a Galois extension. The *space of sites* $X(L/K)$ is defined as $\{\theta : \theta \text{ is a } \widetilde{\Theta}\text{-site of } L, \text{ with } Res_K(\theta)(K) \in \Theta\}$, equipped with the subspace topology of $(\widetilde{\mathbb{Q}_p} \cup \{\infty\})^L \times \widetilde{\Phi}^{L^*}$ (where topologically $\widetilde{\mathbb{Q}_p} \cup \{\infty\}$ is given by one-point compactification, and the notation "A^B" denotes the set of maps $B \to A$).

We write "$X(K)$" if $L = K$; this is the *space of sites of* K.

Finally, to give our most important example:

Definition C.17. Let L/K be a Galois extension. Define

$$\mathfrak{Gal}(L/K) := \langle \mathrm{Gal}(L/K),\, X(L/K) \xrightarrow{d} \mathrm{Hom}(G_{\mathbb{Q}_p}, \mathrm{Gal}(L/K)) \rangle,$$

where $d(\theta) : G_{\mathbb{Q}_p} \to \mathrm{Gal}(L/K)$ is the map

$$d(\theta)(g) := \text{the orbitiser with respect to } \theta \text{ and } g \circ \theta.$$

(Recall 'orbitiser' from *Definition C.15.*)

Remark C.18. It is highly nontrivial that $\mathfrak{Gal}(L/K)$ is indeed a $G_{\mathbb{Q}_p}$-structure.

First, $X(L/K)$ is Boolean [HJ88, Lemma 10.3 (a)]. Indeed, one shows for finite Galois L_0/K that $X(L_0/K)$ is a closed subset of the Boolean space $(E \cup \{\infty\})^{L_0} \times \Phi_E^{L_0^*}$, where E is a sufficiently large finite extension of $\mathbb{Q}_p$. One also shows we have the expected isomorphism $X(L/K) \cong \varprojlim X(L_0/K)$. Next, the action $\theta^\sigma := \theta \circ \sigma$ of $\mathrm{Gal}(L/K)$ on $X(L/K)$ is continuous and regular (*Remark 10.4, Proposition 9.3 (b) ibid.*), and $d : X(L/K) \to \mathrm{Hom}(G_{\mathbb{Q}_p}, \mathrm{Gal}(L/K))$ is continuous as it is the inverse limit of continuous maps $d_{L_0} : X(L_0/K) \to \mathrm{Hom}(G_{\mathbb{Q}_p}, \mathrm{Gal}(L_0/K))$ (argued in *Proposition 10.7 (a) ibid.*; the fact d_{L_0} is continuous follows from *Lemma 10.6 ibid.*). Finally, the action of $\mathrm{Gal}(L/K)$ on $X(L/K)$ is compatible with d, by *Definition C.17* and a diagram chase.

We also recover *Example B.8:* when L/K, F/K are Galois extensions, the canonical restriction map $\mathrm{Res} : \mathfrak{Gal}(L/K) \to \mathfrak{Gal}(F/K)$ is a cover ([HJ88, Proposition 10.7 (b) & (c)]). □

References

[AF16] Anscombe, S. and Fehm, A. The existential theory of equicharacteristic henselian valued fields. *Algebra Number Theory*, **10**(3): pp. 665–683 (2016).

[AJ19] Anscombe, S. and Jahnke, F. Characterising NIP henselian fields. `arXiv:1911.00309` (2019).

[AK65] Ax, J. and Kochen, S. Diophantine Problems Over Local Fields I. *Amer. Jour. Math.*, **87**(3): pp. 605–630 (1965).

[BK17] Blaszczok, A. and Kuhlmann, F. On maximal immediate extensions of valued fields. *Math. Nachr.*, **290**(1): pp. 7–18 (2017).

[Ceg81] Cegielski, P. Theorie elementaire de la multiplacation des entiers naturels. In *Model Theory and Arithmetic* (edited by C. Berline et al.), pp. 44–89. Springer (1981).

[Cha02] Chatzidakis, Z. Properties of Forking in ω-Free Pseudo-Algebraically Closed Fields. *J. Symb. Logic*, **67**(3): pp. 957–996 (2002).

[Che84] Cherlin, G. Undecidability of Rational Function Fields in Nonzero Characteristic. In *Studies in Logic and the Foundations of Mathematics, Volume 112* (edited by G. Lolli, G. Longo, and A. Marcja), pp. 85–95. Elsevier (1984).

[Che14] Chernikov, A. Theories without the tree property of the second kind. *Ann. Pure Appl. Logic*, **165**(2): pp. 695–723 (2014).

[CK12] Chang, C. and Keisler, H. *Model Theory*. Dover. Third Edition (2012).

[CKS15] Chernikov, A., Kaplan, I., and Simon, P. Groups and Fields with NTP_2. *Proc. Amer. Math. Soc.*, **143**(1): pp. 395–406 (2015).

[CQ52] Church, A. and Quine, W. V. Some Theorems on Definability and Decidability. *J. Symb. Logic*, **17**(3): pp. 179–187 (1952).

[CR16] Chernikov, A. and Ramsey, N. On model-theoretic tree properties. *J. Math. Logic*, **16**(2) (2016).

[CS80] Cherlin, G. and Shelah, S. Superstable fields and groups. *Ann. Math. Logic*, **18**(3): pp. 227–270 (1980).

[CvdDM80] Cherlin, G., van den Dries, L., and Macintyre, A. The Elementary Theory of Regularly Closed Fields. *Unpublished manuscript*. Retrieved from `sites.math.rutgers.edu/∼cherlin/Preprint/CDM2.pdf` (Distributed 1980).

[Del81] Delon, F. *Quelques propriétés des corps valués en théorie des modèles*. Ph.D. thesis, Université Paris VII (1981).

[Del99] Delon, F. Separably closed fields. In *Model Theory and Algebraic Geometry* (edited by E. Bouscaren), pp. 143–177. Springer. Lecture Notes in Mathematics, vol. 1696 (1999).

[Dit18] Dittmann, P. *A Model-Theoretic Approach to the Arithmetic of Global Fields*. Ph.D. thesis, University of Oxford (2018).

[DPR61] Davis, M., Putnam, H., and Robinson, J. The Decision Problem for Exponential Diophantine Equations. *Ann. of Math. (2)*, **74**(3): pp. 425–436 (1961).

[Dur80] Duret, J.-L. Les corps faiblement algébriquement clos non séparablement clos ont la propriété d'indépendence. In *Model theory of algebra and arithmetic* (*Proc. Conf., Karpacz, 1979*) (edited by L. Pacholski, J. Wierzejewski, and A. Wilkie), pp. 136–162. Springer. Lecture Notes in Mathematics, vol. 834 (1980).

[Efr91] Efrat, I. Absolute Galois Groups of p-Adically Maximal PpC Fields. *Forum Math.*, **3**(5): pp. 437–460 (1991).

[Efr92] Efrat, I. Undecidability of pseudo p-adically closed fields. *Arch. Math.*, **58**(7–8): pp. 444–452 (1992).

[Eis03] Eisenträger, K. Hilbert's Tenth Problem for algebraic function fields of characteristic 2. *Pacific J. Math.*, **210**(2): pp. 261–281 (2003).

[Eis12] Eisenträger, K. Hilbert's Tenth Problem for function fields of varieties over algebraically closed fields of positive characteristic. *Monatsh. Math.*, **168**(1): pp. 1–16 (2012).

[ELTT65] Ershov, Y., Lavrov, I., Taimanov, A., and Taitslin, M. Elementary Theories. *Russian Math. Surveys*, **20**(4): pp. 35–105. (English version). (1965).

[EO07] Ealy, C. and Onshuus, A. Characterizing Rosy Theories. *J. Symb. Logic*, **72**(3): pp. 919–940 (2007).

[EP05] Engler, A. J. and Prestel, A. *Valued Fields*. Springer. Springer Monographs in Mathematics (2005).

[Ers65a] Ershov, Y. On the elementary theory of maximal normed fields. *Soviet Math. Dokl.*, **6**: pp. 1390–1393 (1965).

[Eršˇ65b] Eršov, Y. Нерзрешимость некоторых Полей. *Dokl. Akad. Nauk SSSR*, **161**(1): pp. 27–29. English: "Undecidability of certain fields" (1965).

[Eršˇ80] Eršov, Y. Проблемы разрешимости и конструктивныые модели. "Nauka", Moscow. English: "Decision problems and constructivizable models", Monographs in Mathematical Logic and Foundations of Mathematics (1980).

[Ers81] Ershov, Y. Undecidability of Regularly Closed Fields. *Algebra and Logic*, **20**(4): pp. 257–260 (1981).

[Ers84] Ershov, Y. Two theorems on regularly r-closed fields. *J. Reine Angew. Math.*, **347**: pp. 154–167 (1984).

[ES09] Eisenträger, K. and Shlapentokh, A. Undecidability in Function Fields of Positive Characteristic. *Int. Math. Res. Not. IMRN*, **2009**(21): pp. 4051–4086 (2009).

[ES13] Eisenträger, K. and Shlapentokh, A. Hilbert's Tenth Problem over function fields of positive characteristic not containing the algebraic closure of a finite field. `arXiv:1306.2669` (2013).

[ES17] Eisenträger, K. and Shlapentokh, A. Hilbert's Tenth Problem over function fields of positive characteristic not containing the algebraic closure of a finite field. *J. Eur. Math. Soc. (JEMS)*, **19**(7): pp. 2103–2138 (2017).

[Feh10] Fehm, A. *Decidability of Large Fields of Algebraic Numbers*. Ph.D. thesis, Tel Aviv University (2010).

[Feh17] Fehm, A. The Elementary Theory of Large Fields of Totally $\mathfrak{S}$-adic Numbers. *J. Inst. Math. Jussieu*, **16**(1): pp. 121–154 (2017).

[FJ08] Fried, M. and Jarden, M. *Field Arithmetic*. Springer-Verlag. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge; A Series of Modern Surveys in Mathematics, Volume 11, 3rd Edition (2008).

[Fri87] Fried, M. D. Irreducibility results for separated variables equations. *J. Pure Appl. Algebra*, **48**(1-2): pp. 9–22 (1987).

[Gro87] Grob, C. *Die Entscheidbarkeit der Theorie der maximalen pseudo p-adisch abgeschlossenen Körper*. Ph.D. thesis, Universität Konstanz (1987).

[Haa18] Haase, C. A Survival Guide to Presburger Arithmetic. *SIGLOG News*, **5**(3): pp. 67–82 (2018).

[Har84] Haran, D. The Undecidability of Pseudo Real Closed Fields. *Manuscripta Math.*, **49**: pp. 91–108 (1984).

[Har90] Haran, D. Cohomology Theory of Artin-Schreier Structures. *J. Pure Appl. Algebra*, **69**: pp. 141–160 (1990).

[Har93] Haran, D. On the Cohomological Dimension of Artin-Schreier Structures. *J. Algebra*, **156**(1): pp. 219–236 (1993).

[HHJ19] Halevi, Y., Hasson, A., and Jahnke, F. A Conjectural Classification of Strongly Dependent Fields. *Bull. Symb. Log.*, **25**(2): pp. 182–195 (2019).

[HHJ20] Halevi, Y., Hasson, A., and Jahnke, F. Definable V-topologies, Henselianity and NIP. *J. Math. Log.*, **20**(2): pp. 1–33 (2020).

[Hil00] Hilbert, D. Mathematische Probleme. *Nachr. Königl. Gesell. Wiss. Göttingen, Mathematisch-Physikalische Klasse*, pp. 253–297 (1900).

[HJ85] Haran, D. and Jarden, M. The Absolute Galois Group of a Pseudo Real Closed Field. *Ann. Sc. Norm. Super. Pisa Cl. Sci. Série 4*, **12**(3): pp. 449–489 (1985).

[HJ88] Haran, D. and Jarden, M. The Absolute Galois Group of a Pseudo p-Adically Closed Field. *J. Reine Angew. Math.*, **383**: pp. 147–206 (1988).

[HJ21] Haran, D. and Jarden, M. *The Absolute Galois Group of a Semi-Local Field*. Springer. Springer Monographs in Mathematics (2021).

[HJP05] Haran, D., Jarden, M., and Pop, F. P-adically projective groups as absolute Galois groups. *Int. Math. Res. Not. IMRN*, **2005**(32): pp. 1957–1995 (2005).

[Hod93] Hodges, W. *Model Theory*. Cambridge University Press. Encyclopedia of Mathematics and its Applications, Volume 42 (1993).

[HP19] Halevi, Y. and Palacín, D. The dp-rank of Abelian groups. *J. Symb. Logic*, **84**(3): pp. 957–986 (2019).

[HR85] Herfort, W. and Ribes, L. Torsion elements and centralizers in free products of profinite groups. *J. Reine Angew. Math.*, **358**: pp. 155–161 (1985).

[Jar72] Jarden, M. Elementary statements over large algebraic fields. *Trans. Amer. Math. Soc.*, **164**: pp. 67–91 (1972).

[Jar88] Jarden, M. The algebraic nature of the elementary theory of PRC fields. *Manuscripta Math.*, **60**: pp. 463–475 (1988).

[Jar91] Jarden, M. Algebraic realization of p-adically projective groups. *Compos. Math.*, **79**(1): pp. 21–62 (1991).

[JTWY21] Johnson, W., Tran, C.-M., Walsberg, E., and Ye, J. The étale-open topology and the stable field conjecture. `arXiv:2009.02319v2` (2021).

[Koe14] Koenigsmann, J. Undecidability in number theory. In *Model theory in Algebra, Analysis and Arithmetic* (edited by H. D. Macpherson and C. Toffalori), pp. 159–195. Springer-Verlag. *Available at* `arXiv:1309.0441` (2014).

[Koe16a] Koenigsmann, J. Defining $\mathbb{Z}$ in $\mathbb{Q}$. *Ann. of Math.*, **183**(1): pp. 73–93 (2016).

[Koe16b] Koenigsmann, J. On a Question of Abraham Robinson. *Israel J. Math.*, **214**(2): pp. 931–943 (2016).

[KP11] Krupiński, K. and Pillay, A. On stable fields and weight. *J. Inst. Math. Jussieu*, **10**(2): pp. 349–358 (2011).

[KPSV16] Koenigsmann, J., Pasten, H., Shlapentokh, A., and Vidaux, X. Definability and Decidability Problems in Number Theory. *Oberwolfach Rep.*, **13**(4): pp. 2793–2866 (2016).

[KR92a] Kim, K. H. and Roush, F. W. Diophantine unsolvability for function fields over certain infinite fields of characteristic p. *J. Algebra*, **152**(1): pp. 230–239 (1992).

[KR92b] Kim, K. H. and Roush, F. W. Diophantine unsolvability of $\mathbb{C}(t_1, t_2)$. *J. Algebra*, **150**(1): pp. 35–44 (1992).

[Kru15] Krupiński, K. Superrosy fields and valuations. *Ann. Pure Appl. Logic*, **166**(3): pp. 342–357 (2015).

[Kün89] Künzi, U. M. Decidable theories of pseudo-p-adic closed fields. *Algebra and Logic*, **28**(6): pp. 421–438 (1989).

[Lan94] Lang, S. *Algebraic Number Theory*. Springer. Second Edition, Graduate Texts in Mathematics 110 (1994).

[Lea67] Leahey, W. Sums of Squares of Polynomials with Coefficients in a Finite Field. *Amer. Math. Monthly*, **74**(7): pp. 816–819 (1967).

[Mac71] Macintyre, A. On ω_1-categorical theories of fields. *Fund. Math.*, **71**(1): pp. 1–25 (1971).

[Mac76] Macintyre, A. On Definable Subsets of p-Adic Fields. *J. Symb. Logic*, **41**(3): pp. 605–610 (1976).

[Mac98] Mac Lane, S. *Categories for the Working Mathematician*. Springer. Second Edition, Graduate Texts in Mathematics 5 (1998).

[Mar02] Marker, D. *Model Theory: An Introduction*. Springer. Graduate Texts in Mathematics 217 (2002).

[Mar18] Marker, D. Model Theory of Valued Fields. *Lecture notes, Available at* `homepages.math.uic.edu/∼marker/valued_fields.pdf` (2018).

[Mat70] Matiyasevich, Y. Enumerable sets are Diophantine. *Soviet Math. Dokl.*, **11**: pp. 354–358 (1970).

[Mon17] Montenegro, S. Pseudo real closed fields, pseudo p-adically closed fields and NTP_2. *Ann. Pure Appl. Logic*, **168**(1): pp. 191–232 (2017).

[Ons02] Onshuus, A. *Thorn-Forking in Rosy Theories*. Ph.D. thesis, University of California at Berkeley (2002).

[Pas17] Pasten, H. Definability of frobenius orbits and a result on rational distance sets. *Monatsh. Math.*, **182**: pp. 99–126 (2017).

[Pen73] Penzin, Y. Undecidability of fields of rational functions over fields of characteristic 2. *Algebra i Logika*, **12**: pp. 205–210 (1973).

[Phe87] Pheidas, T. An Undecidability Result for Power Series Rings of Positive Characteristic II. *Proc. Amer. Math. Soc.*, **103**(3): pp. 526–530 (1987).

[Phe91] Pheidas, T. Hilbert's Tenth Problem for fields of rational functions over finite fields. *Invent. Math.*, **103**(1): pp. 1–8 (1991).

[Phe04] Pheidas, T. Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic. *J. Algebra*, **273**(1): pp. 395–411 (2004).

[Poo07] Poonen, B. Uniform first-order definitions in finitely generated fields. *Duke Math. J.*, **138**(1): pp. 1–21 (2007).

[Poo09] Poonen, B. Characterizing integers amongst rational numbers with a universal-existential formula. *Amer. Jour. Math.*, **131**(3): pp. 675–682 (2009).

[Pop90] Pop, F. Fields of totally Σ-adic numbers. *Unpublished manuscript.* Announced in *Oberwolfach Report 45/1990* on *Arithmetik der Körper* in 1990, DOI: 10.14760/TB-1990-45 (1990).

[PR84] Prestel, A. and Roquette, P. *Formally p-adic Fields.* Springer. Lecture Notes in Mathematics 1050 (1984).

[Pre81] Prestel, A. Pseudo Real Closed Fields. In *Set Theory and Model Theory* (edited by R. B. Jensen and A. Prestel), pp. 127–156. Springer. Lecture Notes in Mathematics, vol. 872 (1981).

[PZ99] Pheidas, T. and Zahidi, K. Undecidable existential theories of polynomial rings and function fields. *Comm. Algebra*, **27**(10): pp. 4993–5010 (1999).

[PZ00] Pheidas, T. and Zahidi, K. Undecidability of existential theories of rings and fields: A survey. *Contemp. Math.*, **270**: pp. 49–105 (2000).

[Raj93] Rajwade, A. R. *Squares.* Cambridge University Press. London Mathematical Society: Lecture Note Series 171 (1993).

[Rei03] Reiner, I. *Maximal Orders.* Clarendon Press, Oxford. London Mathematical Society Monographs – New Series 28 (2003).

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

[Rob50] Robinson, R. An Essentially Undecidable Axiom System. *Proc. Int. Cong. Math.*, **1**: pp. 729–730 (1950).

[Rob51] Robinson, R. Undecidable rings. *Trans. Amer. Math. Soc.*, **70**(1): pp. 137–159 (1951).

[Rob59] Robinson, J. The undecidability of algebraic rings and fields. *Proc. Amer. Math. Soc.*, **10**: pp. 950–957 (1959).

[Rob62] Robinson, J. On the decision problem for algebraic rings. In *Studies in mathematical analysis and related topics, Essays in honor of George Pólya* (edited by G. Szegö et al.), pp. 297–304. Stanford University Press (1962).

[Ros02] Rosen, M. *Number Theory in Function Fields*. Springer-Verlag. Graduate Texts in Mathematics 210 (2002).

[Rot99] Rotman, J. J. *An Introduction to the Theory of Groups*. Springer. Graduate Texts in Mathematics 148, 4th Edition (1999).

[Rum80] Rumely, R. Undecidability and definability for the theory of global fields. *Trans. Amer. Math. Soc.*, **262**(1): pp. 195–217 (1980).

[RZ00] Ribes, L. and Zalesskii, P. *Profinite Groups*. Springer. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge; A Series of Modern Surveys in Mathematics, Volume 40, 2nd Edition (2000).

[Sch85] Schinzel, A. Reducibility of polynomials in several variables II. *Pacific J. Math.*, **118**(2): pp. 531–563 (1985).

[She80] Shelah, S. Simple unstable theories. *Ann. Math. Logic*, **19**(3): pp. 177–203 (1980).

[Shl93] Shlapentokh, A. Diophantine relations between rings of S-integers of fields of algebraic functions in one variable over constant fields of positive characteristic. *J. Symb. Logic*, **58**(1): pp. 158–192 (1993).

[Shl96] Shlapentokh, A. Diophantine Undecidability over Algebraic Function Fields over Finite Fields of Constants. *J. Number Theory*, **58**(2): pp. 317–342 (1996).

[Shl98] Shlapentokh, A. Diophantine definability over holomorphy rings of algebraic function fields with infinite number of primes allowed as poles. *Internat. J. Math.*, **9**(8): pp. 1041–1066 (1998).

[Shl00] Shlapentokh, A. Hilbert's Tenth Problem for Algebraic Function Fields over Infinite Fields of Constants of Positive Characteristic. *Pacific J. Math.*, **193**(2): pp. 463–500 (2000).

[Shl02a] Shlapentokh, A. Diophantine Undecidability of Function Fields of Characteristic Greater than 2, Finitely Generated over Fields Algebraic over a Finite Field. *Compos. Math.*, **132**(2): pp. 99–120 (2002).

[Shl02b] Shlapentokh, A. On Diophantine Definability and Decidability in Some Rings of Algebraic Functions of Characteristic 0. *J. Symb. Logic*, **67**(2): pp. 759–786 (2002).

[Shl05] Shlapentokh, A. Diophantine Undecidability for some Function Fields of Infinite Transcendence Degree and Positive Characteristic. *J. Math. Sci.*, **130**(2): pp. 4631–4642 (2005).

[Shl07] Shlapentokh, A. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press (2007).

[Shl15] Shlapentokh, A. On definitions of polynomials over function fields of positive characteristic. `arXiv:1502.02714` (2015).

[Sho93] Shoenfield, J. R. *Recursion Theory*. Springer-Verlag. Lecture Notes in Logic, Volume 1 (1993).

[Sil09] Silverman, J. *The Arithmetic of Elliptic Curves*. Springer. Second Edition, Graduate Texts in Mathematics 106 (2009).

[Sim15] Simon, P. *A Guide to NIP Theories*. Cambridge University Press. Lecture Notes in Logic (2015).

[Sti09] Stichtenoth, H. *Algebraic Function Fields and Codes*. Springer. Second Edition, Graduate Texts in Mathematics 254 (2009).

[Sto21] Stonestrom, A. Some model theory of $\mathrm{Th}(\mathbb{N};\cdot)$. `arXiv:2109.01131` (2021).

[SV14] Shlapentokh, A. and Videla, C. Definability and decidability in infinite algebraic extensions. *Ann. Pure Appl. Logic*, **165**(7–8): pp. 1243–1262 (2014).

[TMR53] Tarski, A., Mostowski, A., and Robinson, R. *Undecidable Theories*. North-Holland. Studies in Logic and the Foundations of Mathematics (1953).

[TZ12] Tent, K. and Ziegler, M. *A Course in Model Theory*. Cambridge University Press. Lecture Notes in Logic (2012).

[vdD14] van den Dries, L. Lectures on the Model Theory of Valued Fields. In *Model theory in Algebra, Analysis and Arithmetic* (edited by H. D. Macpherson and C. Toffalori), pp. 55–157. Springer-Verlag (2014).

[vdDL81] van den Dries, L. and Lubotzky, A. Subgroups of Free Profinite Groups and Large Subfields of $\widetilde{\mathbb{Q}}$. *Israel J. Math.*, **39**(1): pp. 957–996 (1981).

[Vid94] Videla, C. Hilbert's Tenth Problem for rational function fields in characteristic 2. *Proc. Amer. Math. Soc.*, **120**(1): pp. 249–253 (1994).

[Wag00] Wagner, F. *Simple Theories.* Springer. Mathematics and Its Applications 503 (2000).

[Wei74] Weil, A. *Basic Number Theory.* Springer Verlag (1974).

[Zie82] Ziegler, M. Einige unentscheidbare Körpertheorien. *Enseign. Math. II*, **28**(1–2): pp. 269–280 (1982).