# On the Decidability of Finite Extensions of Decidable Fields

Kesavan Thanagopal

Hertford College
University of Oxford

*A thesis submitted for the degree of*
*Doctor of Philosophy*

Trinity 2018

## Abstract

This paper is primarily concerned with the following question which first appeared in Koenigsmann's *On a Question of Abraham Robinson's*:

*Is a finite field extension of a decidable field always decidable?*

This offers a "twist" to a question that was originally posed by Abraham Robinson in 1973 which had asked whether every finitely generated extension of an undecidable field remains undecidable. The above-mentioned work of Koenigsmann from 2016 (and independently, a result of Cherlin, van den Dries, and Macintyre much earlier in the 1980s) showed that there are indeed undecidable fields which admit decidable finite extensions. This paper aims to show that one could, similarly, find examples of decidable fields which admit undecidable finite extensions, thereby answering the above-stated question negatively.

This result is achieved by identifying a sufficient condition which a decidable field must satisfy in order for it to have an undecidable finite extension. In an earlier iteration of this work, we had pointed out what we had believed to be one such condition. Unfortunately, this turned out not to be the case, which we illustrate using an explicit example. Through this demonstration, we were able to accentuate the weakness of the formerly-mentioned criterion, which we strengthen in this thesis. We provide justification that the strengthened criterion is indeed sufficient – any decidable field satisfying this strengthened criterion would form a counterexample to the above-mentioned question.

We study one such class of decidable fields, known as the wonderful extensions of the rational numbers, first introduced by Ershov in the early 2000s, whose (sufficiently saturated) elementary extensions satisfy this strengthened criterion. This provides us with a concrete counterexample which shows that there are indeed decidable fields which admit undecidable finite extensions. We also point out various attempts at finding other counterexamples to the above-mentioned question, the difficulties faced in those instances, and some further questions in the flavour of the above-mentioned question that appear to be interesting in their own rights.

# On the Decidability of Finite Extensions of Decidable Fields


Kesavan Thanagopal

Hertford College

University of Oxford

A thesis submitted for the degree of

*Doctor of Philosophy*

Trinity 2018

# Acknowledgements

This dissertation marks the end of an emotionally and intellectually enriching experience I have had in and through the University of Oxford. This journey would not have been possible without the help and guidance I had received throughout the past four years and I am truly indebted to many. I wish to take this opportunity to say a big thank you to all those who have been there.

Professor Jochen Koenigsmann, for agreeing to be my supervisor at the very start of this journey. Thank you so much for guiding me through this entire period, probing me to gain a better understanding of the subject matter, and reassuring me that what I was writing made sense through the various comments and encouragements. Thank you for being patient with me and believing in me when I was slow to make progress and did not manage to meet the deadlines that I had set for myself. Thank you for not giving up on me when I was about to give up on myself! Working with you throughout this period has provided me with the opportunity to learn more about Model Theory, Valued Fields, Field Arithmetic and other disciplines within Mathematics which, up until that point of time, were rather new to me. Thank you for introducing me to these subjects, and the study of decidability which has fascinated me ever since. The question on whether finite extensions of decidable fields remain decidable was something which you posed to me at the very beginning of this journey as a way for me to get into the habit of working with questions of this sort. Never did we imagine that this question was much harder to solve than expected. In an attempt to address this question, I had explored various other subject matters within Mathematics which I would otherwise have not done. Thank you for opening my eyes to these various subject matters that I had been truly ignorant of, up until this point.

Dr Peter Neumann, with whom I have worked with as his Teaching Assistant for Logic and Algebraic Number Theory over the course of my tenure as a graduate student. Thank you for all your valuable comments and encouragements throughout my time in Oxford, both professionally and personally. Thank you also for being not only a mentor I could look up to, but a good friend as well, providing me with various advice and suggestions regarding my academic work and my future

in general. Peter has been under the weather this year, and I wish him a speedy recovery so that he would be able to spend time doing what he loves – sharing his passion for Mathematics and Mathematics Education with the next generation of Mathematicians.

The Logic Group in Oxford for being so supportive throughout my venture into Model Theory – Professor Ehud Hrushovski, Professor Boris Zilber, Professor Jonathan Pila for offering valuable advice with regards to the question that I had been working on, suggesting possible avenues to venture into in a bid to get at a definitive answer, and suggesting improvements on previous iterations of this work. To all the friends I have made in the Logic Group over the course of my time here in Oxford: thank you for your friendship without which these four years would not have been the same!

All the friends I have made throughout my time in Oxford – friends from Hertford College, from my office, and Notre Dame – who have painstakingly listened to my "crazy" thoughts and ideas about things far beyond Mathematics. Thank you all for being really good friends, making this journey on rough waters a lot smoother and pleasant to say the least.

My family members – my father, mother and sister – who have been there for me, always supporting me and lending me a listening ear whenever I needed them. Thank you also for the financial support, allowing me pursue this doctoral programme. I am truly grateful that my parents were willing to support me, allowing me to pursue something out of my academic interest alone. I also wish to take this opportunity to say a big hello to the latest addition to my family – my nephew, baby Akilan, who was born mid-September.

Most importantly, I want to thank God for blessing me with all the above-mentioned love, care and concern from family, friends and teachers whom I have met and worked with. This dissertation would never have been possible if not for His grace.

Kesavan S/O Thanagopal

# Abstract

This paper is primarily concerned with the following question which first appeared in Koenigsmann's *On a Question of Abraham Robinson's*:

*Is a finite field extension of a decidable field always decidable?*

This offers a "twist" to a question that was originally posed by Abraham Robinson in 1973 which had asked whether every finitely generated extension of an undecidable field remains undecidable. The above-mentioned work of Koenigsmann from 2016 (and independently, a result of Cherlin, van den Dries, and Macintyre much earlier in the 1980s) showed that there are indeed undecidable fields which admit decidable finite extensions. This paper aims to show that one could, similarly, find examples of decidable fields which admit undecidable finite extensions, thereby answering the above-stated question negatively. This thesis is broken down into four main chapters.

In Chapter 1, we discuss the motivation and the history of this question. We aim to provide partial answers to Koenigsmann's question and explain situations where a finite extension of a decidable field remains decidable. This chapter also highlights the difficulty in finding a suitable counterexample that would show that there are indeed decidable fields which become undecidable under finite extensions – almost all known "classical" fields have this property. We end the chapter with a promising criterion that a field must possess in order for there to be a suitable counterexample to Koenigsmann's question.

Chapter 2 points out the insufficiency of the criterion established at the end of Chapter 1. We had mistakenly identified the criterion in Chapter 1 as being sufficient in an earlier iteration of this work, but in this chapter, we show that this cannot be the case, explaining why the said criterion is insufficient. In order to understand the intricacies of the matter, we appeal to an example involving pseudo algebraically closed (PAC) fields which accentuates this matter. Necessary background information on PAC fields are highlighted at the beginning of the chapter to ensure that the material in this paper is sufficiently self-contained. We provide a refined criterion at the end of the chapter and explain why this criterion is indeed sufficient in aiding us find a counterexample – any field which satisfies

this refined criterion would be a counterexample that would show the existence of decidable fields with undecidable finite extensions.

In Chapter 3, we provide an example of a field whose sufficiently saturated extension satisfies the refined criterion. These fields, known as Ershov's Wonderful Extensions of $\mathbb{Q}$, are multi-valued fields that satisfy three main properties – a near-Boolean property, a local-global principle, and a maximality condition. In order to better understand the structure of these wonderful extensions, we begin the chapter with a brief introduction to valued and multi-valued fields. We then introduce the wonderful extensions of $\mathbb{Q}$ (and a related class of fields known as $W$-extensions of $\mathbb{Q}$) which have been described by Ershov in a series of papers and an encyclopedic monograph in the most general sense. We streamline these arguments and show that such fields do indeed exist, focusing specifically on the $W$-extensions (and $W^+$-extensions/ wonderful extensions) of $\mathbb{Q}$. We provide explicit descriptions and examples of such fields, something that was not provided in Ershov's *On Surprising Extensions of the Field of Rationals* which introduced these fields. We also show that $W$-extensions (and $W^+$-extensions) are "model-theoretically" unique, i.e. there is no first-order means of telling apart two $W$-extensions of $\mathbb{Q}$ (and correspondingly, $W^+$-extensions of $\mathbb{Q}$). This provides the basis of a decidability result for these fields. We then go on to explain how one could use these fields to construct a counterexample to Koenigsmann's question by showing that a sufficiently saturated extension of such fields would satisfy the refined criterion as set out in Chapter 2.

In the final chapter, we highlight some of the other avenues that we had earlier pursued in an attempt to find a counterexample to the above-stated question. Since the counterexamples to Robinson's original question were discovered within the class of PAC fields, it was believed that one could similarly find counterexamples to Koenigsmann's question within this realm as well. This led to the idea of coding undecidability into graph structures which could, in turn, be coded within projective profinite groups – an avenue suggested by Hrushovski in private communication. We point out some of the difficulties that were faced while pursuing this option. While we were ultimately unsuccessful in finding a counterexample within the class of PAC fields, several interesting observations and related questions sprung up during this pursuit which we believe are worth exploring further in future works.

# Contents

**Notations** **ix**

**1 Introduction** **1**
1.1 Motivation . . . . . 1
1.2 Some Observations and Partial Results . . . . . 3

**2 Criterion Refined** **11**
2.1 Introduction to Some "Non-Classical" Fields . . . . . 12
2.1.1 Hilbertian Fields . . . . . 12
2.1.2 Pseudo Algebraically Closed Fields . . . . . 13
2.2 Refining Criterion 2.0.1 . . . . . 22
2.2.1 Insufficiency of Criterion 2.0.1 . . . . . 23
2.2.2 Strengthening Criterion 2.0.1 . . . . . 26

**3 Ershov's Wonderful Extensions of $\mathbb{Q}$** **31**
3.1 Introduction to Valued and Multi-Valued Fields . . . . . 32
3.2 Wonderful Extensions of $\mathbb{Q}$ . . . . . 57
3.2.1 A Sketch of the Existence of Wonderful Extensions of $\mathbb{Q}$ . . 58
3.2.2 A Sketch of the Decidability of Wonderful Extensions of $\mathbb{Q}$ . 77
3.3 The Undecidability of Finite Extensions of Wonderful Extensions of $\mathbb{Q}$ 89

**4 Attempts at Constructing a PAC Counterexample** **99**
4.1 Modifying Known Counterexamples . . . . . 100
4.2 Coding "Undecidability" . . . . . 106
4.2.1 Addressing Question 1 . . . . . 107
4.2.2 Addressing Question 2 . . . . . 122

**References** **135**

**Index** **142**

# Notations

| | |
|---|---|
| $\widetilde{K}$ . . . . . | The (separable) algebraic closure of $K$ |
| $\mathtt{Th}(K)$ . . . . . | The first-order theory of $K$ |
| $\mathscr{L}_{\mathbf{ring}}$ . . . . . | The language of rings, $\mathscr{L}_{\text{ring}} := \{+, \times, \ ; \ 0, 1\}$ |
| $\mathscr{L}_{\mathbf{or}}$ . . . . . | The language of ordered rings, $\mathscr{L}_{\text{or}} := \mathscr{L}_{\text{ring}} \cup \{<\}$ |
| $\mathscr{L}_{\mathbf{CSIS}}$ . . . . . | The language of complete stratified inverse systems |
| $\mathscr{L}_{\mathbf{log}}$ . . . . . | The language of linearly ordered groups, $\mathscr{L}_{\text{log}} := \{0 \ ; \ +, - \ ; \ \leq\}$ |
| $K^{\mathbf{prime}}$ . . . . . | The prime subfield of $K$ which is isomorphic to $\mathbb{Q}$ if the characteristic of $K$ is zero, or isomorphic to the finite field $\mathbb{F}_p$ for some rational prime $p$ if the characteristic of $K$ is $p$ |
| $\mathtt{Sent}_{\mathscr{L}_{\mathbf{ring}}}$ . . . . | The set of sentences in the language of rings |
| $\mathtt{Formulae}_{\mathscr{L}_{\mathbf{ring}}}$ . | The set of formulae in the language of rings |
| $\mathbb{Q}_p$ . . . . . | The field of $p$-adic numbers |
| **PAC Field** . . | A pseudo algebraically closed field |
| $\mathfrak{X}(K)$ . . . . . | The space of orderings on $K$, $\mathfrak{X}(K) := \{P \mid P \text{ is an ordering of } K\}$ |
| $\mathbf{G}_K$ . . . . . | The absolute Galois group of $K$, $\mathbf{G}_K := \text{Gal}(\widetilde{K}/K)$ |
| $K^{\mathbf{alg}}$ . . . . . | The algebraic part of $K$, $K^{\text{alg}} := \begin{cases} K \cap \widetilde{\mathbb{Q}} & \text{if the characteristic of the field } K \text{ is } 0; \\ K \cap \widetilde{\mathbb{F}_p} & \text{if the characteristic of the field } K \text{ is } p > 0. \end{cases}$ |
| $\mathtt{Th}^{\mathbf{alg}}(K)$ . . . . | The subset of $\mathtt{Th}(K)$ that determines $K^{\text{alg}}$ up to isomorphism |
| $\mathcal{G}$ . . . . . | A profinite group, $\mathcal{G} := \varprojlim_{i \in I} G_i$, where $G_i$'s are finite groups, and $I$ a partially ordered set |
| $\widehat{F}_\omega$ . . . . . | The free profinite group on countably many generators |
| $\mathtt{S}(\mathcal{G})$ . . . . . | The complete inverse system of $\mathcal{G}$ |
| $K^*$ . . . . . | A sufficiently saturated elementary extension of $K$ |
| $q(R)$ . . . . . | The quotient field of a valuation ring $R$ |

$\mathfrak{m}_R$ . . . . . The maximal ideal of a local ring $R$

$\Gamma_R$ . . . . . The value group of a valuation ring $R$

$\upsilon_R$ . . . . . The valuation of the field $K = q(R)$ determined by the valuation ring of $R$.

$K_R$ . . . . . The residue field, $K_R = K_{\upsilon_R} = R/\mathfrak{m}_R$

$\langle K, R\rangle \leq \langle K', R'\rangle$ The valued field $\langle K', R'\rangle$ is an extension of the valued field $\langle K, R\rangle$

$R^h$ . . . . . The Henselization of the valuation ring $R$

$\mathbb{H}_R(K)$ . . . . . The Henselization of $\langle K, R\rangle$, $\mathbb{H}_R(K) := \langle K^h, R^h\rangle$

$R_S$ . . . . . The localization of $R$ at $S$, $R_S = S^{-1}R = \left\{\frac{r}{s} \;\middle|\; r \in R, s \in S\right\}$

$R_{\mathfrak{p}}$ . . . . . The localization of $R$ at $\mathfrak{p}$, $R_{\mathfrak{p}} = \{\frac{r}{s} \mid r \in R, s \in R \setminus \mathfrak{p}\}$

$R^{ic}$ . . . . . The integral closure of $R$

$R_W$ . . . . . The holomorphy ring which is an intersection of all the valuation rings in $W$, $R_W := \bigcap\{R_i \mid R_i \in W\}$

$W(R)$ . . . . . The set $\{R_{\mathfrak{m}} \mid \mathfrak{m}$ is a maximal ideal of $R\} = \{R_{\mathfrak{m}} \mid \mathfrak{m} \in m\mathrm{Spec}(R)\}$

$V_{a^{-1}}$ . . . . . Open sets in the Zariski topology, $V_{a^{-1}} = \{R_i \mid R_i \in W,\ a^{-1} \in R_i\}$, where $a \in R_W \setminus \{0\}$

$W_a$ . . . . . The set $W \setminus V_{a^{-1}}$, where $W$ is an affine family of valuation rings

$\mathbb{P}$ . . . . . The set of all rational primes

$\mathbb{P}_{\mathbf{nr}}$ . . . . . A non-recursive set of rational primes

$R \preccurlyeq_1 R'$ . . . . . $R$ is existentially closed in $R'$

$J(R)$ . . . . . The Jacobson radical of $R$

$\mathbb{R}_L(K)$ . . . . . The real closure of $\langle K, L\rangle$, $\mathbb{R}_L(K) := \langle K^{rc_L}, L^{rc}\rangle$, where $K^{rc_L}$ is the real closure of the field $K$ (with respect to the ordering $L$), and $L^{rc}$, its (unique) ordering

$\mathbb{A}_{\mathbb{Z}}$ . . . . . The ring of integral adeles of $\mathbb{Q}$, $\mathbb{A}_{\mathbb{Z}} := \mathbb{R} \times \widehat{\mathbb{Z}}$

$\mathbb{A}_{\mathbb{Q}}$ . . . . . The ring of adeles of $\mathbb{Q}$, $\mathbb{A}_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{A}_{\mathbb{Z}}$

$E(W)$ . . . . . The set of all subsets of $W$ that are open-closed and compact in the Constructive topology, $E(W) := \{W_A \mid A \subseteq_{\text{finite}} R_W \setminus \{0\}\}$

$\mathbb{E}(R)$ . . . . . The lattice structure, $\mathbb{E}(R) := \langle E(R), \wedge, \vee, \perp\rangle$

$\gamma_p(x)$ . . . . . The $p$-adic Kochen operator, $\gamma_p(x) := \frac{1}{p} \cdot \frac{x^p - x}{(x^p - x)^2 - 1}$

$R_p[\gamma(L)]$ . . . . The subring of $L$ generated by $\gamma_p(L) \cup R_p$ where $R_p = \lambda_p^{-1}(\mathbb{Z}_p)$ is the valuation ring of $K$ associated with the prime $p$

$R^p_{\mathbf{Koc}}(L)$ . . . . The $p$-adic Kochen ring,

$$R^p_{\mathrm{Koc}}(L) := \left\{ \frac{t}{1-ps} \;\middle|\; t, s \in R_p[\gamma_p(L)] \text{ and } 1-ps \neq 0 \right\}$$

*In re mathematica ars proponendi quaestionem pluris facienda est quam solvendi.*

*In mathematics the art of proposing a question must be held of higher value than solving it.*

— Georg Cantor [Can67]

# 1 Introduction

## Contents


**1.1 Motivation . . . . . 1**
**1.2 Some Observations and Partial Results . . . . . 3**


## 1.1 Motivation

This paper aims to address the following question raised in Koenigsmann's "On a Question of Abraham Robinson" [Koe16]:

**Question 1.1.1** (cf. Question 4 of [Koe16])**.** *Is a finite field extension of a decidable field always decidable?*

This question offers a twist on a question that was originally posed by Abraham Robinson [Rob73] in his retiring presidential address, presented at the annual meeting of the Association for Symbolic Logic in Dallas, in 1973. In that address, Robinson asked the following:

**Question 1.1.2.** *Is a finitely generated extension of an undecidable field always undecidable?*

As it turns out, the answer to Question (1.1.2) is a definitive "no" in a rather strong sense, and this was proven by Koenigsmann [Koe16][1]via the following theorem:

**Theorem 1.1.3** (cf. Theorem 1 of [Koe16])**.** *There are uncountably many pairwise elementarily inequivalent undecidable algebraic extensions $K$ of $\widetilde{\mathbb{Q}}(t)$ for which every proper finite extension, $L$, of $K$ is decidable (and all these $L$'s are elementarily equivalent).*

Here, $\widetilde{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$, and $\widetilde{\mathbb{Q}}(t)$ denotes the rational function field in one variable over $\widetilde{\mathbb{Q}}$. In fact, one could narrow down Robinson's question to fields that are algebraic over $\mathbb{Q}$ and ask, instead, the following:

**Question 1.1.4.** *Is a finite extension, $L$, of an undecidable algebraic extension, $K$, of $\mathbb{Q}$ always undecidable?*

Indeed, if $K$ were taken to be a number field (and so $K$ is a finite extension of $\mathbb{Q}$), then this had to be the case since any finite extension, $L$, of a number field is itself a finite extension of $\mathbb{Q}$, and is thus undecidable by a result of Julia Robinson [Rob59]. This, however, is not the case in general. Again, Koenigsmann's paper points out that there are finite extensions of undecidable fields that are decidable via the following theorem:

**Theorem 1.1.5** (cf. Theorem 2 of [Koe16])**.** *For every prime $p$, there are infinitely many pairwise non-isomorphic decidable algebraic extensions, $L$, of $\mathbb{Q}$ having uncountably many undecidable subfields, $K$, of degree $[L : K] = p$.*

Before proceeding any further, we begin by first elucidating what we mean by a ***decidable field***. A field $K$ is said to be decidable if the (first-order) theory of $K$, denoted $\mathtt{Th}(K)$, in the language of rings, $\mathscr{L}_{\text{ring}} := \{+, \times, \ ; \ 0, 1\}$,

[1] As it turns out, Gregory Cherlin, Lou van den Dries and Angus Macintyre had already addressed this question sometime in 1980 in their (yet) unpublished manuscript entitled *The Elementary Theory of Regularly Closed Fields* (cf. [CDM80a]; [CDM80b]), in which they had constructed an "outlandish example" of an undecidable field of infinite transcendence degree over $\mathbb{Q}$ with all proper finite extensions being decidable and isomorphic.

is decidable. That is to say that there exists an algorithm which, given an input of any $\mathscr{L}_{\text{ring}}$-sentence, $\varphi$, produces an output

$$\textsc{Output} = \begin{cases} \texttt{Yes} & \text{if } \varphi \in \texttt{Th}(K), \text{ or equivalently, } K \models \varphi \\ \texttt{No} & \text{otherwise} \end{cases}$$

or equivalently, that there is an effective axiomatisation of the theory of $K$, $\texttt{Th}(K)$.

While there are known instances where finite extensions of decidable fields remain decidable, in general, it is not entirely clear why decidability should always "move up" finite extensions, and this paper aims to investigate whether this would, inevitably, have to be the case so long as the field extension considered is a finite one. It is worth pointing out that if we were to relax the condition necessitating that the field extension be a finite one and allow, instead, for infinite extensions to be considered, then one could easily cook up counterexamples where the base field is decidable and the field extension is undecidable; for instance, consider a real closed field $K$, which is known to be decidable by a result of Alfred Tarski [Tar51][2], and let the field extension be $L = K(\alpha)$, where $\alpha$ is an element transcendental over $K$. Then, by a result of Raphael M. Robinson [Rob64], we know that $L$ is undecidable since one is able to define a model for the arithmetic of positive integers in $L$.

## 1.2 Some Observations and Partial Results

As mentioned above, there are several known instances where finite extensions of certain decidable fields remain decidable. We begin by first highlighting those known instances:

**Observation 1.2.1.** *If the base field, $K$, is taken to be a finite field, then any finite extension, $L$, of $K$, would itself also be finite and therefore would remain decidable as well.*

[2] It is worth pointing out that while Tarksi showed that $\mathbb{R}$ is decidable in the language of ordered rings, $\mathscr{L}_{\text{or}} := \mathscr{L}_{\text{ring}} \cup \{<\}$, $\mathbb{R}$ (and hence any other real closed field) is also decidable in $\mathscr{L}_{\text{ring}}$ since the same algorithm that checks whether a $\mathscr{L}_{\text{or}}$-sentence $\varphi \in \texttt{Th}(\mathbb{R})$ would necessarily check if a $\mathscr{L}_{\text{ring}}$-sentence $\psi \in \texttt{Th}(\mathbb{R})$. This follows immediately because every $\mathscr{L}_{\text{ring}}$-sentence is, after all, a $\mathscr{L}_{\text{or}}$-sentence.

Furthermore, we have the following:

**Observation 1.2.2.** *Suppose $K$ is a decidable field, and let $L$ be a finite extension of $K$, obtained by adjoining elements which are algebraic over the prime subfield, $K^{prime}$[3], of $K$. Then $L$ is decidable as well.*

Instead of proving the above observation, we aim to provide a proof for a more general claim of the above. Namely,

**Observation 1.2.3.** *Suppose $L = K(\alpha) = K[X]/\left(\sum_{i=0}^{n-1} a_i X^i\right)$ is a finite field extension of a decidable field $K$, and the $n$-tuple of coefficients $\overline{a}$ realises an isolated type. Then $L$ is also decidable.*

*Proof.* We begin by first showing that $L = K(\alpha)$ is interpretable in $K$ using the language $\mathscr{L}_{\text{ring}} \cup \{\overline{a}\}$ where $\overline{a}$ is the $n$-tuple of coefficients of the minimal polynomial of $\alpha$ over $K$.

We interpret the symbols of $\mathscr{L}_{\text{ring}} = \{+, \times\ ;\ 0, 1\}$ in the following manner:

- "$+$" as the usual addition on the vector space $K^n$, the direct sum of $n$ copies of $K$;
- "$\times$" in the following way:
  Let
  $$M_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$
  be a $(n \times n)$ matrix. Note that we had derived this matrix from $f_n(\overline{a})(\alpha) = 0$. Then, we have that
  $$(x_1, x_2, \ldots, x_n) \times (y_1, y_2, \ldots, y_n) = (x_1 I_{n\times n} + x_2 M_\alpha + x_3 M_\alpha^2 + \cdots + x_n M_\alpha^{n-1}) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix},$$
  where $I_{n\times n}$ is the $n \times n$ identity matrix;

[3] We recall that when the field $K$ is of characteristic zero, $K^{prime}$ is isomorphic to $\mathbb{Q}$, and when the characteristic of $K$ is $p$ for some rational prime $p$, then $K^{prime}$ is isomorphic to $\mathbb{F}_p$, the finite field of $p$ elements.

- the constant "0" as $(0, 0, \ldots, 0)$;
- the constant "1" as $(1, 0, \ldots, 0)$.

Note that while "+", "0" and "1" are all definable in $K$ without any additional parameters, "$\times$" was defined using the $n$-tuple $\overline{a}$. However, since we had included the $n$-tuple $\overline{a}$ into our expanded language, we see that $L = K(\alpha)$ is indeed interpretable in $K$ using the language $\mathscr{L}_{\text{ring}} \cup \{\overline{a}\}$.

Now since $L$ is interpretable in $K$ using the expanded language $\mathscr{L}_{\text{ring}} \cup \{\overline{a}\}$, if $K$ were to be decidable in the expanded language, then $L$ has to be decidable in the expanded language too. Notice further, that if $L$ were to be decidable in the expanded language, $\mathscr{L}_{\text{ring}} \cup \{\overline{a}\}$, then, in particular, $L$ would also be decidable in $\mathscr{L}_{\text{ring}}$. Thus, in order to show that $L$ is decidable in $\mathscr{L}_{\text{ring}}$, it suffices to show that $K$ is decidable in the expanded language $\mathscr{L}_{\text{ring}} \cup \{\overline{a}\}$, i.e. the structure $\langle K \ ; \ +, \times \ ; \ \overline{a} \rangle$ is decidable.

Since, by our assumption, we know that $\overline{a}$ realises an isolated type, let us suppose that $\theta(\overline{x})$ isolates $\mathtt{tp}(\overline{a})$. We then have that

$$\langle K \ ; \ +, \times \ ; \ \overline{a} \rangle \models \psi(\overline{a}) \qquad \text{if and only if} \qquad K \models \forall \overline{x} \ \left( \theta(\overline{x}) \to \psi(\overline{x}) \right).$$

Since $K$ is decidable in $\mathscr{L}_{\text{ring}}$, the latter statement can be recursively determined and so we see that the structure $\langle K \ ; \ +, \times \ ; \ \overline{a} \rangle$ is indeed decidable. We thus have that $L$ is decidable in $\mathscr{L}_{\text{ring}} \cup \{\overline{a}\}$, and hence, also in $\mathscr{L}_{\text{ring}}$. □

Since $n$-tuples of algebraic elements realise isolated types, Observation (1.2.3) is indeed a generalisation of Observation (1.2.2). Observation (1.2.3) above also alludes to why Question (1.1.1) is only interesting if we "control" what is allowed within our language – if our language consists of as many constant symbols $c_i$'s, each to be interpreted as a (distinct) element of the structure, then any finite extension of a decidable field (as considered within this expanded language) would remain decidable as the finite extension would trivially be parameter-free interpretable in

such a language. Our next observation underscores the main difficulty in finding possible counterexamples to Question (1.1.1):

**Observation 1.2.4.** *The following "classical" fields, known to be decidable in $\mathscr{L}_{ring}$, are not suitable (as the desired base field $K$) in helping us generate a counterexample that would provide a negative answer to Question* (1.1.1)*:*

1. *Any finite field;*
2. *Any real closed field;*
3. *Any algebraically closed field;*
4. *The field of p-adic numbers for any prime p.*

*Proof.*

1. As pointed out above, finite extensions of finite fields are themselves just finite fields, which are clearly decidable;
2. By a 1951 result of Alfred Tarski [Tar51], it is known that any real closed field is decidable. Any proper finite extension of a real closed field would be an algebraically closed field, which is also a "classical" field known to be decidable by yet another result of Tarski in the above-mentioned paper [Tar51];
3. Algebraically closed fields do not have any proper finite extensions;
4. That the field of $p$-adic numbers is decidable is a result proven by James Ax and Simon B. Kochen [AK65], and independently, by Yuri L. Ershov [Ers65], in 1965[4].

   Now suppose that $L = \mathbb{Q}_p(\alpha)$ is a finite extension of $\mathbb{Q}_p$, and suppose further that $f(X)$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}_p$. By an application of

[4] Similar to the case we had observed with the decidability of $\mathbb{R}$ in $\mathscr{L}_{\text{ring}}$, the theory of the field of $p$-adic numbers, $\mathbb{Q}_p$, was originally shown to be decidable in an expanded language – in this case, the language of valued fields, $\mathscr{L}_{\text{ring}} \cup \{\mathcal{R}'\}$, where $\mathcal{R}'$ is a unary relation symbol standing for the valuation ring. As before, by restricting our language to $\mathscr{L}_{\text{ring}}$, we could then use the same algorithm to decide whether each $\mathscr{L}_{\text{ring}}$-sentence belongs to $\texttt{Th}(\mathbb{Q}_p)$ or not.

Krasner's Lemma, we can then "approximate" $f(X)$ by another polynomial $g(X)$, and, in fact, choose $g(X) \in \mathbb{Q}[X]$ rather than simply having $g(X) \in \mathbb{Q}_p[X]$ (this can be done essentially because $\mathbb{Q}$ is dense in $\mathbb{Q}_p$) such that $g(X)$ has a root $\beta$, with $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. Now, we have that $\mathbb{Q}_p(\beta)$ is a finite extension of $\mathbb{Q}_p$ obtained by adjoining to $\mathbb{Q}_p$ an element, $\beta$, which is algebraic over $\mathbb{Q}$ (the prime field of $\mathbb{Q}_p$ since the characteristic of $\mathbb{Q}_p$ is zero). Then, by Observation (1.2.2), we have that the decidability of the field $\mathbb{Q}_p$ would "move up" to its finite extension, making finite extensions of the field of $p$-adic numbers decidable as well.

□

Thus far, we have seen instances where finite extensions of decidable fields remain decidable. Furthermore, Observation (1.2.4) highlights the main difficulty in finding a suitable base field which may be used to construct any possible counterexamples that would indicate definitively a negative solution to Question (1.1.1) – the observation highlights the fact that if such a counterexample were to exist, then the corresponding base field would have to be some decidable "non-classical" field. Unfortunately, there are not that many known "non-classical" fields which happen to be decidable.

Are we then inclined towards finding a proof asserting a positive solution to Question (1.1.1)? While those instances which seem to propound an overall positive solution to Question (1.1.1) might provide us with some reasons to pursue looking for a definitive solution in that direction, (though, as in the case with Question (1.1.4), it could very well turn out that the actual solution may oppose "commonly known" examples), we instead make the following observation which might make it possible for us to construct a counterexample to Question (1.1.1):

**Observation 1.2.5.** *A decidable field can become undecidable if the language is modified.*

One obvious way would be to consider the following: Take the field $\mathbb{R}$. This field is known to be decidable in the language of rings, $\mathscr{L}_{\text{ring}}$[5]. However, if we modify the language to include a one-place predicate symbol $\mathscr{N}$, which is interpreted as picking out the natural numbers of $\mathbb{R}$,

$$\text{i.e. for all } x \in \mathbb{R},\ x \in \mathscr{N} \longleftrightarrow x \text{ is a natural number,}$$

then, in this new language, $\mathscr{L} = \mathscr{L}_{\text{ring}} \cup \{\mathscr{N}\}$, the field of real numbers becomes undecidable, for arithmetic of natural numbers (which is known to be undecidable) can be interpreted within this modified language.

A more illuminating example of the above observation would be if we had modified our language to include a constant symbol, $c$, which is to be interpreted as realising an undecidable Dedekind cut instead. Then in the language $\mathscr{L}' = \mathscr{L}_{\text{ring}} \cup \{c\}$, the field of real numbers also becomes undecidable. Indeed, if the field of real numbers were to be decidable in this new language, then one could effectively enumerate the rationals and print them on a list $\mathtt{Q}$[6], and every time an element of $\mathbb{R}$ is printed onto this list (i.e. the element is a rational number), one could check whether this element satisfies the formula

$$\varphi(x) := \exists y \left( (c - x = y^2) \wedge (y \neq 0) \right).$$

If it does, then print the element on a second list, $\mathtt{LC}$; otherwise print the element on a third list, $\mathtt{UC}$. In effect, this procedure takes as its input elements in the list $\mathtt{Q}$ and sorts out those elements onto lists $\mathtt{LC}$ or $\mathtt{UC}$. However, this ensures that the sets

$$\{a \in \mathbb{Q} \mid a < c\} \quad \text{and} \quad \{b \in \mathbb{Q} \mid c < b\}$$

are decidable (membership of these sets can be recursively determined by the above-mentioned procedure), contradicting the fact that $c$ was chosen to be interpreted

[5] Refer to [2].

[6] We aim to point out that while the *set of rational numbers* is itself not definable (or indeed interpretable) within the field of real numbers in $\mathscr{L}_{\text{ring}}$, each rational number *individually* is $\varnothing$-definable within the field in $\mathscr{L}_{\text{ring}}$, and so it is possible for us to effectively enumerate the rationals, by listing each element one at a time, even in this expanded language.

as an element that realises an undecidable Dedekind cut.

Through this inspection, we highlight the fact that in general, if we are able to "talk" about some undecidable subsets of our field within our modified language, then the field would have to be undecidable within this modified language, for otherwise, if the field were decidable, then there has to exist a decision procedure which determines membership of the undecidable subset, which clearly cannot happen. This observation thus provides us with some insights as to how one might be able to construct a desired counterexample – if we are able to "talk" about an undecidable subset within our finite field extension in $\mathscr{L}_{\text{ring}}$, a subset which, in particular, was not expressible in the base field using $\mathscr{L}_{\text{ring}}$, then we can obtain an undecidable finite field extension of a decidable field. We will return to this observation a little later (cf. Chapter 4).

We end the chapter with one final observation:

**Observation 1.2.6.** *Suppose $K$ is a decidable field which admits only finitely many pairwise elementarily inequivalent extensions $L_1, L_2, \ldots, L_k$ of any fixed degree $n > 1$. Then every extension $L_i$ for $i \in \{1, 2, \ldots, k\}$ is decidable.*

*Proof.* Since the $L_i$'s are all pairwise elementarily inequivalent, there exists some $\mathscr{L}_{\text{ring}}$-sentence, $\varphi_i$, which holds in $L_i$ but not in any other $L_j$, whenever $i \neq j$ (simply take the conjunct of those sentences that differentiates $L_i$ from each $L_j$ where $j \in \{1, 2, \ldots, k\} \setminus \{i\}$). Now, suppose we consider the expansion of our ring language to include a predicate, $\mathscr{K}$, which identifies the field $K$. Then the theory of $L_i$ in the expanded language $\mathscr{L} := \mathscr{L}_{\text{ring}} \cup \{\mathscr{K}\}$ can be seen as the theory of the pair $(L_i, K)$. This theory of the pair $(L_i, K)$ is axiomatised by the theory of $K$, the sentence that $L_i$ is a degree $n$-extension of $K$, and the sentence $\varphi_i$. Since $K$ is decidable, this axiomatisation is recursive, and hence the theory of the pair $(L_i, K)$ is decidable as well. Thus, $(L_i, K)$ remains decidable in the reduct (i.e. within the language, $\mathscr{L}_{\text{ring}}$) since the same algorithm used to decide whether a sentence in the

expanded language belongs to the theory of the pair $(L_i, K)$ could be used in the reduct. However, the theory of the pair $(L_i, K)$ in the reduct is precisely the theory of $L_i$ in $\mathscr{L}_{\text{ring}}$ . □

Observation (1.2.6) calls attention to the fact that if one were to find a counterexample to answer Question (1.1.1) negatively, then it is necessary to find a decidable field which admits infinitely many pairwise elementarily inequivalent extensions. As we shall see, by means of an example in the coming chapter, this criterion is insufficient in generating counterexamples.

*As far as I know, only a small minority of mathematicians, even of those with Platonist views, accept the idea that there may be mathematical facts which are true but unknowable.*

— Abraham Robinson [Rob65]

# 2
# Criterion Refined

## Contents


**2.1 Introduction to Some "Non-Classical" Fields . . . . . 12**
2.1.1 Hilbertian Fields . . . . . 12
2.1.2 Pseudo Algebraically Closed Fields . . . . . 13
**2.2 Refining Criterion 2.0.1 . . . . . 22**
2.2.1 Insufficiency of Criterion 2.0.1 . . . . . 23
2.2.2 Strengthening Criterion 2.0.1 . . . . . 26


In the previous chapter, we had pointed out that if a counterexample to answer Question (1.1.1) negatively were to exist, then the base field, $K$, must satisfy the following criterion:

**Criterion 2.0.1.** *$K$ is a decidable field which admits infinitely many pairwise elementarily inequivalent extensions of some fixed degree $n > 1$.*

In this chapter, we refine the above criterion by first highlighting that it is insufficient in producing suitable counterexamples. Towards this end, we introduce the following classes of "non-classical" fields that arise rather naturally in the study of Field Arithmetic.

## 2.1 Introduction to Some "Non-Classical" Fields

### 2.1.1 Hilbertian Fields

We begin with the definition of a Hilbertian field:

**Definition 2.1.1** (A Hilbertian Field)**.** *A field $K$ is said to be Hilbertian if it satisfies (the "generalised") Hilbert's Irreducibility Theorem: i.e. If for every irreducible polynomial*

$$f(X_1, X_2, \ldots, X_r, Y_1, Y_2, \ldots, Y_s)$$

*in $r+s$ variables over $K$, there exists infinitely many $r$-tuples $(t_1, t_2, \ldots, t_r)$ with $t_i \in K$ such that $f(t_1, t_2, \ldots, t_r, Y_1, Y_2, \ldots, Y_s)$ is irreducible in $s$ variables over $K$. In other words, for every irreducible*

$$f(X_1, \ldots, X_r, Y_1, \ldots, Y_s) \in K[X_1, \ldots, X_r, Y_1, \ldots, Y_s],$$

*there exists infinitely many irreducible specialisations.*

As an example, by using the "classical" Hilbert's Irreducibility Theorem (where we take $K = \mathbb{Q}$), we see that the field of rational numbers, $\mathbb{Q}$, is Hilbertian, and more generally, every number field (a finite extension of $\mathbb{Q}$) is Hilbertian. The following proposition helps us identify various Hilbertian fields, the proofs of which could be found in Chapter 4 of Andrzej Schinzel's *Polynomials With Special Regard to Reducibility* [Sch00].

**Proposition 2.1.2.**

*(a) Every finitely generated infinite field is Hilbertian;*

*(b) Every finitely generated transcendental extension of an arbitrary field is Hilbertian;*

*(c) Every finitely generated extension of a Hilbertian field is Hilbertian.*

We also have the following Weissauer's Theorem:

**Theorem 2.1.3** (Weissauer's Theorem)**.** *Let $K$ be a Hilbertian field. Suppose $L$ is a Galois extension of $K$, and $M$ is a proper finite separable extension of $L$. Then the field $M$ is Hilbertian.*

### 2.1.2 Pseudo Algebraically Closed Fields

We now introduce a different class of "non-classical" fields known as pseudo algebraically closed (PAC) fields.

**Definition 2.1.4** (A Pseudo Algebraically Closed Field)**.** *A field $K$ is said to be **pseudo algebraically closed**, or PAC, if every absolutely irreducible affine variety, $V$, defined over $K$ has a $K$-rational point, i.e. a point with all its coordinates in $K$.*

We note that Hilbert's Nullstellensatz asserts that every variety defined over an algebraically closed field, $\widetilde{K}$, has a $\widetilde{K}$-rational point. Hence, every algebraically closed field is indeed PAC. We now state some properties of PAC fields relevant to our endeavour, albeit without proofs – all of which could be found in detail in Chapter 11 of Michael D. Fried and Moshe Jarden's *Field Arithmetic* [FJ08].

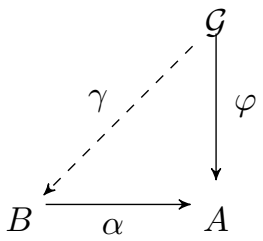
**Proposition 2.1.5** (Some Properties of PAC Fields)**.** *Let $K$ be a PAC field. Then:*

*(a) the space of orderings on $K$, denoted by $\mathfrak{X}(K) := \{P \mid P \text{ is an ordering of } K\}$ is empty;*

*(b) if $L$ is an algebraic extension of $K$, then $L$ is PAC as well. In particular, the property of being PAC "moves up" finite field extensions;*

*(c) $K$ is existentially closed in every regular extension $L$ of $K$. In fact, the converse is also true (i.e. if $K$ is existentially closed in every regular extension, then $K$ is PAC).*

The absolute Galois group of a PAC field – which happens to be a projective profinite group – plays a central role in the study of the theory of such fields. We, therefore, take a slight detour to recall some facts about these structures. A profinite group, $\mathcal{G}$, is said to be **projective** if it satisfies the following universal property: whenever $A$ and $B$ are profinite groups, $\varphi : \mathcal{G} \longrightarrow A$ a continuous homomorphism and $\alpha : B \longrightarrow A$ a continuous epimorphism, there exists a continuous homomorphism $\gamma : \mathcal{G} \longrightarrow B$ such that $\alpha \circ \gamma = \varphi$. In other words, the following diagram commutes:




We say that the pair, $(\varphi : \mathcal{G} \longrightarrow A, \quad \alpha : B \longrightarrow A)$ as above, forms an embedding problem for the profinite group $\mathcal{G}$ – this problem is called **finite** if $B$ itself is finite. The existence of a continuous homomorphism $\gamma$ such that $\alpha \circ \gamma = \varphi$ (as above) is then called a **weak solution** to the prescribed embedding problem. It is thus common to say that a profinite group, $\mathcal{G}$, is projective if and only if every finite embedding problem for $\mathcal{G}$ is weakly solvable. If $\gamma$ is, instead, a continuous epimorphism (i.e. a surjective homomorphism), then it is called a (proper) solution to the prescribed embedding problem. We say that $\mathcal{G}$ is **free of countable rank** if and only if every finite embedding problem for $\mathcal{G}$ is (properly) solvable[1]. It is also worth making explicit the following: whenever $\gamma$ is a proper solution to an embedding problem of the form as described above, the condition $\alpha \circ \gamma = \varphi$ ensures that the continuous homomorphism $\varphi : \mathcal{G} \longrightarrow A$ is, in fact, a continuous epimorphism.

The discussion on profinite groups and, in particular, projective profinite groups is relevant in our investigation of PAC fields since by a result of Lubotzky and van den Dries (cf. Proposition 4.8 of [LD81]), a profinite group, $\mathcal{G}$, is projective if and only if $\mathcal{G}$ is isomorphic to the absolute Galois group of some PAC field. Furthermore, the absolute Galois group of a field $K$ often plays a significant role in determining the decidability of $K$ as it generally encodes a wealth of information about the field $K$. In fact, when the field $K$ is PAC, the decidability of $K$ reduces to checking if

[1] It is worth pointing out that some books refer to "a weak solution" (i.e. when $\gamma$ is a continuous homomorphism) simply as "a solution", and explicitly use the term "proper solution" to refer to instances where $\gamma$ happens to be a continuous epimorphism. In this paper, we would explicitly make use of the phrases "weak solution" (and correspondingly, "weakly solvable"), and "proper solution" (and correspondingly, "properly solvable") to describe situations where $\gamma$ is a continuous homomorphism and where $\gamma$ is a continuous epimorphism respectively to avoid any confusion.

the absolute Galois group of $K$ is decidable and whether the theory that determines the algebraic part of $K$ is decidable. We will make this statement precise in the proceeding theorem. Before we state the theorem though, let us establish some notational conventions: For a PAC field, $K$, of characteristic zero, we denote by

- $\widetilde{K}$ the (separable) algebraic closure of $K$;
- $\mathbf{G}_K := \mathrm{Gal}(\widetilde{K}/K)$ the absolute Galois group of $K$ which is, in fact, a projective profinite group by Theorem 11.6.2 of [FJ08];
- $K^{\mathrm{alg}} := K \cap \widetilde{\mathbb{Q}}$ the algebraic part of $K$, defined as the set of elements of $K$ which are algebraic over its prime subfield, $\mathbb{Q}$;
- $\mathtt{Th}^{\mathrm{alg}}(K)$ the subset of $\mathtt{Th}(K)$ that determines $K^{\mathrm{alg}}$ up to isomorphism, axiomatised by saying which irreducible, monic polynomials in $\mathbb{Z}[X]$ have a zero in $K$ and which ones do not.

From the work of Cherlin, van den Dries and Macintyre [CDM81], we get the following theorem:

**Theorem 2.1.6** (Decidability Criterion I)**.** *Let $K$ be a PAC field. The theory of $K$, denoted $\mathtt{Th}(K)$, is determined by the isomorphism types of the field $K^{alg}$ (which is determined by the set of polynomials in $\mathbb{Z}[X]$ with a root in $K$) and of the restriction map $\mathbf{G}_K \longrightarrow \mathbf{G}_{K^{alg}}$ (considered as morphism in the category of profinite groups).*

While we do not prove the above theorem, we have, in particular, the following proposition from Koenigsmann's [Koe16], which helps us determine whether a PAC field satisfying a certain condition is decidable by isolating the question to simply determining whether the corresponding theory that determines the algebraic part of the PAC field (up to isomorphism) is decidable.

**Proposition 2.1.7** (Decidability Criterion II)**.** *Let $K$ be a countable PAC field of characteristic zero with $\mathbf{G}_K \cong \widehat{F}_\omega$, where $\widehat{F}_\omega$ is the free profinite group on countably many generators. Then $K$ is decidable if and only if $\mathtt{Th}^{alg}(K)$ is decidable.*

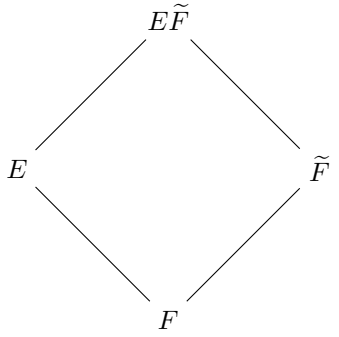
*Proof.*

1. We begin by extending the language of rings, $\mathscr{L}_{\text{ring}}$, by (infinitely) countably many predicate symbols $R_n$ (one for each $n \in \mathbb{N}$) so as to be able to talk about those monic polynomials which have a root in $K^{\text{alg}}$, and those that don't;

2. Let $T_{R,0}$ be the theory of fields of characteristic zero with algebraic part $K^{\text{alg}}$ satisfying the following axiom:

$$R_n(X_0, \ldots, X_{n-1})$$
$$\Longleftrightarrow$$
$$(\exists Z)(Z^n + X_{n-1}Z^{n-1} + \cdots + X_0 = 0) \text{ for each } R_n,\ n \in \mathbb{N};$$

3. Suppose that the fields $F$ and $E$ satisfy $T_{R,0}$, with $F$ a substructure of $E$. In this case, we say that $E$ is a $T_{R,0}$-extension of $F$, i.e. the field extension $E$ over $F$ is an extension of models of $T_{R,0}$. Recall that the field extension $E$ over $F$ is an extension of models of $T_{R,0}$ if and only if $F$ is algebraically closed in $E$. Since we are working with fields of characteristic zero, $E$ is also separable over $F$, and as such $E$ is a regular extension of $F$. Thus, $E$ is linearly disjoint from $\widetilde{F}$ over $F$, and so we have the following diagram, where $E\widetilde{F}$ is the compositum of $E$ and $\widetilde{F}$ (the smallest field containing both $E$ and $\widetilde{F}$):




It follows that $T_{R,0}$ has the amalgamation property;

4. Let $\widetilde{T}_{R,0}$ be a model companion of $T_{R,0}$ whose models are $\omega$-free (i.e. any countable elementary substructure has absolute Galois group $\widehat{F}_\omega$), PAC fields of characteristic zero with algebraic part $K^{\text{alg}}$. Such a model companion exists by Theorem 27.2.3 in [FJ08]. Since $T_{R,0}$ has the amalgamation property, then $\widetilde{T}_{R,0}$ is, in fact, a model completion of $T_{R,0}$;

5. Recall that a model $F$ of $\widetilde{T}_{R,0}$ is said to be $\widetilde{T}_{R,0}$-existentially closed if $F$ is existentially closed in each of its $\widetilde{T}_{R,0}$-extensions. By using Proposition 2.1.5(c) and applying Abraham Robinson's Test for Model Completeness (cf. Lemma 27.1.11 of [FJ08]), we can conclude that $\widetilde{T}_{R,0}$ is model complete. Thus, by Proposition 3.5.19 of [CK12], $\widetilde{T}_{R,0}$ admits quantifier elimination;

6. Since this theory has quantifier elimination, then it is decidable if and only if the atomic formulae are decidable. This happens if and only if we know which polynomials $Z^n + a_{n-1}Z^{n-1} + \cdots + a_0$ have roots in $K^{\text{alg}}$ (i.e. if and only if we are able to decide which sentences of the form $R_n(a_0, \ldots, a_{n-1})$ with $a_i \in \mathbb{Z}$ hold in $K$), which, in turn, is possible if and only if $\mathtt{Th}^{alg}(K)$ is decidable.

□

The above proposition is also particularly helpful in our study of decidability of finite extensions of PAC fields satisfying the conditions stated in that proposition since finite extensions of PAC fields correspond to taking open subgroups of the associated absolute Galois groups, i.e. if $L$ is a finite field extension of a PAC field, $K$, then $\mathbf{G}_L$ is an open subgroup of $\mathbf{G}_K$. Since the profinite analogue of the Nielsen-Schreier theorem holds for open subgroups (cf. Proposition 17.6.2 of [FJ08]), all open subgroups of $\widehat{F}_\omega$ are free and of rank $\omega$, i.e. are themselves all isomorphic to $\widehat{F}_\omega$. Hence, in such a situation, checking the decidability of a finite extension, $L$, of a countable PAC field, $K$, of characteristic zero with $\mathbf{G}_K \cong \widehat{F}_\omega$ boils down to once again checking if the theory that determines the algebraic part of $L$ is decidable, i.e. checking whether $\mathtt{Th}^{alg}(L)$ is decidable.

**Remark 2.1.8.** *While the decidability of PAC fields can be deduced from its absolute Galois group and the decidability of the theory that determines the algebraic part of the field, this recipe is not true in general; for instance, let $\mathbb{F}_p(t)$ be the field of rational functions (in the indeterminate $t$) with coefficients in the finite field with $p$ elements (where we take $p$ to be a prime number greater than 2), and consider the maximal cyclotomic extension of $\mathbb{F}_p(t)$, denoted by $\widetilde{\mathbb{F}}_p(t)$. By Corollary 4.2 (b) of [Har95] (cf. Section 4 of [Jar95], as well as Theorem in [Pop93b]), we know that $\mathbf{G}_{\widetilde{\mathbb{F}}_p(t)} \cong \widehat{F}_\omega$. Furthermore, the algebraic part of $\widetilde{\mathbb{F}}_p(t)$ is simply $\widetilde{\mathbb{F}}_p$ and thus, $\mathtt{Th}^{alg}(\widetilde{\mathbb{F}}_p(t))$ is also decidable. However, being a function field of characteristic $p > 2$, $\widetilde{\mathbb{F}}_p(t)$ is known to be undecidable by a result of Eisenträger and Shlapentokh [ES09].*

As pointed out above, Proposition 2.1.7 differs from Theorem 2.1.6 by informing us that in the event that the absolute Galois group of the PAC field, $K$, is isomorphic to $\widehat{F}_\omega$, one only needs to check if $\mathtt{Th}^{alg}(K)$ is decidable, suggesting that the absolute Galois group of $K$, $\mathbf{G}_K \cong \widehat{F}_\omega$, is, in fact, decidable. This is indeed so, and follows from the following result of Kenkichi Iwasawa:

**Theorem 2.1.9** (cf. Theorem 4 of [Iwa53], Corollary 3.5.10 of [RZ10])**.** *Let $\mathcal{G}$ be a profinite group of rank $\aleph_0$. Then $\mathcal{G}$ is a free profinite group on a countably infinite set converging to 1 (i.e. $\mathcal{G} \cong \widehat{F}_\omega$) if and only if every finite embedding problem for $\mathcal{G}$ has a proper solution.*

By Remarks 23.4.1 and 23.4.2 of [FJ08] the statement "every finite embedding problem over a field, $K$, is properly solvable" is elementary[2], and can be expressed in the language of rings with an additional unary predicate to represent the elements of the field $K$, i.e. in the language $\mathscr{L} = \mathscr{L}_{\text{ring}} \cup \{\mathscr{K}\}$ (cf. the expanded language used in the proof of Observation (1.2.6)). Since Theorem 2.1.9 asserts that the statement "every finite embedding problem over $K$ is properly solvable" completely

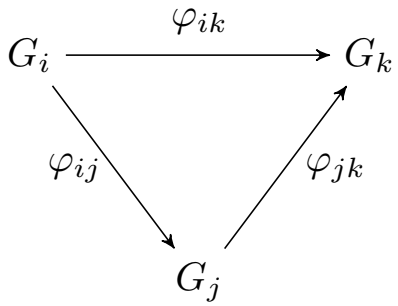
[2] The statement "the embedding problem over a field $K$" is commonly written to express the statement "the embedding problem over the profinite group $\mathcal{G}$" where $\mathcal{G} = \mathbf{G}_K$ corresponds to the absolute Galois group of the field $K$. We will follow this convention and use the former statement whenever the profinite group is obtained as the absolute Galois group of a PAC field $K$, and the latter whenever we are purely discussing about a profinite group which doesn't necessarily arise from any particular field.

axiomatises the theory of $\widehat{F}_\omega$, and the fact that this can be written in a recursive way as suggested by Remarks 23.4.1 and 23.4.2 of [FJ08] allows one to conclude that the theory of $\widehat{F}_\omega$ is decidable in the language $\mathscr{L}$, and hence also in the reduct $\mathscr{L}_{\text{ring}}$.

In our investigation of PAC fields, it is common to encounter absolute Galois groups of such fields which do not necessarily happen to be (isomorphic to) $\widehat{F}_\omega$, and as such, it might be instructive to study profinite groups arising as absolute Galois groups of such fields in a language that is better equipped to handle both its group structure and its topology – after all, profinite groups are abstract groups equipped with a compact, Hausdorff, totally disconnected group topology. We therefore need a language that would be able to take into consideration both the algebraic structure, as well as the topological structure of these groups. This leads us to consider the **language of complete stratified inverse systems**, $\mathscr{L}_{\text{CSIS}}$, as first introduced by Cherlin, van den Dries, and Macintyre in [CDM80a] and [CDM80b], and later developed by Chatzidakis in [Cha84]. This language allows one to study profinite groups by dualizing the problem and studying, instead, a rather simple algebraic system, working with embeddings of complete systems as opposed to continuous epimorphisms of profinite groups. In light of the fact that a profinite group, $\mathcal{G}$, is defined as an inverse limit

$$\mathcal{G} = \varprojlim_{i \in I} G_i$$

of a surjective inverse system $\{G_i, \varphi_{ij}, I\}$ of finite groups, $G_i$ (with each group equipped with the discrete topology), $\mathscr{L}_{\text{CSIS}}$ appears to be a "natural" language to study such profinite groups – here $I = (I, \preccurlyeq)$ denotes a directed partially ordered set (also known as a directed poset) with the finite groups, $G_i$, indexed by $I$, and $\varphi_{ij} : G_i \longrightarrow G_j$ is a continuous group homomorphism, defined whenever $i \succcurlyeq j$ such that the diagrams of the form




commute whenever they are defined, i.e. whenever $i, j, k \in I$ and $i \succcurlyeq j \succcurlyeq k$.

**Definition 2.1.10.** *Let $\mathscr{L}_{CSIS}$ denote the many-sorted language $\{\lessdot, \mathscr{B}, \mathscr{T}\}$ with sorts indexed by the positive integers, with $\lessdot$ and $\mathscr{B}$ being binary relation symbols, and $\mathscr{T}$ being a ternary relation symbol. For a profinite group, $\mathcal{G}$, and a non-empty collection, $\mathcal{N} = \{N \trianglelefteq_{open} \mathcal{G} \mid \mathcal{G}/N \text{ is finite}\}$, of open normal subgroups[3] of $\mathcal{G}$ such that $\mathcal{G}/N$ is finite[4], let $\mathtt{S}(\mathcal{G})$ be the following $\mathscr{L}_{CSIS}$ structure: The universe of $\mathtt{S}(\mathcal{G})$ is $\bigcup\limits_{N \in \mathcal{N}}^{\cdot} \mathcal{G}/N$. Furthermore,*

- *$gN$ is of sort $n$ if and only if $[\mathcal{G} : N] \leq n$;*
- *$gN_1 \lessdot hN_2$ if and only if $N_1 \subseteq N_2$;*
- *$\mathscr{B}(gN_1, hN_2)$ if and only if $gN_1 \lessdot hN_2$ and $gN_2 = hN_2$;*
- *$\mathscr{T}(g_1N_1, g_2N_2, g_3N_3)$ if and only if $N_1 = N_2 = N_3$ and $g_1g_2N_1 = g_3N_1$.*

*$\mathtt{S}(\mathcal{G})$ is called the **complete inverse system** of $\mathcal{G}$. Note that, $gN \in \mathtt{S}(\mathcal{G})$ is a coset of $N$, where $N$ is, in turn, an open normal subgroup of $\mathcal{G}$.*

[3] As profinite groups are compact topological spaces, an open subgroup of a profinite group, $\mathcal{G}$, necessarily has finite index. On the other hand, if $\mathcal{G}$ is a topologically finitely generated profinite group (i.e. $\mathcal{G}$ contains a dense finitely generated subgroup), then by a result of Nikolay Nikolov and Dan Segal (cf. Theorem 1.1 of [NS03]) every subgroup of finite index in $\mathcal{G}$ is open.

[4] We say that $\mathcal{N}$ is **filtered from below** if $\mathcal{N}$ satisfies the following condition:

$$\text{whenever } N_1, N_2 \in \mathcal{N}, \text{ there exists } N \in \mathcal{N} \text{ such that } N \leq N_1 \cap N_2.$$

Note that if $\mathcal{N}$ is as described above, then it is indeed (non-empty and) filtered from below. Note further that the finite groups, $G_i$, that we referred to earlier in our definition of profinite groups can then be seen as corresponding to the finite groups, $\mathcal{G}/N$, for $N \in \mathcal{N}$ with these finite groups inheriting the profinite topology.

**Remark 2.1.11.**

- *Note that $\preccurlyeq$ is a transitive and reflexive relation, that induces an equivalence relation $x \sim y$ if and only if $x \preccurlyeq y$ and $y \preccurlyeq x$. If we denote the corresponding class of $x$ by $[x]$, then we see that $gN_1 \sim hN_2$ if and only if $N_1 = N_2$ and $[gN_1] = [N_1] = \mathcal{G}/N_1$. This, in turn, induces a partial ordering on the set $\mathtt{S}(\mathcal{G})/\sim$ of equivalence classes;*

- *The ternary relation, $\mathscr{T}$, defines on every equivalence class, a group operation;*

- *If $x \preccurlyeq y$, then the binary relation, $\mathscr{B}$, defines a group epimorphism*

$$\pi_{xy} : [x] \longrightarrow [y].$$

  *If $gN_1 \preccurlyeq hN_2$, then the map*

$$\pi_{N_1N_2} : \mathcal{G}/N_1 \longrightarrow \mathcal{G}/N_2$$

  *is the canonical projection;*

- *The inverse system is called complete as it contains all continuous quotients of $\mathcal{G}$.*

- *The manuscripts of Cherlin, van den Dries, and Macintyre (cf. [CDM80a]; [CDM80b]) show, in particular, that for a PAC field $K$ with absolute Galois group $\mathbf{G}_K$, the theory of the system $\mathtt{S}(\mathbf{G}_K)$ is interpretable in $\mathtt{Th}(K)$ (using $\mathscr{L}_{ring}$). Hence, if $\mathtt{S}(\mathbf{G}_K)$ is undecidable in $\mathscr{L}_{CSIS}$, then correspondingly, $\mathtt{Th}(K)$ is undecidable in $\mathscr{L}_{ring}$.*

We point out that, henceforth, whenever we talk about decidability of a profinite group $\mathcal{G}$, we are, in fact, referring to the decidability of the corresponding complete inverse system of $\mathcal{G}$, $\mathtt{S}(\mathcal{G})$, in the language $\mathscr{L}_{\mathrm{CSIS}}$. Recall that we say that a profinite group, $\mathcal{G}$, is **small** if for every $n \in \mathbb{N}$, there are only finitely many open subgroups $H \leq \mathcal{G}$ of index $n$. Now note that Observation (1.2.6), in particular, asserts that if $K$ is a decidable field with small absolute Galois group and of finite degree of imperfection, then every finite extension of $K$ is decidable. Thus, if one were to

consider a decidable PAC field, $K$ (in the language $\mathscr{L}_{\text{ring}}$), whose absolute Galois group, $\mathbf{G}_K$, is small and indeed decidable in $\mathscr{L}_{\text{CSIS}}$, by virtue of the last point in Remark 2.1.11, then since every finite extension of $K$ is decidable (in the language $\mathscr{L}_{\text{ring}}$), the corresponding open subgroups of $\mathbf{G}_K$ are also decidable (in the language $\mathscr{L}_{\text{CSIS}}$). Alternatively, examination of the proof of Observation (1.2.6) shows that the exact same argument can be utilised to show directly that if $\mathcal{G}$ is a decidable small profinite group, and $n$ is a positive integer such that the open subgroups, $H$, of index $n$ lie in only finitely many complete elementary classes (and this holds trivially in small profinite groups), then every open subgroup $H$ of $\mathcal{G}$ of index $n$ is decidable.

We point out that through the above discussion, it is easy to see that $\widehat{F}_\omega$ remains decidable in $\mathscr{L}_{\text{CSIS}}$. Now, we say that a PAC field, $K$, is **$\omega$-free** if and only if every finite embedding problem for $\mathbf{G}_K$ is properly solvable, i.e. $\mathbf{G}_K \equiv \widehat{F}_\omega$ (in the language $\mathscr{L}_{\text{CSIS}}$). Note that if, in addition, $K$ is countable, then by Theorem 2.1.9, we have that $\mathbf{G}_K$ is, in fact, actually isomorphic to $\widehat{F}_\omega$[5]. We note that in the proof of Proposition 2.1.7, we only needed that the model companion of $T_{R,0}$ has models that are $\omega$-free. As such, we could "weaken" Proposition 2.1.7 in the following way:

**Corollary 2.1.12.** *Let $K$ be an $\omega$-free PAC field of characteristic zero. Then $K$ is decidable if and only if $\mathtt{Th}^{alg}(K)$ is decidable.*

## 2.2 Refining Criterion 2.0.1

With the above detour, we are now able to show that Criterion 2.0.1, as it stands, would not be sufficient in generating a counterexample to answer Question (1.1.1) negatively.

[5] Indeed, there are uncountable $\omega$-free PAC fields whose absolute Galois groups are not isomorphic to $\widehat{F}_\omega$.

### 2.2.1 Insufficiency of Criterion 2.0.1

In order to show the insufficiency of Criterion 2.0.1, we construct a decidable field, $K$, which admits infinitely many pairwise elementarily inequivalent extensions of some fixed degree $n > 1$, all of which remain decidable.

**Theorem 2.2.1.** *There exists a decidable PAC field $K$ admitting infinitely many pairwise elementarily inequivalent quadratic extensions, all of which are decidable.*

*Proof.* Let $K$ be a countable PAC field of characteristic zero with $\mathbf{G}_K \cong \widehat{F}_\omega$, and algebraic part, $K^{\mathrm{alg}} = K \cap \widetilde{\mathbb{Q}} = \mathbb{Q}$. We first claim that $K$ is decidable. Now, by Decidability Criterion II (Proposition 2.1.7), in order to show that $K$ is decidable, it suffices to show that $\mathtt{Th}^{\mathrm{alg}}(K)$ is decidable. By Step 6 of the proof of Proposition 2.1.7, we know that $\mathtt{Th}^{\mathrm{alg}}(K)$ is decidable if and only if we can determine which polynomials $f(Z) = Z^n + a_{n-1}Z^{n-1} + \cdots + a_0$ where $a_i \in \mathbb{Z}$ have roots in $K^{\mathrm{alg}} = \mathbb{Q}$. By Gauss's Lemma, we know that if a polynomial of the form $f(Z)$ as described above has a root $r$ in $\mathbb{Q}$, then $r$ is in fact an integer factor of $a_0$ (i.e. $r \in \mathbb{Z}$ divides $a_0$). Since $a_0$ can only have finitely many divisors $d_1, d_2, \ldots, d_s$, we can check for each $i \in \{1, 2, \ldots, s\}$ whether $f(d_i) = 0$. If there exists some $i \in \{1, 2, \ldots, s\}$ for which $f(d_i) = 0$, then we can take $r = d_i$ and conclude that the given $f(Z)$ has a root in $K^{\mathrm{alg}} = \mathbb{Q}$. Otherwise, $f(d_i) \neq 0$ for all $i \in \{1, 2, \ldots, s\}$ and so the polynomial $f(Z)$ does not have a root in $K^{\mathrm{alg}} = \mathbb{Q}$. This provides an effective algorithm to determine whether any given monic polynomial with integer coefficients has a root in $K^{\mathrm{alg}}$, and as such, we can conclude that $\mathtt{Th}^{\mathrm{alg}}(K)$ is decidable from whence we get that $K$ is also decidable.

We now claim that $K$ has infinitely many pairwise elementarily inequivalent quadratic extensions. Indeed, let $L_i$ be the quadratic extension of $K$ obtained by adjoining a square root of the $(i+1)^{\mathrm{th}}$ rational prime, i.e. $L_i = K(\sqrt{p_{i+1}})$. Since there are infinitely many rational primes, there are infinitely many such quadratic extensions. That all of these quadratic extensions are pairwise elementarily inequivalent can be seen by considering sentences of the form $\varphi_i := \exists x \ (x^2 - p_{i+1} = 0)$.

For any pair $(i, j)$ with $i \neq j$, we see that $L_i \models \varphi_i$ but $L_j \not\models \varphi_i$, and so $L_i \not\equiv L_j$.

We now aim to show that all these quadratic extensions, $L_i$'s, are themselves decidable. As mentioned above, since the profinite analogue of the Nielsen-Schreier theorem holds for open subgroups, all open subgroups of $\widehat{F}_\omega$ are themselves isomorphic to $\widehat{F}_\omega$. Thus, appealing to Decidability Criterion II (Proposition 2.1.7) once again, we only need to show that the theory that determines the algebraic part, $L_i^{\text{alg}} = L_i \cap \widetilde{\mathbb{Q}} = \mathbb{Q}(\sqrt{p_{i+1}})$, of such $L_i$'s are all decidable. As before, this comes down to determining which polynomials of the form $f(Z) = Z^n + a_{n-1}Z^{n-1} + \cdots + a_0$ where $a_i \in \mathbb{Z}$ have roots in $L_i^{\text{alg}} = \mathbb{Q}(\sqrt{p_{i+1}})$. Note that if a root $\alpha \in \mathbb{Q}(\sqrt{p_{i+1}})$ to $f(Z)$ were to exist, then $\alpha$ would, in particular, be an algebraic integer since $f(Z)$ is a monic polynomial with integer coefficients. Since $L_i^{\text{alg}}$ is a quadratic number field, we know that the ring of integers of $L_i^{\text{alg}}$ is determined by whether $p_{i+1} \equiv 1 \mod 4$ or $p_{i+1} \equiv 2 \text{ or } 3 \mod 4$. In particular, if $\alpha$ belongs in the ring of integers of $L_i^{\text{alg}}$, then

$$\alpha = \begin{cases} \frac{r}{2} + \frac{s}{2}\sqrt{p_{i+1}}, & \text{for} \quad p_{i+1} \equiv 1 \mod 4 \quad \text{with } r, s \in \mathbb{Z}, \quad r \equiv s \mod 2; \\ r + s\sqrt{p_{i+1}}, & \text{for} \quad p_{i+1} \equiv 2 \text{ or } 3 \mod 4 \quad \text{with } r, s \in \mathbb{Z}. \end{cases}$$

We can therefore substitute the corresponding form of $\alpha$ into the monic polynomial $f(Z)$ based on the quadratic number field in question, and by comparing coefficients, determine whether appropriate $r, s \in \mathbb{Z}$ exist by solving simultaneous equations. If such $r$ and $s$ exist, then $f(Z)$ has a root in $L_i^{\text{alg}}$. Otherwise, the polynomial $f(Z)$ has no roots in $L_i^{\text{alg}}$. This allows us to determine whether any given monic polynomial with integer coefficients has a root in $L_i^{\text{alg}}$, and as such, we can conclude that $\texttt{Th}^{\text{alg}}(L_i)$ is decidable from whence we get that $L_i$ is again also decidable. We therefore have that all the $L_i$'s are decidable. □

Would the situation be any different if we had passed the above field, $K$, to a sufficiently saturated elementary extension, $K^*$, instead? Note that $K^*$ would itself be an $\omega$-free PAC field since, based on the exposition from above, the property of being $\omega$-free is elementary, and further, the property of being PAC is elementary – cf. Proposition 11.3.2 of [FJ08]. Hence, the theory of $K^*$ would once again be

determined essentially by its absolute Galois group (which is elementarily equivalent to $\widehat{F}_\omega$) and the theory that determines the algebraic part of $K^*$. It is worth noting that $\mathbf{G}_{K^*}$ is not isomorphic to $\widehat{F}_\omega$ in this instance – the sufficiently saturated extension $K^*$ has uncountably many open subgroups of index $n$. Now, the fact that $K^* \succcurlyeq K$ allows us to conclude that $K^*$ is itself decidable with at least as many different pairwise elementarily inequivalent quadratic extensions as $K$ had. Given that a saturated extension is "element-rich", it is reasonable to ask whether there are any new quadratic extensions in $K^*$ that does not directly correspond to those quadratic extensions $L_i$'s of $K$ as described above – if such new extensions were to arise, then one might speculate that some of these new extensions (and only these new extensions) could give rise to undecidable theories since those quadratic extensions $L_i^*$'s of $K^*$ that corresponds to the quadratic extensions $L_i$'s of $K$ would inevitably be decidable for the same reason that the $L_i$'s are decidable.

While one could always find some non-standard (rational) element, $\alpha \in K^*$ such that $\alpha$ does not belong in the square class of $\mathbb{Q}$ (since $K^*$ is sufficiently saturated), and construct the quadratic extension $L^* = K^*(\sqrt{\alpha})$, we claim that even such a new quadratic extension would remain decidable. We first note that this quadratic extension is indeed a new one as $L^*$ is pairwise elementarily inequivalent to all the other quadratic extensions $L_i^*$'s of $K^*$ which correspond respectively to the quadratic extensions $L_i$'s of $K$ – this follows from the fact that $(L_i^*)^{alg} = \mathbb{Q}(\sqrt{p_{i+1}})$ while $(L^*)^{alg} = \mathbb{Q}$, and the theories that determine these algebraic parts can therefore be distinguished (so this is indeed a new quadratic extension that arises only in a sufficiently saturated extension of $K$).

Further, notice that since $K^*$ is an $\omega$-free PAC field of characteristic zero, it is, in fact, Hilbertian – a result of Moshe Jarden attributed to Peter Roquette (cf. Theorem 3.1 of [Jar80]). By Proposition 2.1.2 (c) and Proposition 2.1.5 (b), $L^*$ is also Hilbertian PAC of characteristic zero. By Theorem A of [FV92], we then have that every finite embedding problem over $L^*$ is properly solvable, i.e.

$\mathbf{G}_{L^*} \equiv \widehat{F}_\omega$ as well. Combining the facts that $\mathbf{G}_{L^*} \equiv \widehat{F}_\omega$ and $(L^*)^{alg} = \mathbb{Q}$ tells us, via Corollary 2.1.12, that $L^*$ is also decidable. It is worth noting that since, for a PAC field, the data about its absolute Galois group and the theory that determines the algebraic part of the field fully characterise theory of the PAC field, we have, in this case, that $L^* \equiv K^*$.

Notice, furthermore, that if we take another non-standard (rational) element, $\beta \in K^*$ where $\beta$ also does not belong in the square class of $\mathbb{Q}$, with $\beta$ being distinct from $\alpha$, we would essentially get a quadratic extension, $K^*(\sqrt{\beta})$, that is elementarily equivalent to $L^* = K^*(\sqrt{\alpha})$, since there is no first-order way of distinguishing $\alpha$ from $\beta$ – in both instances, by the exposition above, we have that

$$(K^*(\sqrt{\alpha}))^{alg} = (K^*(\sqrt{\beta}))^{alg} = \mathbb{Q},$$

and the respectively absolute Galois groups are related in the following way:

$$\mathbf{G}_{K^*(\sqrt{\alpha})} \equiv \mathbf{G}_{K^*(\sqrt{\beta})} \equiv \widehat{F}_\omega.$$

Indeed, it is the case that the theory of $L^*$ consists of all the sentences that are true in almost all of the $L_i^*$'s. This highlights that one would not be able to extend this process by taking further saturated extensions, $K^{**}$, of $K^*$, to get new quadratic extensions that are elementarily inequivalent to any of those of $K^*$ as previously described – we get at most one new quadratic extension that is pairwise elementarily inequivalent to the others that correspond with quadratic extensions of the unsaturated base field, $K$, and moving to further saturated extensions of of $K$ would not provide us with anything new.

### 2.2.2 Strengthening Criterion 2.0.1

The above PAC field not only highlights the inadequacy of Criterion 2.0.1, but the preceding analysis also provides a glimpse into how one might strengthen Criterion 2.0.1 so as to guarantee an undecidable finite extension. As with the example above, if we had started with a base field, $K$, that admits infinitely

many pairwise elementarily inequivalent quadratic extensions, then by taking a sufficiently saturated extension $K^*$ of $K$, it may happen that $K^*$ admits at most one more (non-standard) quadratic extension that is itself also pairwise elementarily inequivalent to the infinitely many other quadratic extensions that correspond to those of $K$. In such situations, $K$ (and indeed, any saturated extension of $K$) has only countably many pairwise elementarily inequivalent quadratic extensions, and this does not, prima facie, allow us to make any undecidability claims. In fact, in the particular example above, it happened to be the case that all the quadratic extensions obtained were themselves decidable. If we had, instead, begun with some field (or a sufficiently saturated extension of that field) which admits *uncountably* many pairwise elementarily inequivalent extensions of a fixed degree $n > 1$, then a simple counting argument shows that most of the degree $n$-extensions would have to be undecidable since there can only be at most countably many decidable theories (as there are at most only countably many different algorithms). It is worth pointing out that if $K$ is a field which has a saturated extension, $K^* \succcurlyeq K$, that admits uncountably many pairwise elementarily inequivalent extensions, then it is possible to identify one such undecidable finite extension (say $L^*$) and "move" only to a sufficiently saturated extension $K^{**}$ of $K$ with

$$K \preccurlyeq K^{**} \preccurlyeq K^*$$

in which this particular finite extension is realised, i.e. one does not have to move to a saturated extension which realises *all* the uncountably many pairwise elementarily inequivalent extensions, but only up to an adequately saturated extension which realises one of those undecidable extensions – note that this particular saturated extension may itself only admit $\aleph_0$-many pairwise elementarily inequivalent extensions.

In order to identify fields which (perhaps in a sufficiently saturated extension) have the potential of admitting uncountably many pairwise elementarily inequivalent extensions, we first begin by recalling the notion of Boolean independence. A subset

$X$ of a Boolean algebra $A$ is **independent** if $X$ freely generates the subalgebra of $A$ which it generates. Within our context, the relevant Boolean algebra to consider would be the Lindenbaum-Tarski algebra algebra, and so we say that a set $\Upsilon = \{\varphi_i \mid 1 \leq i \leq k\} \subseteq \mathtt{Sent}_{\mathscr{L}_{\text{ring}}}$ of $\mathscr{L}_{\text{ring}}$-sentences is Boolean independent if $\bigwedge_{i=1}^{k} \psi_i$ is not a contradiction where $\psi_i$ is either $\varphi_i$ or $\neg\varphi_i$. Alternatively, we can say that the set $\{\psi_i \mid 1 \leq i \leq k\}$ is consistent. Notice that since each $\psi_i$ is either $\varphi_i$ or $\neg\varphi_i$, there are a total of $2^k$ many different consistent sets.

Now suppose we have a decidable field $K$ which admits infinitely many extensions $L_\alpha$'s of a certain fixed degree $m > 1$. Suppose further that there exists a Boolean independent set $\Upsilon = \{\varphi_i \mid i < \omega\}$ of $\mathscr{L}_{\text{ring}}$-sentences such that for any $\varphi_i \in \Upsilon$ and any infinite collection of $L_\alpha$'s, $\varphi_i$ is true in infinitely many of those $L_\alpha$'s and false in infinitely many other of those $L_\alpha$'s. This allows us to sequentially, for each $i$, partition any given infinite collection of degree $m$-extensions of $K$ into two further infinite collections of $m$-extensions of $K$ – one in which $\varphi_i$ is true and the other in which $\neg\varphi_i$ is true. So if we denote by $\Delta$ the infinite collection of degree $m$-extensions of $K$, then the sentence $\varphi_1$ partitions $\Delta$ into two infinite sets $\Delta_{\varphi_1}$ and $\Delta_{\neg\varphi_1}$ such that for every $L_\alpha \in \Delta_{\varphi_1}$, we have that $L_\alpha \models \varphi_1$ and for every $L_\alpha \in \Delta_{\neg\varphi_1}$, we have that $L_\alpha \not\models \varphi_1$. We can then partition $\Delta_{\varphi_1}$ into further infinite collections $\Delta_{\varphi_1,\varphi_2}$ and $\Delta_{\varphi_1,\neg\varphi_2}$ based on whether $L_\alpha \in \Delta_{\varphi_1}$ models $\varphi_2$ or $\neg\varphi_2$, and similarly for $\Delta_{\neg\varphi_1}$. Continuing this process allows us to see that we would eventually get $2^{\aleph_0}$ many different partitions of $\Delta$, and by virtue of the fact that $\Upsilon$ is a Boolean independent set, we would get $2^{\aleph_0}$ many different consistent theories. Hence, we see that within a sufficiently saturated extension $K^*$ of $K$ one could realise all of the $2^{\aleph_0}$ many theories, i.e. $K^*$ would be a decidable field having uncountably many finite extensions of degree $m$ which are all pairwise elementarily inequivalent. A simple Cantor-like counting argument would indicate that most of these extensions would have to be undecidable, thereby providing a negative answer to Question (1.1.1).

In order to be able to express the above-mentioned idea of partitioning the collection of degree $m$-extensions of a decidable field $K$, let us introduce the following terminology: we say that a Boolean independent set $\Upsilon = \{\varphi_i \mid 1 \leq i \leq k\}$ is **realisable** in degree $m$-extensions of $K$ if every set of the form $\{\psi_i \mid 1 \leq i \leq k\}$ where $\psi_i$ is either $\varphi_i$ or $\neg\varphi_i$ is modelled by finite extensions $L_i$'s of $K$ of the fixed degree $m > 1$.We now update Criterion 2.0.1 to the following instead:

**Criterion 2.2.2.** *$K$ is a decidable field and there exists some Boolean independent set, $\Upsilon$, where $|\Upsilon| = \aleph_0$, which is realisable in degree $m$-extensions of $K$ for some $m \in \mathbb{N}_{>1}$.*

It is clear, through the exposition above, that if $K$ is a decidable field that satisfies Criterion 2.2.2 then, $K$ admits a finite extension of a certain fixed degree $m$ that is undecidable, thereby providing a negative answer to Question (1.1.1). It is worth noting that if $K$ satisfies Criterion 2.2.2, then, in particular, $K$ satisfies Criterion 2.0.1. In this way, Criterion 2.2.2 can be viewed as a "strengthening" of Criterion 2.0.1. In the coming chapter, we study a certain elementary class $\mathfrak{C}$ of decidable fields, first introduced by Ershov, and show that for this class of fields, one can find a reasonable choice of a Boolean independent set $\Upsilon$ of cardinality $\aleph_0$ that is realisable in quadratic extensions of $K$ for some $K \in \mathfrak{C}$. The fields in this class are therefore ideal in allowing us to show that there are indeed decidable fields which admit finite extensions that happen to be undecidable, thereby answering Question (1.1.1) negatively.

*Alles Gescheite ist schon gedacht worden.*
*Man muss nur versuchen, es noch einmal zu denken.*

*All intelligent thoughts have already been thought;*
*what is necessary is only to try to think them again.*

— Johann Wolfgang von Goethe [Goe29]

# 3

# Ershov's Wonderful Extensions of $\mathbb{Q}$

## Contents


**3.1 Introduction to Valued and Multi-Valued Fields . . . . 32**
**3.2 Wonderful Extensions of $\mathbb{Q}$ . . . . . 57**
3.2.1 A Sketch of the Existence of Wonderful Extensions of $\mathbb{Q}$ 58
3.2.2 A Sketch of the Decidability of Wonderful Extensions of $\mathbb{Q}$ 77
**3.3 The Undecidability of Finite Extensions of Wonderful Extensions of $\mathbb{Q}$ . . . . . 89**


In this chapter, we introduce the wonderful extensions of $\mathbb{Q}$ (also sometimes referred to as $W^+$-extensions of $\mathbb{Q}$), and a slightly "weaker" variant of such fields called the $W$-extensions of $\mathbb{Q}$. These are classes of multi-valued fields first discovered and extensively studied by Yuri Ershov in the late 1990's and early 2000's. The existence of such fields and their decidability are highly non-trivial results established by Ershov over a series of articles and an encyclopedic monograph (cf. [Ers00]; [Ers01a]; [Ers01b]; [Ers02a]; [Ers02b]; [Ers02c]). Rather than undertaking the odious task of providing a full treatise of the subject, we aim to instead provide a brief sketch of the main beats involved in proving the existence and the decidability of such extensions, referring back to the above-mentioned monograph and papers for in-depth proofs whenever necessary. Before we introduce these classes of fields,

however, we take yet another slight detour in recalling some relevant results from Valued Fields, and introduce some relevant notions in the study of multi-valued fields.

## 3.1 Introduction to Valued and Multi-Valued Fields

**Definition 3.1.1** (Valuation Ring)**.** *A subring $R$ of a field $K$ is called a* ***valuation ring*** *of $K$ if for any $a \in K \setminus \{0\}$, $a \in R$ or $a^{-1} \in R$.*

If $R$ is a valuation ring of a field $K$, then we call $K$ the quotient field of $R$. A domain, $R$, is called a valuation ring if $R$ is a valuation ring of its **quotient field**, denoted by $q(R)$. We make the following observations regarding valuation rings:

**Observation 3.1.2** (Properties of Valuation Rings)**.**

1. *If $R$ is a valuation ring with quotient field $K$, and $R'$ is a ring such that*

$$R \subseteq R' \subseteq K,$$

*then $R'$ is also a valuation ring of $K$, i.e. every intermediate ring is also a valuation ring of $K$;*

2. *If $\mathfrak{p}$ is a prime ideal of a valuation ring $R$, then $\overline{R} = R/\mathfrak{p}$ is a valuation ring;*

3. *If $R$ is a valuation ring, then for any two elements $a, b \in R$, either $a \mid b$ or $b \mid a$ holds. Consequently, the ideals of $R$ are totally ordered by inclusion;*

4. *Every valuation ring has a unique maximal ideal, i.e. every valuation ring is a local ring.*

*Proof.*

1. This follows immediately from the definition of valuation rings;

2. Let $\overline{K} = q(\overline{R})$, and suppose $\overline{a} \in \overline{K} \setminus \{0\}$ be such that $\overline{a} = \overline{b} \cdot \overline{c}^{-1}$ for some $\overline{b}, \overline{c} \in \overline{R} \setminus \{0\}$. We aim to show that either $\overline{a}$ or $\overline{a}^{-1}$ is in $\overline{R}$. Let $b, c \in R$ such that $\overline{b} = b + \mathfrak{p}$ and $\overline{c} = c + \mathfrak{p}$. Since $R$ is a valuation ring, either $b \cdot c^{-1} \in R$ or $(b \cdot c^{-1})^{-1} = c \cdot b^{-1} \in R$. If $b \cdot c^{-1} \in R$, then $\overline{b \cdot c^{-1}} = b \cdot c^{-1} + \mathfrak{p} = \overline{b} \cdot \overline{c}^{-1} = \overline{a} \in \overline{R}$. Otherwise, a similar working shows that $\overline{a}^{-1} \in \overline{R}$;

3. Let $K = q(R)$ be the quotient field of $R$. Suppose that $a \nmid b$. Then for all $r \in R$, $b \neq a \cdot r$, i.e. $b \cdot a^{-1} \notin R$. Since $R$ is a valuation ring, $(b \cdot a^{-1})^{-1} = a \cdot b^{-1} \in R$, i.e. there exists some $s \in R$ such that $a \cdot b^{-1} = s$. Thus, $b \mid a$. This, in particular, shows that the principal ideals $(a)_R$ and $(b)_R$ of $R$ generated by the elements $a$ and $b$ respectively are ordered by inclusion. Indeed, if $a \mid b$, then $b \in (a)_R$ and so $(b)_R \subseteq (a)_R$. Now suppose that $I, J$ are ideals of $R$ and suppose that $I \not\subseteq J$. Then there exists some $i \in I \setminus J$. Now, since $I \not\subseteq J$, for all $j \in J$, $j \nmid i$. Thus, we must have that $i \mid j$ as previously argued. Thus, we have that $J \subseteq (i)_R \subseteq I$;

4. Any ring with identity possesses at least one maximal ideal, and by part (3), since the ideals of a valuation ring $R$ are ordered by inclusion, there can be at most one maximal ideal.

□

Let $R$ be a valuation ring, and $K = q(R)$. We denote the maximal ideal of $R$ by $\mathfrak{m}_R$. Note that since $R$ is a local ring, $R \setminus \mathfrak{m}_R$ is the multiplicative group $U(R)$ of invertible elements (or units) of the ring $R$. The quotient field $R/\mathfrak{m}_R$ is called the residue field of $R$, denoted $K_R$. Note further that for any $a \in q(R) \setminus \{0\}$ we have that $a \notin R$ if and only if $a^{-1} \in \mathfrak{m}_R$. Indeed, if $a \notin R$, then $a^{-1} \in R$ (and, in fact, $a^{-1}$ is not a unit). Thus, $(a^{-1})_R \neq R$. Consequently, $(a^{-1})_R$ is a proper ideal of $R$, and so $(a^{-1}) \subseteq \mathfrak{m}_R$. We then have that $a^{-1} \in \mathfrak{m}_R$. Conversely, suppose $a^{-1} \in \mathfrak{m}_R$. Assume to the contrary that $a \in R$. Then, surely $1 = a^{-1} \cdot a \in \mathfrak{m}_R$, contradicting the fact that a maximal ideal of $R$ is, by definition, a proper ideal.

When dealing with a family of valuation rings of a field, the following proposition helps us to identify when the intersection of these valuation rings is itself a valuation ring.

**Proposition 3.1.3.** *Let $I$ be some index and suppose $W = \{R_i \mid i \in I\}$ is a family of valuation rings of a field $K$. Suppose further that for any $a, b \in I$, there exists a $c \in I$ such that $R_c \subseteq R_a \cap R_b$. Then the ring $R = \bigcap_{i \in I} R_i$ is a valuation ring of $K$.*

*Proof.* Suppose to the contrary that $R$ is not a valuation ring. Then there exists some $k \in K \setminus \{0\}$ such that neither $k$ nor $k^{-1}$ belong to $R$. Since $R = \bigcap_{i \in I} R_i$, then there exists some $a, b \in I$ such that $k \notin R_a$ and $k^{-1} \notin R_b$. Since there exists some $c \in I$ such that $R_c \subseteq R_a \cap R_b$ by the assumption, we have that $k, k^{-1} \notin R_c$. However, $R_c \in W$, and so is, in particular, a valuation ring of $K$, and so for any $k \in K$, either $k \in R_c$ or $k^{-1} \in R_c$ must hold. This gives rise to a contradiction as required. □

We can further associate, to the valuation ring $R$ of a field $K$, an additional derivative structure known as the (linearly ordered) value group, $\Gamma_R$, which is the quotient of the multiplicative group of the field $K$ (i.e. the group of non-zero elements of $K$) by the multiplicative group of the units of $R$,

$$\text{i.e.} \quad \Gamma_R := (K \setminus \{0\})/U(R).$$

Note that the linear order on $\Gamma_R$ is defined by the cone of non-negative elements $(R \setminus \{0\})/U(R)$. Note further that by taking quotients of the multiplicative group of the field $K$, we have essentially excluded the element $0 \in K$ from consideration. As such, for convenience, it is customary to extend $\Gamma_R$ to a linearly ordered semigroup, $\Gamma_R \cup \{\infty\}$, which would then allow us to consider the whole of $K$. Note that the symbol $\infty$ denotes an element that is not in the value group $\Gamma_R$, and is not ascribed any meaning other than those prescribed by the following rules:

- $\infty \geq \alpha$ for all $\alpha \in \Gamma_R$; and
- $\alpha + \infty = \infty + \alpha = \infty$ for all $\alpha \in \Gamma_R$.

The above rules thereby allows us to extend the ordering and the group law on $\Gamma_R$ to the whole of $\Gamma_R \cup \{\infty\}$.

**Definition 3.1.4** (Valued Field)**.** *Suppose $R$ is a valuation ring and $K = q(R)$ be the corresponding quotient field of $R$. The **valuation**, $\upsilon_R$, of the field $K$ determined by the valuation ring $R$ is a map*

$$\upsilon_R : K \to \Gamma_R \cup \{\infty\}$$

*from $K$ to the ordered abelian semigroup, $\Gamma_R \cup \{\infty\}$, such that the following conditions hold:*

1. $v_R(x) = \infty$ *if and only if* $x = 0$;
2. $v_R(x \cdot y) = v_R(x) + v_R(y)$;
3. $v_R(x + y) \geq \min\{v_R(x), v_R(y)\}$, *with equality holding if* $v_R(x) \neq v_R(y)$.

*For any $a \in K$, $v_R(a)$ is called the* ***value of the element*** *$a$. The field $K$, together with the valuation $v_R$, is called a* ***valued field****, denoted as the pair $\langle K, v_R \rangle$.*

Note that we will always assume that the valuation is surjective. The valuations determined by valuation rings are valuations of a field $K$, and it turns out that there are no other valuations besides those arising from these – if $R$ is a valuation ring, then

$$R = \{a \in K \mid v_R(a) \geq 0\}$$

and conversely, if we have a valuation $v$ of a valued field $K$, then the set $\{a \in K \mid v(a) \geq 0\}$ forms a valuation ring of $K$. Note that the corresponding maximal ideal, $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$. If the valuation, $v_R$, is given, then we sometimes also denote the residue field $K_R = R/\mathfrak{m}_R$ as $K_{v_R}$.

**Remark 3.1.5.** *Given how a valuation of a field corresponds to some valuation ring of the field, it is also common to call the pair $\langle K, R \rangle$ a valued field, where $R$ is a valuation ring of the field $K$ without having to explicitly represent the valuation as was the case in Definition* 3.1.4.

A prominent example of a valued field that is relevant especially in our discourse is the pair $\langle K, v \rangle$ where $K = \mathbb{Q}$ and $v = v_p$ is the so-called $p$-adic valuation: For any $x \in \mathbb{Q} \setminus \{0\}$, we can write $x = \frac{a}{b} \cdot p^n$ with $a, b, n \in \mathbb{Z}$ and $\gcd(a, b) = 1$ such that $p \nmid a$. By setting $v_p(x) = n$, we give a valuation on $\mathbb{Q}$ known as the $p$-adic valuation. In this instance,

- the valuation ring is $R_p = \mathbb{Z}_{(p)} = \{\frac{x}{y} \mid x, y \in \mathbb{Z},\ \gcd(p, y) = 1\} \subseteq \mathbb{Q}$;
- the maximal ideal is $\mathfrak{m}_p = (p)_K$, the principal ideal generated by the prime $p$;

- the residue field is $K_{\upsilon_p} = R_p/\mathfrak{m}_p = \mathbb{Z}_{(p)}/(p)_K \cong \mathbb{F}_p$;
- the value group is $\Gamma_{R_p} = \mathbb{Z}$.

We point out some basic properties of a valuation $\upsilon_R$ which follow mainly as a consequence of the definition of $\upsilon_R$: For $a, b \in K \setminus \{0\} = q(R) \setminus \{0\}$ and $\upsilon_R$ as defined above,

1. $\upsilon_R(1) = 0$;
2. $\upsilon_R(a^{-1}) = -\upsilon_R(a)$;
3. $\upsilon_R(-a) = \upsilon_R(a)$;
4. If $\upsilon_R(a) \leq \upsilon_R(b)$, then the principal ideal of $R$ generated by $a$, $(a)_R$, contains the principal ideal of $R$ generated by $b$, $(b)_R$, i.e. $(a)_R \supseteq (b)_R$;
5. If $f \in R[x]$ and $a, b \in R$, then $\upsilon_R\left(f(a) - f(b)\right) \geq \upsilon_R(a - b)$.

Indeed, the first 3 properties follow immediately from the definition of a valuation, noting further that for any $a \in R \setminus \{0\}$, $\upsilon_R(a) = \upsilon_R(1 \cdot a) = \upsilon_R(1) + \upsilon_R(a)$. From part (1), we can then get part (2) and (3) by noting that $\upsilon_R(1) = \upsilon_R(a \cdot a^{-1})$ and $\upsilon_R(1) = \upsilon_R(-1 \times -1)$. For part (4), notice that since $\upsilon_R(a) \leq \upsilon_R(b)$, we have that $\upsilon_R(b) - \upsilon_R(a) \geq 0$ and so by part (2), $\upsilon_R(b \cdot a^{-1}) \geq 0$. Thus, $b \cdot a^{-1} \in R$, from whence we get that $(b)_R \subseteq (a)_R$. In order to show the validity of part (5), let $f = c_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$. Then

$$f(a) - f(b) = c_n(a^n - b^n) + \cdots + c_1(a - b) = (a - b) \cdot g(a, b)$$

for some $g(x, y) \in R[x, y]$, and so $\upsilon_R(f(a) - f(b)) = \upsilon_R(a - b) + \upsilon_R(g(a, b)) \geq \upsilon_R(a - b)$ since $g(a, b) \in R$ (and so $\upsilon_R(g(a, b)) \geq 0$).

It is particularly noteworthy in our study to ask what happens to the relevant structures (such as the valuation ring, value group, residue field etc.) when we consider extensions of valued fields. In order to tackle this issue, we introduce some well-established terminology. Suppose that $R$ and $R'$ are valuation rings such that

$R \subseteq R'$. We say that $R'$ **dominates** $R$, denoted as $R \sqsubseteq R'$, if $\mathfrak{m}_{R'} \cap R = \mathfrak{m}_R$. This is equivalent to the condition $R' \cap q(R) = R$.

**Definition 3.1.6** (Extension of a Valued Field)**.** *Suppose $\langle K, R\rangle$ and $\langle K', R'\rangle$ are valued fields. We say that $\langle K', R'\rangle$ is an **extension** of $\langle K, R\rangle$, denoted*

$$\langle K, R\rangle \leq \langle K', R'\rangle$$

*if $K$ is a subfield of $K'$ and $R'$ dominates $R$.*

It is easy to see that if $\langle K', R'\rangle$ is an extension of $\langle K, R\rangle$, then the field $K_R = R/\mathfrak{m}_R$ is naturally isomorphic to a subfield of the field $K'_{R'} = R'/\mathfrak{m}_{R'}$, i.e. there exists a natural embedding of the residue field $K_R$ in the residue field $K'_{R'}$. Similarly, the linearly ordered group $\Gamma_R = (K \setminus \{0\})/U(R)$ is naturally isomorphic to a subgroup of the linearly ordered group $\Gamma_{R'} = (K' \setminus \{0\})/U(R')$, i.e. there exists a natural embedding of the value group $\Gamma_R$ in the value group $\Gamma_{R'}$. This, in turn, implies that if $v_R$ and $v_{R'}$ are valuations of $K$ and $K'$ respectively, then $v_R = v_{R'} \restriction K$. A prominent extension in the study of valued fields occurs when both the above-mentioned embeddings are onto.

**Definition 3.1.7** (An Immediate Extension)**.** *Suppose $\langle K, R\rangle \leq \langle K', R'\rangle$ is an extension of valued fields. We say that the extension is **immediate** if the embedding of the residue field $K_R$ in the residue field $K'_{R'}$ and the embedding of the value group $\Gamma_R$ in the value group $\Gamma_{R'}$ is surjective,*

$$\textit{i.e. } (\Gamma_{R'} : \Gamma_R) = [K'_{R'} : K_R] = 1.$$

*We will express this condition by simply saying that $K$ and $K'$ have the same value group and residue field, writing $\Gamma_{R'} = \Gamma_R$ and $K'_{R'} = K_R$.*

The following lemma is a useful characterisation of immediate extensions:

**Lemma 3.1.8.** *Suppose that $\langle K, R\rangle \leq \langle K', R'\rangle$ is an extension of valued fields. The extension is immediate if and only if for every $k' \in K' \setminus \{0\}$ there is a $k \in K$ such that $v_{R'}(k' - k) > v_{R'}(k')$.*

*Proof.* Suppose that $\langle K, R\rangle \leq \langle K', R'\rangle$ is an immediate extension. Let $k' \in K \setminus \{0\}$. Then $v_{R'}(k') \in \Gamma_{R'} = \Gamma_R$, and so there exists some $s \in K$ such that $v_R(s) = v_{R'}(k')$. Note that since $v_R = v_{R'} \restriction K$, there is no harm in saying that $v_{R'}(s) = v_{R'}(k')$. Then, $v_{R'}(k') - v_{R'}(s) = 0$ and so $v_{R'}(k's^{-1}) = 0$, i.e. $k's^{-1} \in U(K')$. We thus have that $\overline{k's^{-1}} \in K'_{R'} = K_R$. So there exists a $t \in K$ such that $\bar{t} = \overline{k's^{-1}}$ from whence we get that $k's^{-1} - t \in \mathfrak{m}_{R'}$. Thus, $v_{R'}(k's^{-1} - t) > 0$ and so,

$$v_{R'}(k' - st) = v_{R'}(k's^{-1} - t) + v_{R'}(s) > v_{R'}(s) = v_{R'}(k')$$

with $k = st \in K$ being the desired element.

Conversely, if $k' \in K'$ and $k \in K$ are such that $v_{R'}(k' - k) > v_{R'}(k')$, then by Condition 3 of Definition 3.1.4, we have that $\Gamma_{R'} \ni v_{R'}(k') = v_{R'}(k) = v_R(k) \in \Gamma_R$. On the other hand, if $k' \in K'$ is such that $v_{R'}(k') = 0$ and $k \in K$ with $v_{R'}(k'-k) > 0$, then $k' - k \in \mathfrak{m}_{R'}$ and hence, $K'_{R'} \ni \overline{k'} = \overline{k} \in K_R$. □

**Lemma 3.1.9.** *Suppose that $\langle K, R\rangle \leq \langle K', R'\rangle$ is an immediate extension, and let $k' \in K' \setminus K$. Let*

$$v_{R'}(k' - K) := \{v_{R'}(k' - k) \mid k \in K\}.$$

*Then*

1. *$v_{R'}(k' - K)$ has no maximal element;*
2. *If $\alpha \in v_{R'}(k'-K)$ and there is a $\beta \in \Gamma_R$ such that $\beta < \alpha$, then $\beta \in v_{R'}(k'-K)$.*

*Proof.*

1. Suppose for a contradiction that $v_{R'}(k' - K)$ has a maximal element, and let $m \in K$ be such that $v_{R'}(k' - m)$ is that maximal element. Since $k' \in K' \setminus K$, we have that $k' - m \in K' \setminus \{0\}$. Thus, by Lemma 3.1.8, there exists some $k \in K$ such that

   $$v_{R'}(k' - m - k) = v_{R'}(k' - (m + k)) > v_{R'}(k' - m).$$

   However, $m + k \in K$ and so $v_{R'}(k' - (m + k)) \in v_{R'}(k' - K)$, contradicting the maximality of $v_{R'}(k' - m)$.

2. Suppose that there exist $k_1, k_2 \in K$ such that $\upsilon_{R'}(k'-k_1) = \alpha$ and $\upsilon_{R'}(k_2) = \beta$ with $\upsilon_{R'}(k_2) < \upsilon_{R'}(k'-k_1)$. Take $k_3 = k_1+k_2 \in K$ and consider $\upsilon_{R'}(k'-k_3) \in \upsilon_{R'}(k'-K)$. Now, we have that

$$\begin{aligned}\upsilon_{R'}(k'-k_3) &= \upsilon_{R'}(k'-k_1-k_2)\\ &= \upsilon_{R'}\left((k'-k_1)-k_2\right)\\ &\geq \min\{\upsilon_{R'}(k'-k_1), \upsilon_{R'}(k_2)\}\\ &= \min\{\upsilon_{R'}(k'-k_1), \upsilon_{R'}(k_2)\}\\ &= \beta\end{aligned}$$

□

**Remark 3.1.10.** *Note that part (2) of the above lemma indicates that $\upsilon_{R'}(k'-K)$ is a convex subgroup of $\Gamma_{R'} = \Gamma_R$. Notice that in particular, if $\Gamma_{R'}$ is (isomorphic to) $\mathbb{Z}$, then since $\mathbb{Z}$ does not have any non-trivial proper convex subgroup, $\upsilon_{R'}(k'-K)$ is itself (isomorphic to) $\mathbb{Z}$ too.*

Among the class of immediate extensions of valued fields are the so-called Henselizations of valued fields. In order to describe what they are, we first look at Henselian valued fields which are of particular interest and of central importance within the subject area.

**Definition 3.1.11** (Henselian Valued Field)**.** *A valuation ring $R$ of a field $K$ is called a **Henselian valuation ring** if for any separable algebraic extension $K'$ of $K$, there is a unique valuation ring of $K'$ dominating $R$. In this case, we say that $\langle K, R\rangle$ is a **Henselian valued field**.*

**Remark 3.1.12.** *If $\langle K, R\rangle$ is a Henselian valued field with valuation $\upsilon_R$, then we also say that $K$ is Henselian with respect to the valuation $\upsilon_R$. In this case, it is clear that $\upsilon_R$ has a unique extension to every algebraic extension of $K$. In particular, $\upsilon_R(\sigma(x)) = \upsilon_R(x)$ for any $x$ in the separable closure of $K$, where $\sigma \in \mathbf{G}_K$. Thus, every algebraic extension of a Henselian field remains Henselian.*

It is worth noting that $R$ being a Henselian ring is equivalent to saying that $R$ is a valuation ring in which the following statement, commonly referred to as Hensel's Lemma, holds:

**Lemma 3.1.13** (Hensel's Lemma)**.** *Suppose $f \in R[x]$ is a monic polynomial whose reduction $\overline{f} \in K_R[x]$ has a simple root $\alpha \in K_R$. Then $\alpha$ can be lifted to a root of $f$ in $R$, i.e. there exists some root of $f$, $\beta$, such that $\overline{\beta} = \alpha$.*

Every valued field $\langle K, R\rangle$ admits a Henselian minimal separable algebraic extension $\langle K^h, R^h\rangle$ known as its **Henselization** (or its Henselian closure). Here, $R^h$ is a Henselian valuation ring which dominates $R$ such that for any Henselian valuation ring $R'$ dominating $R$, there exists an $R$-isomorphic embedding of $R^h$ into $R'$, and $K^h = q(R^h)$. Note that, in particular, $K^h$ is a separable algebraic extension of $K$. For notational convenience, we denote by $\mathbb{H}_R(K)$ the Henselization of $\langle K, R\rangle$, i.e. $\mathbb{H}_R(K) := \langle K^h, R^h\rangle$. If $\langle K', R'\rangle$ is a Henselian extension of $\langle K, R\rangle$, then $\mathbb{H}_R(K)$ can be found inside of $\langle K', R'\rangle$.

Suppose that $\langle K', R'\rangle$ is a valued field and $K$ is a subfield of $K'$. We say that $K$ is **dense** in $\langle K', R'\rangle$ if for any $k' \in K'$ and any $\gamma \in \Gamma_{R'}$, there exists a $k \in K$ such that $\upsilon_{R'}(k' - k) > \gamma$. Note that in this case, by the proof of Lemma 3.1.8, we see that the valued field $\langle K', R'\rangle$ is an immediate extension of $\langle K, R\rangle$ where $R = R' \cap K$. The following simple lemma would come in handy in the later subsection:

**Lemma 3.1.14.** *Suppose $\langle K, R\rangle$ be a valued field with value group $\Gamma_R$ (isomorphic to) $\mathbb{Z}$. Then $\langle K, R\rangle$ is dense in every immediate extension. In particular, it is dense in its henselization $\mathbb{H}_R(K)$.*

*Proof.* By part (2) of Lemma 3.1.9, we have that for any immediate extension $\langle K', R'\rangle$ of $\langle K, R\rangle$ and any $k' \in K' \setminus K$, the set $\upsilon_{R'}(k' - K)$ is a convex subgroup of $\Gamma_R = \Gamma_{R'} \cong \mathbb{Z}$, and so, by Remark 3.1.10, $\upsilon_{R'}(k' - K) \cong \mathbb{Z}$. Thus, any $\gamma \in \Gamma_{R'}$ is of the form $\upsilon_{R'}(k' - s)$ for some $s \in K$. By part (1) of Lemma 3.1.9, the set

$\upsilon_{R'}(k' - K)$ does not have a maximal element, and hence, there is some $k \in K$ such that

$$\upsilon_{R'}(k' - k) > \upsilon_{R'}(k' - s) = \gamma,$$

from whence we have that $\langle K, R\rangle$ is dense in $\langle K', R'\rangle$. □

**Remark 3.1.15.** *We note that the above lemma is a specific instance of a more general result that states that if the value group, $\Gamma_R$, of a valued field, $\langle K, R\rangle$, is an Archimedean group, then $K$ is dense in $\mathbb{H}_R(K)$. For our purposes, however, the above lemma itself is sufficient.*

Given a commutative ring $R$ with identity, and a subset $S \subseteq R$ that is closed under multiplication with $0 \notin S$ and $1 \in S$, the localization of $R$ at $S$ is the ring

$$R_S = S^{-1}R = \left\{ \frac{r}{s} \;\middle|\; r \in R, s \in S \right\}.$$

Throughout this paper, the subset $S$ being considered would be complements of prime ideals, i.e. for some prime ideal $\mathfrak{p}$ of $R$, we take $S = R \setminus \mathfrak{p}$. For notational convenience, we will use $R_\mathfrak{p}$ instead of $R_{R\setminus\mathfrak{p}}$ to refer to this particular ring. This ring is called the **localization** of $R$ at $\mathfrak{p}$.

**Remark 3.1.16.** *Note that $R_\mathfrak{p} = \{\frac{r}{s} \mid r \in R, s \in R \setminus \mathfrak{p}\}$ is, in fact, a local ring with (unique) maximal ideal*

$$\mathfrak{p}_{R\setminus\mathfrak{p}} = \mathfrak{p}R_\mathfrak{p} = \left\{ \frac{r}{s} \;\middle|\; r \in \mathfrak{p}, s \in R \setminus \mathfrak{p} \right\}.$$

*The group of units of $R_\mathfrak{p}$ is given by*

$$U(R_\mathfrak{p}) = \left\{ \frac{r}{s} \in R_\mathfrak{p} \;\middle|\; r \in R \setminus \mathfrak{p} \right\}.$$

*Further, note that $R$ is, in fact, a subset of $R_\mathfrak{p}$ by identifying any $r \in R$ with the fraction $\frac{r}{1} \in R_\mathfrak{p}$.*

**Proposition 3.1.17.** *Let $R$ be a subring of a field $K$, and suppose $M$ is an $R$-module contained in a $K$ vector space $V$. Then, we have that*

$$M = \bigcap_{\mathfrak{m}} M_\mathfrak{m} = \bigcap_{\mathfrak{p}} M_\mathfrak{p},$$

*where $\mathfrak{m}$ ranges over the maximal ideals of $R$, $\mathfrak{p}$ ranges over the prime ideals of $R$, and the intersections take place in $V$.*

*Proof.* From Remark 3.1.16, it is clear that $M \subseteq \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$. Thus, we only need to show the reverse inclusion. Suppose $x \in \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$, and consider the set $\{r \in R \mid rx \in M\}$. It is easy to check that this set forms an $R$-ideal, say $\mathfrak{r}$. Note that $\mathfrak{r}$, however, is not contained in any maximal ideal $\mathfrak{m}$. Indeed, since $x \in \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$, then, in particular, $x \in M_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m}$. Thus, there exists $r, s$ such that

$$x = \frac{r}{s} \qquad r \in M,\ s \in M \setminus \mathfrak{m}.$$

Hence $r = sx \in M$, and so $s \in \mathfrak{r}$. If $\mathfrak{r} \subseteq \mathfrak{m}$, then $s \in \mathfrak{m}$, contradicting that $s \in M \setminus \mathfrak{m}$. It follows that $\mathfrak{r} = R$, from whence we have that since $1 \in \mathfrak{r}$, $x = 1 \cdot x \in M$. This establishes the first equality.

For the second equality, notice that since every prime ideal $\mathfrak{p}$ is contained in some maximal ideal $\mathfrak{m}$, each $M_{\mathfrak{m}} \subseteq M_{\mathfrak{p}}$. Furthermore, every maximal ideal is prime. Hence $\bigcap_{\mathfrak{m}} M_{\mathfrak{m}} = \bigcap_{\mathfrak{p}} M_{\mathfrak{p}}$. □

**Proposition 3.1.18.** *Let $R$ be any domain. Then the integral closure, $R^{ic}$, of $R$ in $q(R)$ is given by*

$$R^{ic} = \bigcap_{R \subseteq V \subseteq q(R)} V,$$

*where $V$ are all the valuation rings of $q(R)$ containing $R$.*

*Proof.* We first note that any valuation ring is integrally closed. Since the intersection of integrally closed domains is integrally closed, and since $R \subseteq \bigcap_{R \subseteq V \subseteq q(R)} V$, we have that $R^{ic} \subseteq \bigcap_{R \subseteq V \subseteq q(R)} V$. For the reverse inclusion, let $x \in \bigcap_{R \subseteq V \subseteq q(R)} V$. We need to show that $x$ is integral over $R$. Suppose to the contrary, $x$ is not integral. Let $x = y^{-1}$. Note that if $y^{-1} \notin R^{ic}$, then surely $y^{-1} \notin R[y]$. Since $y$ is not a unit in the ring $R[y]$, the ideal generated by $y$ in the ring $R[y]$ is not the whole of $R[y]$. Hence there is a maximal ideal $\mathfrak{m}$ containing $(y)_{R[y]}$ and so there exists some valuation domain $V$ containing $R[y]$ with $(y)_V \neq V$. However, this contradicts the fact hat $x = y^{-1} \in V$. Thus, $x$ is integral from whence we conclude that $R^{ic} = \bigcap_{R \subseteq V \subseteq q(R)} V$. □

Recall that if $I$ and $J$ are fractional ideals of a noetherian domain $R$ with $K = q(R)$, we can perform the following arithmetic operations:

- Addition: $I + J := \{i + j \mid i \in I, j \in J\}$;
- Multiplication: $I \cdot J = IJ$ which is the set generated by $\{ij \mid i \in I, j \in J\}$;
- Quotient: $(I : J) := \{x \in K \mid xJ \subseteq I\}$.

These operations give rise to further fractional ideals. A fractional ideal $I$ of $R$ is **invertible** if there exists some fractional ideal $J$ such that $IJ = R$. We point out that if $I$ is a fractional ideal of $R$, then $I$ is invertible if and only if $I(R : I) = R$. Indeed, note that if inverses were to exist, then they would have to be unique since if we were to suppose that $I$ is an invertible ideal with $J$ and $J'$ being the inverses of $I$, then since $IJ = R = IJ'$, we have that $J = JR = JIJ' = RJ' = J'$. We thus, just need to show that the inverse of $I$ is $(R : I)$. Suppose $I$ is invertible such that $IJ = R$. Then $jI \subseteq R$ for all $j \in J$, and so $J \subseteq (R : I)$. Now, $R = IJ \subseteq I(R : I) \subseteq R$ which forces an equality throughout.

**Lemma 3.1.19.** *If $R$ is a domain that admits only finitely many maximal ideals, then every invertible ideal is, in fact, principal.*

*Proof.* Indeed, suppose $R$ admits only $n < \omega$ many maximal ideals, say $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$, and suppose $I$ is some invertible ideal of $R$. Since $I(R : I) = R$, there exist $a_i \in I$ and $b_i \in (R : I)$ such that $a_i b_i \notin \mathfrak{m}_i$. By the Chinese Remainder Theorem, we then have $c_i \in R$ such that $c_i \notin \mathfrak{m}_i$ and $c_i \in \bigcap_{j \neq i} \mathfrak{m}_j$. Now consider $d = \sum_{i=1}^{n} c_i b_i$. It is clear that $dI \subseteq R$ is an ideal of $R$ and not contained in any maximal ideals since $da_i \notin \mathfrak{m}_i$. Hence, $dI = R$ and so $I = d^{-1}R = (d^{-1})_R$ is the ideal generated by $d^{-1}$ and thus is principal. □

The following lemma shows that the arithmetic operations as described above respect localization:

**Lemma 3.1.20.** *Suppose $I$ and $J$ are fractional ideals of $R$, $K = q(R)$, and let $\mathfrak{p}$ be a prime ideal of $R$. Then $I_\mathfrak{p}$ and $J_\mathfrak{p}$ are fractional ideals of $R_\mathfrak{p}$. Furthermore,*

$$(I+J)_\mathfrak{p} = I_\mathfrak{p} + J_\mathfrak{p} \quad (IJ)_\mathfrak{p} = I_\mathfrak{p} J_\mathfrak{p} \quad (I:J)_\mathfrak{p} = (I_\mathfrak{p} : J_\mathfrak{p})$$

*are all fractional ideals of $R_\mathfrak{p}$.*

*Proof.* Note that $I_\mathfrak{p} = IR_\mathfrak{p}$ is a finitely generated $R_\mathfrak{p}$ module, and is therefore (by definition) a fractional ideal of $R_\mathfrak{p}$. For the same reason, $J_\mathfrak{p}$ is also a fractional ideal of $R_\mathfrak{p}$. Now, we have

$$(I+J)_\mathfrak{p} = (I+J)R_\mathfrak{p} = IR_\mathfrak{p} + JR_\mathfrak{p} = I_\mathfrak{p} + J_\mathfrak{p}$$

and

$$(IJ)_\mathfrak{p} = (IJ)R_\mathfrak{p} = IR_\mathfrak{p} JR_\mathfrak{p} = I_\mathfrak{p} J_\mathfrak{p}.$$

Furthermore,

$$(I:J)_\mathfrak{p} = \{x \in K \mid xJ \subseteq I\}_\mathfrak{p} = \{x \in K \mid xJ_\mathfrak{p} \subseteq I_\mathfrak{p}\} = (I_\mathfrak{p} : J_\mathfrak{p}).$$

□

**Proposition 3.1.21.** *Suppose $I$ is a fractional ideal of a noetherian domain $R$. Then $I$ is invertible if and only if its localization at every maximal ideal $\mathfrak{m}$ of $R$ is invertible.*

*Proof.* Let us suppose that $I$ is invertible. Then by our exposition above, we see that $I(R:I) = R$. Suppose $\mathfrak{m}$ is a maximal ideal of $R$. Then, by Lemma 3.1.20, we have that $I_\mathfrak{m}(R_\mathfrak{m} : I_\mathfrak{m}) = R_\mathfrak{m}$, so, in particular, $I_\mathfrak{m}$ is invertible as well. On the other hand, if we suppose $I_\mathfrak{m}$ is invertible for every maximal ideal $\mathfrak{m}$, then $I_\mathfrak{m}(R_\mathfrak{m} : I_\mathfrak{m}) = R_\mathfrak{m}$ for every $\mathfrak{m}$. Since $R$ satisfies the conditions of Proposition 3.1.17, we have that $R = \bigcap_\mathfrak{m} R_\mathfrak{m}$. We therefore get the following equality

$$\bigcap_\mathfrak{m} (I(R:I))_\mathfrak{m} = \bigcap_\mathfrak{m} I_\mathfrak{m}(R_\mathfrak{m} : I_\mathfrak{m}) = \bigcap_\mathfrak{m} R_\mathfrak{m} = R.$$

Thus, we have that $I(R:I) = R$, from whence we conclude that $I$ is invertible. □

**Remark 3.1.22.** *Note that the same proof works to show that $I$ is invertible if and only if its localization at every prime ideal $\mathfrak{p}$ of $R$ is invertible.*

We recall that a domain is called a Prüfer domain if every finitely generated ideal in the domain is invertible. These domains were first introduced by Heinz Prüfer (after whom the domain is named) in his 1932 paper [Prü32], and the notion has since been generalised to commutative rings with identity.

**Definition 3.1.23** (A Prüfer Ring)**.** *A domain $R$ is called a **Prüfer ring** if every non-zero finitely generated ideal of $R$ is invertible.*

Note that any non-zero finitely generated ideal of $R$ is invertible if and only if any two-generated ideal of $R$ is invertible. One direction is obvious. For the reverse direction, note that if $I_1 + I_2$, $I_1 + I_3$, and $I_2 + I_3$ are invertible ideals of $R$, then there exist $J_1, J_2, J_3$, ideals of $R$ such that $(I_1 + I_2)J_1 = (I_1 + I_3)J_2 = (I_2 + I_3)J_3 = R$. Then by noticing that

$$(I_1 + I_2) \cdot (I_1 + I_3) \cdot (I_2 + I_3) = (I_1 + I_2 + I_3) \cdot (I_1I_2 + I_1I_3 + I_2I_3),$$

we get that

$$\begin{aligned} R &= (I_1 + I_2) \cdot (I_1 + I_3) \cdot (I_2 + I_3) \cdot J_1 \cdot J_2 \cdot J_3 \\ &= (I_1 + I_2 + I_3) \cdot (I_1I_2 + I_1I_3 + I_2I_3) \cdot J_1 \cdot J_2 \cdot J_3 \end{aligned}$$

and thus see that $(I_1 + I_2 + I_3)$ is, in fact, invertible. We can then prove the above statement by induction: assume that for any $n \geq 2$, any non-zero ideal with less than 2 generators is invertible. Let $I$ be an ideal generated by $a_1, a_2, \ldots, a_n$. Let $I_1$ be the ideal generated by $a_1$, $I_2$ be the ideal generated by $a_2$, and $I_3$ be the ideal generated by the elements $a_3, \ldots, a_n$. Then it is clear that $I = I_1 + I_2 + I_3$. Further, notice that $I_1 + I_2$, $I_1 + I_3$, and $I_2 + I_3$ are all ideals generated by lesser than $n$ generators. By the induction hypothesis, these are invertible, and thus $I$ is invertible as well. This demonstrates that we can change the definition of Prüfer rings to only consider non-zero two-generated ideals of $R$, i.e. $R$ is a **Prüfer ring**

if every non-zero two-generated ideal of $R$ is invertible.

For our purposes, we will use an equivalent condition that was established by Wolfgang Krull (who had named these domains in honour of Prüfer) involving the localization of $R$ at a prime ideal $\mathfrak{p}$ to define the notion of Prüfer rings. Recall that a **Bézout ring** is a ring in which the sum of two principal ideals is again a principal ideal (and so every finitely generated ideal is principal since the sum of any two principal ideals $I = (a)_R$ and $J = (b)_R$ is precisely the (two-generated) ideal generated by $a$ and $b$). In light of the exposition above, it is clear that any Bézout ring is a Prüfer ring.

**Lemma 3.1.24.** *Let $R$ be a local ring. $R$ is a valuation ring if and only if $R$ is a Bézout ring.*

*Proof.* Note that by Condition 3 of Observation (3.1.2), it is clear that if $R$ is a valuation ring, then every finitely generated ideal of $R$ is principal. Indeed, if $I = (a)_R + (b)_R$ is an ideal of $R$ for some $a, b \in R$, then since either $a \mid b$ or $b \mid a$, either $(a)_R$ is contained in $(b)_R$ or vice-versa. Hence $I$ is a principal ideal. Thus $R$ is a Bézout ring. On the other hand, suppose $R$ is a local Bézout ring with (unique) maximal ideal $\mathfrak{m}$, and suppose $a, b \in R$. Without a loss of generality, let us suppose that $\gcd(a, b) = 1$. We thus have that $(a)_R + (b)_R = R$. It is then clear that both of $a$ and $b$ cannot be contained within $\mathfrak{m}$. Hence, one of them must be a unit and thus divides the other. So either $ab^{-1}$ or $(ab^{-1})^{-1} = ba^{-1}$ is in $R$, from whence we conclude that $R$ is a valuation ring. □

**Theorem 3.1.25.** *Let $R$ be an integral domain. Then $R$ is a Prüfer ring if and only if for every maximal ideal $\mathfrak{m}$ of $R$, the localization $R_{\mathfrak{m}}$ is a valuation ring.*

*Proof.* For the forward direction, it suffices for us to show that $R_{\mathfrak{m}}$ is a Bézout ring in light of Lemma 3.1.24. Suppose $\frac{r_1}{s_1}, \frac{r_2}{s_2}, \ldots, \frac{r_n}{s_n} \in R_{\mathfrak{m}}$ such that $r_i \in R$ and $s \in R \setminus \mathfrak{m}$. Consider the ideal $I = (r_1)_R + (r_2)_R + \cdots + (r_n)_R$. Since $R$ is Prüfer, $I$ is invertible and so $I_{\mathfrak{m}} = (\frac{r_1}{s_1})_{R_{\mathfrak{m}}} + (\frac{r_2}{s_2})_{R_{\mathfrak{m}}} + \cdots + (\frac{r_n}{s_n})_{R_{\mathfrak{m}}}$ is invertible by Proposition 3.1.21. Since $R_{\mathfrak{m}}$

is a local ring, it has only one maximal ideal, and so by Lemma 3.1.19, $I_{\mathfrak{m}}$ is principal.

In the reverse direction, let $R_{\mathfrak{m}}$ be a valuation ring. Then clearly it is a Bézout ring by Lemma 3.1.24. Suppose $I$ is a finitely generated ideal of $R$, generated by $i_1, i_2, \ldots, i_n$. We need to show that $I$ is invertible. Note that since $I$ is finitely generated, so is $I_{\mathfrak{m}}$, and thus, $I_{\mathfrak{m}}$ is principal. Suppose, to the contrary, that $I$ is not invertible. Then there exists an ideal $J$ such that $IJ \subseteq \mathfrak{m}$. Since $I_{\mathfrak{m}} = IR_{\mathfrak{m}}$ is principal, there exists some $i \in I$ such that $I_{\mathfrak{m}} = (i)_{R_{\mathfrak{m}}}$. Note that there thus exist some $r_k \in R$ and $s_k \in R \setminus \mathfrak{m}$ such that $i_k = i\frac{r_k}{s_k}$ for $1 \leq k \leq n$. Let $s = s_1 \cdot s_2 \cdots s_n$. Then, $s \cdot i^{-1} \cdot i_k \in R$ for every generator $i_k$ of $I$. Thus, we have that $s \cdot i^{-1} \in J$. This implies that $s = s \cdot i^{-1} \cdot i \in JI \subseteq \mathfrak{m}$, contradicting the fact that $s \in R \setminus \mathfrak{m}$. Thus $I$ is invertible, from whence we have that $R$ is a Prüfer ring. □

Note that if $R$ is a Prüfer ring and there exists another ring $R'$ such that $R \subseteq R' \subseteq q(R)$, then $R'$ is itself also a Prüfer ring. Indeed, if $\mathfrak{m}'$ is a maximal ideal of $R'$, and $\mathfrak{p} = \mathfrak{m}' \cap R$, let $\mathfrak{m}$ be a maximal ideal of $R$ containing $\mathfrak{p}$. Then we have the following chain of localizations

$$R_{\mathfrak{m}} \subseteq R_{\mathfrak{p}} \subseteq R'_{\mathfrak{m}'}.$$

Since $R_{\mathfrak{m}}$ is a valuation ring by Theorem 3.1.25, then by part (1) of Observation (3.1.2), we have that both $R_{\mathfrak{p}}$ and $R'_{\mathfrak{m}'}$ are valuation rings of $q(R)$. In light of this, notice that another equivalent condition to $R$ being a Prüfer ring is that $R_{\mathfrak{p}}$ is a valuation ring for every prime ideal $\mathfrak{p}$ of $R$. Indeed, the discussion preceding this statement asserts that $R_{\mathfrak{p}} \supseteq R_{\mathfrak{m}}$ is a valuation ring, while the "forward direction" of our proof of Theorem 3.1.25 can be re-written replacing all considerations of maximal ideals by prime ideals without any issue.

We now turn our attention to multi-valued fields. Let $K$ be a multi-valued field, with a family of valuation rings $W = \{R_1, R_2, \ldots, R_n\}$. When $n$ is finite, these multi-valued fields are also commonly referred to in the literature as $n$-fold valued fields. For our purposes, however, we will consider primarily the situation

where $n$ is countably infinite. We first introduce the notion of independence between two valuation rings.

**Definition 3.1.26.** *Let $R_1$ and $R_2$ be proper valuation rings of a field $K$. We say that $R_1$ and $R_2$ are **independent** if the subring of $K$ generated by $R_1$ and $R_2$, denoted $S$, is not proper, i.e. $S = K$. A family $W$ of valuation rings of a field $K$ is said to be independent if $R_1$ and $R_2$ are independent for any pair $R_1, R_2 \in W$ with $R_1 \neq R_2$.*

**Remark 3.1.27.** *Note that the independence of a family of valuation rings, $W$, imply in particular, that any two valuation rings $R_1$ and $R_2$ in $W$ are incomparable by inclusion.*

Much of the study of multi-valued fields involves understanding how the different valuation rings in the family $W$ "interact" with one another. A useful ring which aids in this study is the holomorphy ring of $W$: for a family of valuation rings $W = \{R_i \mid i \in \omega\}$ of a field $K$, the **holomorphy ring**, denoted by $R_W$, is the intersection of all the valuation rings in $W$, i.e.

$$R_W = \bigcap\{R_i \mid R_i \in W\}.$$

For each $R_i \in W$, we denote by $\mathfrak{p}_{R_i}$ the prime ideal $\mathfrak{m}_{R_i} \cap R_W$ of the holomorphy ring $R_W$.

Now suppose $R$ is a Prüfer ring with field of fractions $K = q(R)$. We denote by $W(R)$ the following set

$$W(R) = \{R_{\mathfrak{m}} \mid \mathfrak{m} \text{ is a maximal ideal of } R\} = \{R_{\mathfrak{m}} \mid \mathfrak{m} \in m\mathrm{Spec}(R)\}.$$

By Theorem 3.1.25, we know that this is a family of valuation rings of $K$. As such, we can consider the holomorphy ring of $W(R)$, $R_{W(R)} = \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$. In light of Proposition 3.1.17, we have that $R_{W(R)} = R$. We say that a family of valuation rings

$W$ of a field $K$ is **affine** if the holomorphy ring $R_W$ of $W$ is Prüfer and $W = W(R_W)$. Thus, within an affine family of valuation rings $W$, we have the following equality

$$W = \{(R_W)_{\mathfrak{m}} \mid \mathfrak{m} \text{ is a maximal ideal of the Prüfer ring } R_W\} = W(R_W).$$

It is therefore clear that if $R$ is a Prüfer ring, then the family $W(R) = \{R_{\mathfrak{m}} \mid \mathfrak{m} \in m\text{Spec}(R)\}$ of valuation rings of $K = q(R)$ is affine. Examples of affine families include any finite family of valuation rings of any given field, since the corresponding holomorphy ring of such a family would then be a Prüfer ring by virtue of Proposition 2.3.3 of [Ers01b]. A more appropriate example within the context of our study would be that of the family $W = \{\mathbb{Z}_{(p)} \mid p \text{ a rational prime}\}$ of discrete valuation rings obtained by the localization of $\mathbb{Z}$ at the prime ideal generated by $p$, for all primes $p$. Henceforth, we will say that $K$ is a **multi-valued field** if there is an affine family of valuation rings $W = \{R_i \mid i \in \omega\}$ of $K$, and denote this multi-valued field by $\langle K, W\rangle$ or alternatively, by $\langle K, R\rangle$ where $R$ is a Prüfer ring (with $K = q(R)$) whichever is most convenient within the context.

The discussion above seems to suggest that one could introduce the Zariski topology to study the family $W$ of valuation rings of a field $K$. This is indeed the case – on an affine family $W$ of valuation rings, we introduce the Zariski topology by the basis of open sets of the form

$$V_{a^{-1}} = \{R_i \mid R_i \in W,\ a^{-1} \in R_i\}, \quad \text{where } a \in R_W \setminus \{0\}.$$

**Remark 3.1.28.** *By Proposition 2.3.7 of [Ers01b], we see that a subfamily $W_0 \subset W$ of an affine family $W$ is also affine if and only if $W_0$ is compact in the Zariski topology.*

**Definition 3.1.29** (Boolean and Near-Boolean Families)**.**

- *An affine family $W$ of valuation rings is said to be **Boolean** if all sets $V_{a^{-1}}$ are open-closed (so $W$ is a Boolean space relative to the above-mentioned Zariski topology);*

- *An affine family $W$ of valuation rings is said to be* ***near-Boolean*** *if any proper closed subfamily of $W$ is Boolean.*

Suppose $K$ is a field and $\pi$ is some non-zero element of $K$. A valuation ring $R$ of $K$ is called a $\pi$-valuation ring, with corresponding $\pi$-valuation $v_R$, if $v_R(\pi)$ is the least positive element of the value group $\Gamma_R$ of $v_R$. If there exists at least one such $\pi$-valuation of $K$, then we call $K$ a **formally $\pi$-adic field**. Now for any field $K$ and $\pi \in K \setminus \{0\}$, the family of all $\pi$-valuation rings of $K$ is an example of Boolean families (cf. Proposition 2.4.7 of [Ers01b]). It is clear from the definition above that any Boolean family is automatically a near-Boolean family as well. Thus, we provide examples of near-Boolean families which are not Boolean families. These include the example of the family $W = \{\mathbb{Z}_{(p)} \mid p \text{ a rational prime}\}$ of discrete valuation rings obtained by the localization of $\mathbb{Z}$ at the prime ideal generated by $p$, for all primes $p$, as provided above. Similarly, the family

$$W = \{F[X]_{\mathfrak{m}} \mid \mathfrak{m} \text{ a maximal ideal of the polynomial ring F[X]}\}$$

where $F[X]_{\mathfrak{m}}$ is the localization of the polynomial ring in one variable, $F[X]$, at the maximal ideal $\mathfrak{m}$ for any arbitrary field $F$, would be yet another example of a near-Boolean family that is not a Boolean family.

**Remark 3.1.30.** *Note that if $R_i$ is some valuation ring of the field $q(R_i)$, then for any $r \in q(R_i) \setminus \{0\}$, we have that $r \notin R_i$ if and only if $r^{-1} \in \mathfrak{m}_{R_i}$. Thus, if we let $W$ be an affine family of valuation rings, we can define*

$$W_a := \{R_i \mid R_i \in W,\ a \in \mathfrak{m}_{R_i}\}$$

*for $a \in R_W \setminus \{0\}$ (i.e. $W_a = W \setminus V_{a^{-1}}$). Then $W$ is near-Boolean if the family $W_a$ is Boolean for any $a \in R_W \setminus \{0\}$. In fact, if $W$ is near-Boolean, then the family $W_A$ is Boolean for any finite subset $A \subseteq (R_W \setminus \{0\})$. Note that we can define another topology, sometimes referred to as the* ***Constructive topology****, on $W$ via the subbase $W_a$ for $a \in R_W \setminus \{0\}$.*

**Definition 3.1.31** (B-Rings and NB-Rings)**.**

- *A Prüfer ring $R$ is called a* ***B-ring*** *if the quotient ring, $\overline{R} = R/J(R)$, of $R$, by its Jacobson radical, $J(R) = \bigcap\{\mathfrak{m} \mid \mathfrak{m}$ is a maximal ideal of $R\}$, is a von Neumann regular ring, i.e. the following sentence holds in $\overline{R}$: $\forall x\ \exists y\ \ (x^2y = x)$;*

- *A domain $R$ with identity is called an* ***NB-ring*** *if it is a valuation ring or*

$$M(R) := R \setminus (U(R) \cup J(R)) \neq \varnothing$$

*and for all $a \in M(R)$ the ring $R_a := S_a^{-1}R$ is a B-ring. Here, $U(R)$ is the family of invertible elements of the ring $R$, $J(R)$ is the Jacobson radical of $R$, and $S_a := \{b \mid b \in R,\ (a,b)_R = R\}$ where $(a,b)_R$ is an ideal of $R$ generated by $a$ and $b$.*

**Remark 3.1.32.** *Note that, in particular, we have that $S_0 = U(R)$ and $S_u = R$ for all $u \in U(R)$.*

The connection between Boolean (respectively, near-Boolean) families of valuation rings, and the notions of B-rings (respectively, NB-rings) is established through the following proposition which shows that for an affine family $W$ of valuation rings of a field $K$, the holomorphy ring $R_W$ is indeed able to fully capture the property that $W$ is a Boolean family (and correspondingly, if $W$ is a near-Boolean family):

**Proposition 3.1.33** (cf. Proposition 2.4.3 and Proposition 2.5.3 of [Ers01b])**.** *A family, $W$, of valuation rings of a field, $K$, is*

- *Boolean if and only if the holomorphy ring, $R_W$, is a B-ring;*

- *near-Boolean if and only if the holomorphy ring, $R_W$, is an NB-ring.*

In light of the proposition above, we are able to provide examples of B-rings and NB-rings by constructing at the corresponding holomorphy rings of those examples of Boolean families and near-Boolean families, respectively, that we had provided earlier. In particular, we point out that both the ring of rational integers, $\mathbb{Z}$, and the ring of polynomials in one variable over any arbitrary field $F$, $F[X]$, are NB-rings that are not B-rings.

Of particular relevance to us in the study of wonderful extensions of the rationals is the notion of generalized Dedekind rings. We first recall that $R$ is a Dedekind ring if and only if the following two conditions are satisfied:

1. every element $a$ of $q(R)$ is contained in almost all (i.e. all but finitely many) rings of $W(R) = \{R_{\mathfrak{m}} \mid \mathfrak{m} \in m\text{Spec}(R)\}$, i.e. the set $\{R_{\mathfrak{m}} \in W(R) \mid a \notin R_{\mathfrak{m}}\}$ is finite; and

2. for every maximal ideal $\mathfrak{m}$ of $R$, the localization of $R$ at $\mathfrak{m}$, $R_{\mathfrak{m}}$, is a discrete valuation ring.

Notice that for any $a \in q(R)$, the set $U_a = \{R_{\mathfrak{m}} \in W(R) \mid a \in R_{\mathfrak{m}}\}$ is an open set in the Zariski topology. Further, since the localization of $R$ at $\mathfrak{m}$ is a discrete valuation ring, $\Gamma_{R_{\mathfrak{m}}} \cong \mathbb{Z}$. Using these observations, one can generalize the notion of a Dedekind ring in the following way: a Prüfer ring $R$ is called a **generalized Dedekind ring**[1] if the following conditions are satisfied:

1. every non-empty open set $U$ of the family $W(R)$ is cofinite, i.e. $W(R) \setminus U$ is finite; and

2. for all $R_{\mathfrak{m}} \in W(R)$, the value group $\Gamma_{R_{\mathfrak{m}}}$ is Archimedean.

The relevance of the study of these generalized Dedekind rings within the context of Boolean and near-Boolean families can be seen through the following observation: if $R$ is a generalized Dedekind ring, then the corresponding family $W(R)$ is, in fact, near-Boolean and independent. We had seen that every Dedekind ring satisfies the conditions of a generalized Dedekind ring, and are thus examples of generalized Dedekind rings. Further note that if $R$ is an NB-ring (and so $W(R)$ is a near-Boolean

[1] The notion of "generalized Dedekind ring" as we are describing in this paper appears to be specific to Ershov's works and should not be confused with the same notion as introduced by Nicolae Popescu in his work *On a Class of Prüfer Domains* (cf. [Pop84]) in which a domain $R$ is defined to be a generalized Dedekind domain if and only if it is a Prüfer domain, $\mathfrak{p} \neq \mathfrak{p}^2$ for every non-zero prime ideal $\mathfrak{p}$ of $R$, and every prime ideal of $R$ is the radical of a finitely generated ideal. Yet another notion of "generalized Dedekind domain" has also been introduced by Muhammad Zafrullah in the paper *On Generalized Dedekind Domains* (cf. [Zaf86]) in which an integral domain $R$ is defined to be a generalized Dedekind domain if and only if for all non-zero fractional ideals $I$ and $J$ of $R$ the following condition is satisfied: $(IJ)^{-1} = I^{-1}J^{-1}$.

family) such that for all $R_{\mathfrak{m}} \in W(R)$, the value group $\Gamma_{R_{\mathfrak{m}}}$ is Archimedean, then $R$ is a generalized Dedekind ring. In particular, if $R$ is a valuation ring whose value group is isomorphic to $\mathbb{Q}$ or $\mathbb{R}$, then $R$ is a generalized Dedekind ring that is not a Dedekind ring. We state some properties of generalized Dedekind rings in the form of a proposition:

**Proposition 3.1.34** (cf. Proposition 5 of [Ers01a])**.** *Suppose $R$ is a generalized Dedekind ring with $K = q(R)$.*

1. *Any intermediate ring $R'$ is a generalized Dedekind ring, i.e. for any ring $R'$ such that $R \subseteq R' \subseteq K$, $R'$ is a generalized Dedekind ring;*

2. *If $K'$ is a finite extension of $K$ and $R^{ic}$ is the integral closure of $R$ in $K'$, then $R^{ic}$ is a generalized Dedekind ring.*

If $R$ is generalized Dedekind, then by a corollary of Erhsov (cf. Corollary on page 418 of [Ers09]), we see that the Zariski topology on the family $W(R)$ is the so-called $\tau_1$-topology, referring to a topology consisting of all cofinite sets. Specifically, a topological space is called a **$\tau_1$-space** if the (non-empty) open sets of the space are precisely all the (non-empty) cofinite sets. These $\tau_1$-spaces are endowed with a least $T_1$-topology and carry the following properties:

1. every $\tau_1$-space is compact;

2. every subspace of a $\tau_1$-space is a $\tau_1$-space;

3. for any $\tau_1$-spaces $X$ and $Y$, the map $f : X \to Y$ of $X$ into $Y$ is continuous if and only if $f^{-1}(y)$ is finite for any $y \in Y$;

4. every map of a $\tau_1$-space onto a $\tau_1$-space is open.

Note that property (2), in particular, implies that every subset of a $\tau_1$-space is compact.

**Definition 3.1.35** (Residue Fields Being Ample in Infinity)**.** *We say that residue fields of a near-Boolean family $W$ of valuation rings of a field $K$ are* ***ample in infinity*** *if for any $n > 0$, there is an element $d_n \in R_W \setminus \{0\}$ such that for any $R' \in V_{d_n^{-1}}$, for every absolutely irreducible polynomial $h \in K_{R'}[x, y_0, \ldots, y_{n-1}]$ which is monic and separable in $x$ and has degree $\leq n$ (as a polynomial in $x, y_0, \ldots, y_{n-1}$), and for each polynomial $g \in K_{R'}[\overline{y}] \setminus \{0\}$ of degree $\leq n$, the fact that there exists $a, \overline{b} \in K_{R'}$ such that $h(a, \overline{b}) = 0$ and $h'(a, \overline{b}) \neq 0$ implies that there exists $c, \overline{d} \in K_{R'}$ such that $h(c, \overline{d}) = 0$, $h'(c, \overline{d}) \neq 0$, and $g(\overline{d}) \neq 0$.*

**Remark 3.1.36.** *Note that it is only interesting to ask whether the residue fields of near-Boolean families are ample in infinity, since if $W$ is Boolean, then the residue fields of $W$ are automatically ample in infinity. This follows from the fact that if $R_W$ is a proper B-ring, then its Jacobson radical, $J(R_W)$ is not trivial. Indeed, if $J(R_W) = \{0\}$, then $R_W$ is, in particular, von Neumann regular. However, it is known that von Neumann regular rings without divisors of zero contain only one ideal. Hence, this would indicate that $q(R_W) = R_W$, contradicting the fact that $R_W$ is proper. Since we know that $W$ is Boolean if and only if $R_W$ is a B-ring by Proposition* 3.1.33*, we thus have that $J(R_W) \neq \{0\}$. So each element $d \in J(R_W) \setminus \{0\}$ can be taken to be $d_n$ for any $n$ since we have that $V_{d^{-1}} = \varnothing$.*

This condition on the residue fields of a near-Boolean family is related to the notion of ampleness: A field $K$ is **ample** or **large**[2] if for each polynomial $g \in K[\overline{y}] \setminus \{0\}$ and for every absolutely irreducible polynomial $h \in K[x, \overline{y}]$ which is monic and separable in $x$ and for which there are $a, \overline{b} \in K$ such that $h(a, \overline{b}) = 0$ and $h'(a, \overline{b}) \neq 0$, there exists $c, \overline{d} \in K$ such that $h(c, \overline{d}) = 0$, $h'(c, \overline{d}) \neq 0$, and $g(\overline{d}) \neq 0$. Indeed, we have the following equivalence:

[2] The notion of "large fields" was first used by Florian Pop in [Pop96] to describe a class of fields over which many "interesting mathematics" can be done – for instance, such fields can be used to study inverse Galois theory, torsors of finite groups, rationally connected varieties, elementary theory of function fields, etc. Because of its wide applications within different areas of mathematics, such fields have been called by different names throughout the literature including, "épais", "fertile", "weite Körper", "anti-Mordellic", etc.

**Proposition 3.1.37** (cf. Proposition 12 of [Ers01a]). *Let $W$ be a near-Boolean family. Then the residue fields of $W$ are ample at infinity if and only if for every elementary extension $\langle K', R_{W'}\rangle$ of $\langle K, R_W\rangle$ and for any $R' \in W'$ such that $K \subseteq R'$, the residue field $K_{R'}$ is ample.*

**Definition 3.1.38.** *Let $\langle K, W\rangle$ be a multi-valued field, and let $\varphi(\overline{x})$ be a formula of the signature $\mathscr{L} = \mathscr{L}_{ring} \cup \{\mathcal{O}_v\}$, where $\mathcal{O}_v$ is a unary predicate symbol distinguishing a valuation ring. We say that*

- ***the local truth of $\boldsymbol{\varphi}$ is continuous on $\langle \mathbf{K}, \mathbf{W}\rangle$*** *if for any $\overline{a} \in K$, the set $\{R_i \mid R_i \in W,\ \mathbb{H}_{R_i}(K) \models \varphi(\overline{a})\}$ is open in $W$ (with respect to the Constructive topology);*
- ***local elementary properties are continuous on $\langle \mathbf{K}, \mathbf{W}\rangle$*** *if the local truth of any formula is continuous.*

*Furthermore, for a multi-valued field $\langle K, W\rangle$ with a near-Boolean family $W$, we say that its **local elementary properties are near-continuous** if they are continuous for any subfamily $W_d$, $d \in R_W \setminus \{0\}$.*

Let $R_1 \subseteq R_2$ be an extension of Prüfer rings. We say that the extension is **geometric** if, for any maximal ideal $\mathfrak{m}_2$ of the ring $R_2$, the prime ideal $\mathfrak{m}_2 \cap R_1$ of $R_1$ is maximal. This induces a (continuous in the Zariski topology) **restriction map** from $W(R_2)$ into $W(R_1)$

$$\pi : W(R_2) \to W(R_1),$$

with $\pi\left((R_2)_{\mathfrak{m}_2}\right) = (R_1)_{\mathfrak{m}_2 \cap R_1}$. We now define the notion of an immediate extension for Prüfer rings.

**Definition 3.1.39** (Immediate Extension of Prüfer Rings). *A geometric extension $R_1 \subseteq R_2$ of Prüfer rings with fields of fraction $q(R_1) = K_1 \subseteq K_2 = q(R_2)$ is said to be **immediate** if the following conditions are satisfied:*

1. *the restriction map $\pi : W(R_2) \to W(R_1)$ is a homeomorphism between the topological spaces $W(R_2)$ and $W(R_1)$;*

2. *for every maximal ideal* $\mathfrak{m}_2$ *of* $R_2$*, the extension* $\langle K_1, (R_1)_{\mathfrak{m}_2 \cap R_1} \rangle \leq \langle K_2, (R_2)_{\mathfrak{m}_2} \rangle$ *of valued fields is immediate.*

*In this case,* $R_1 = R_2 \cap K_1$.

**Remark 3.1.40.** *Note that if* $R_1 \subseteq R_2$ *are Dedekind rings, then Condition (1) above reduces to asking that the following mapping*

$$\mathfrak{m}_2 \mapsto \mathfrak{m}_2 \cap R_1, \quad \mathfrak{m}_2 \in mSpec(R_2),$$

*of* $mSpec(R_2)$ *onto* $mSpec(R_1)$ *is one-to-one.*

We state some properties that are preserved under immediate extensions of Prüfer rings.

**Proposition 3.1.41** (Some Properties Preserved Under Immediate Extensions)**.** *Suppose* $R_1 \subseteq R_2$ *is an immediate extension of Prüfer rings, then*

1. *if the family* $W(R_1)$ *is independent, then the family* $W(R_2)$ *is also independent;*
2. *if* $R_1$ *is a B-ring, then* $R_2$ *is a B-ring;*
3. *if* $R_1$ *is a NB-ring, then* $R_2$ *is a NB-ring;*
4. *if local elementary properties of* $W(R_1)$ *are continuous, then the local elementary properties of* $W(R_2)$ *are also continuous;*
5. *if the family* $W(R_1)$ *is near-Boolean and if residue fields of* $W(R_1)$ *are ample in infinity, then the family* $W(R_2)$ *is near-Boolean and the residue fields of* $W(R_2)$ *are also ample in infinity;*
6. *if* $R_1$ *is a generalized Dedekind ring, then* $R_2$ *is also a generalized Dedekind ring.*

Property (1) is established by Proposition 1 of [Ers01a], Property (2) and Property (3) are established as part of Proposition 2 in [Ers01a], Property (4) is an immediate consequence of Theorem 1 of [Ers94a]. Property (5) follows simply from

Property (3) and the definition of being ample in infinity. Property (6) follows from Definition 3.1.39 as $W(R_2)$ being homeomorphic to $W(R_1)$ implies that $W(R_2)$ is a $\tau_1$-space. Further note that by our discussion above, $W(R_2)$ is near-Boolean, and so any non-empty open set $U$ of $W(R_2)$ is cofinite. We thus only need to check if for any $R' \in W(R_2)$, the value group $\Gamma_{R'}$ is Archimedean. Note that since the extension $\langle q(R_1), R' \cap q(R_1)\rangle \leq \langle q(R_2), R'\rangle$ is immediate for any $R' \in W(R_2)$, it follows that the value group $\Gamma_{R'} = \Gamma_{R' \cap q(R_1)}$ is Archimedean.

## 3.2 Wonderful Extensions of $\mathbb{Q}$

With the necessary preliminaries set up in the previous section, we are now able to introduce the wonderful extensions[3] of the field of rational numbers, show that such extensions do exist, and look at some of their model-theoretic properties that are pertinent in showing the decidability of such fields. We will then go on to exhibit how such fields make for "good" base fields – the kind that we are looking for to answer Question (1.1.1) negatively. We primarily refer to articles [Ers00], [Ers01a] and [Ers02c], and the volume [Ers01b] by Ershov in the development of this section.

**Definition 3.2.1** (Wonderful Extensions of $\mathbb{Q}$)**.** *Let $\mathbb{Q}$ be the field of rational numbers, $\mathbb{R}$ the field of real numbers, and $\mathbb{Q}_p$ be the field of $p$-adic numbers with $p \in \mathbb{P}$, where $\mathbb{P}$ is the set of all prime numbers. An extension $K$ of $\mathbb{Q}$ is* ***wonderful*** *if there exist field embeddings $\lambda_r : K \longrightarrow \mathbb{R}$ and $\lambda_p : K \longrightarrow \mathbb{Q}_p$ with $p \in \mathbb{P}$ such that the following three conditions are satisfied:*

1. ***The Near-Boolean Property:***
   *The family $W = \{R_p = \lambda_p^{-1}(\mathbb{Z}_p) \mid p \in \mathbb{P}\}$ of valuation rings of the field $K$ is such that, for every $a \in K$, $\lambda_p(a) \in \mathbb{Z}_p$ for almost all (i.e. all but finitely many) primes $p \in \mathbb{P}$, i.e. the set $\{p \mid p \in \mathbb{P},\ a \notin R_p\}$ is finite;*

2. ***The Local-Global Principle:***
   *For any absolutely irreducible affine variety $V$ defined over $K$, $V$ has a simple*

[3] Referred to, in Russian, as "Удивительных расширениях" in Ershov's original work, this phrase is also sometimes translated as "amazing extensions" or "surprising extensions" by various translators of Ershov's works.

*$K$-rational point, provided that $V$ has a simple $\mathbb{R}$-rational point and a simple $\mathbb{Q}_p$-rational point for each $p \in \mathbb{P}$;*

3. ***The Maximality Property:***
*The field $K$ admits no proper algebraic extension, $K'$, that is embeddable into all fields $\mathbb{R}$ and $\mathbb{Q}_p$ with $p \in \mathbb{P}$.*

It is relatively clear that $\mathbb{Q}$ itself satisfies the near-Boolean Property. Indeed, the valuation rings $R_p$ of $\mathbb{Q}$ are just the discrete valuation rings, $\mathbb{Z}_{(p)} = \{{}^{z}\!/_{n} \mid z, n \in \mathbb{Z},\ p \not| n\}$, given by the localization of the Dedekind domain, $\mathbb{Z}$, at the prime ideal generated by $p$. Since $\mathbb{Z}$ is a Dedekind domain, then every $a$ in the field of fractions of $\mathbb{Z}$ (i.e. $a \in \mathbb{Q}$) is contained in almost all (i.e. all but finitely many) rings $\mathbb{Z}_{(p)}$, and therefore the set $\{p \mid a \notin \mathbb{Z}_{(p)}\}$ is finite. By an application of Chebotarev's Density Theorem, one can further see that $\mathbb{Q}$ also satisfies the Maximality Property – indeed, if an algebraic extension, $F$, of the field $\mathbb{Q}$ is embeddable into almost all fields $\mathbb{Q}_p$, then almost all the rational primes of $\mathbb{Q}$ split completely in $F$ (i.e. the density of the set of all rational primes of $\mathbb{Q}$ which split completely in $F$ is 1) and hence, $F = \mathbb{Q}$. This, in particular, shows that if $K$ is a wonderful extension of $\mathbb{Q}$ (provided that such extensions do exist), then $\mathbb{Q}$ is algebraically closed in $K$.

**Remark 3.2.2.** *Note that if a field $K$ with embeddings $\lambda_r$ and $\lambda_p$ for $p \in \mathbb{P}$ satisfies the Local-Global Principle, then $K$ has unique embeddings into $\mathbb{R}$ and $\mathbb{Q}_p$ for $p \in \mathbb{P}$, and these embeddings coincide precisely with the embeddings $\lambda_r$ and $\lambda_p$ for $p \in \mathbb{P}$ respectively.*

### 3.2.1 A Sketch of the Existence of Wonderful Extensions of $\mathbb{Q}$

We first begin by showing that such wonderful extensions of $\mathbb{Q}$ do, in fact, exist. We will approach this problem in two stages: In the first stage, we disregard any reference made to the real field in Definition 3.2.1 (and the corresponding ordering that would be induced by the embedding into $\mathbb{R}$) and show that there exists a countable immediate extension $K$ of $\mathbb{Q}$ that satisfies the near-Boolean property, the

(modified) local-global principle which now states that for any absolutely irreducible affine variety $V$ of $K$, $V$ has a simple $K$-rational point, provided $V$ has a simple $\mathbb{Q}_p$-rational point for each prime $p$, and the (modified) maximality property which now states that $K$ does not admit any proper algebraic extension that is embeddable into the fields $\mathbb{Q}_p$ for all primes $p$. We will call such extensions **W-extensions of $\mathbb{Q}$**. In the latter stage, we will discuss how one could deal with the inclusion of $\mathbb{R}$ into the mix by pointing out an appropriate property that the field $K$ must satisfy in order for the field to be a wonderful extension of $\mathbb{Q}$ (which we also term as a $W^+$-extension of $\mathbb{Q}$).

Suppose that $\mathfrak{M}$ is an $\mathscr{L}$-structure in some language $\mathscr{L}$, and with universe $M$. Denote by $\mathscr{L}_M$ the expanded language obtained by adding a new constant symbol $c_m$ for each element $m \in M$, i.e. $\mathscr{L}_M = \mathscr{L} \cup \{c_m \mid m \in M\}$, and let $\mathfrak{M}_M := (\mathfrak{M}, m)_{m \in M}$ be the expanded model in $\mathscr{L}_M$ where we interpret each new symbol $c_m$ by the element $m$. Recall that we say that a structure $\mathfrak{M}$ is **existentially closed** in a structure $\mathfrak{N}$, denoted $\mathfrak{M} \preccurlyeq_1 \mathfrak{N}$, if $\mathfrak{M}$ is a substructure of $\mathfrak{N}$, and every existential sentence which holds in $\mathfrak{N}_M$ also holds in $\mathfrak{M}_M$. We state a property of existentially closed structures via the following lemmata.

**Lemma 3.2.3.** *Suppose that $\mathfrak{N}$ and $\mathfrak{E}$ are $\mathscr{L}$-structures in some countable language $\mathscr{L}$ such that is the cardinality of the universe of $\mathfrak{N}$, $|N| \leq \alpha$, and $\mathfrak{E}$ is $\alpha$-saturated. If every existential sentence holding in $\mathfrak{N}$ holds in $\mathfrak{E}$, then $\mathfrak{N}$ is isomorphically embeddable in $\mathfrak{E}$.*

*Proof.* We suppose that $\{n_i \mid i < \alpha\}$ is an enumeration of the elements of $\mathfrak{N}$. We want to find a sequence of elements $e_i$ with $e_i$ in the universe $E$ of $\mathfrak{E}$ such that the mapping $n_i \mapsto e_i$ is an isomorphic embedding of $\mathfrak{N}$ into $\mathfrak{E}$. We proceed by an induction argument on $\beta < \alpha$. Suppose for all $\eta < \beta$, there exist some sequence $\{e_i \in E \mid i < \eta\}$ such that every existential sentence that holds in the expanded model $(\mathfrak{N}, n_\eta)_{\eta<\beta}$ also holds in the expanded model $(\mathfrak{E}, e_\eta)_{\eta<\beta}$. Let $\Sigma$ be the set of all existential formulae $\varphi(x)$ that is satisfied by $n_\beta$ in the model $(\mathfrak{N}, n_\eta)_{\eta<\beta}$. We

want to show that there exists some element $e_\beta \in E$ that satisfies $\Sigma$ as well. We take finite conjunctions of formulae in $\Sigma$, say $\psi$, and consider the existential sentence $\exists x\psi$. Since every existential sentence that holds in $\mathfrak{N}$ holds in $\mathfrak{E}$, all (existential) sentences $\exists x\psi$ obtained as such (i.e. by taking finite conjunctions of formulae in $\Sigma$ and existentially quantifying them) would also hold in $(\mathfrak{E}, e_\eta)_{\eta<\beta}$. We thus have that $\Sigma$ is consistent with the theory of $(\mathfrak{E}, e_\eta)_{\eta<\beta}$. We can then extend $\Sigma$ to some complete type of $(\mathfrak{E}, e_\eta)_{\eta<\beta}$. Note that since $(\mathfrak{E}, e_\eta)_{\eta<\beta}$ is still $\alpha$-saturated, the complete type is realised by some element in $E$. Thus, $\Sigma$ itself is realised by some element in $E$. Let this element be $e_\beta \in E$ as required. We then have that every existential sentence that holds in the expanded model $(\mathfrak{N}, n_\eta)_{\eta\leq\beta}$ also holds in the expanded model $(\mathfrak{E}, e_\eta)_{\eta\leq\beta}$. Since $\alpha$ is a limit ordinal, we then get that every existential sentence that holds in the expanded model $(\mathfrak{N}, n_\beta)_{\beta<\alpha}$ also holds in the expanded model $(\mathfrak{E}, e_\beta)_{\beta<\alpha}$. The lemma now follows by noting that existential sentences contain all atomic and negations of atomic sentences, and so the mapping $n_\beta$ to $e_\beta$ is an isomorphic embedding of $\mathfrak{N}$ into $\mathfrak{E}$. □

**Lemma 3.2.4.** *Let $\mathfrak{M}$ and $\mathfrak{N}$ be $\mathscr{L}$-structures for some countable language $\mathscr{L}$. Every existential sentence holding in $\mathfrak{N}$ holds in $\mathfrak{M}$ if and only if $\mathfrak{N}$ is isomorphically embeddable in some elementary extension of $\mathfrak{M}$.*

*Proof.* For the forward direction, suppose the cardinality of the universe of $\mathfrak{N}$, $|N| \leq \alpha$. We can then find a $\alpha^+$-saturated elementary extension of $\mathfrak{M}$, say $\mathfrak{E}$. Note that the cardinality of the universe of $\mathfrak{E}$ is either finite or $2^\alpha$. By Lemma 3.2.3, we see that $\mathfrak{N}$ is isomorphically embeddable in $\mathfrak{E}$. The reverse direction is trivial by virtue of the fact that existential sentences are preserved under extensions. □

The above lemma thus states that $\mathfrak{M}$ is existentially closed in $\mathfrak{N}$, i.e. $\mathfrak{M} \preccurlyeq_1 \mathfrak{N}$, if and only if there exists some elementary extension $\mathfrak{E}$ of $\mathfrak{N}$ such that $\mathfrak{M}$ is a substructure of $\mathfrak{E}$. Now consider a Prüfer ring $R$. We say that $R$ is **e-closed** if $R$ is existentially closed in every immediate extension $R'$ of $R$, i.e. $R \preccurlyeq_1 R'$ for all immediate extensions $R'$ of $R$. We now attempt to show that for every countable Prüfer ring $R$, there exists a countable e-closed immediate extension $R'$ of $R$.

**Proposition 3.2.5.** *For every (countable) Prüfer ring $R$, there exists a (countable) e-closed immediate extension of $R$.*

*Proof.* Indeed, suppose $R$ is a Prüfer ring , and let $\{\varphi_i \mid i < \omega\}$ be an enumeration of all the existential sentences in an appropriate language to study $R$ (so, in particular, the constants in the existential sentences are interpreted in $R$). We construct an ascending chain of immediate extensions of $R$

$$R_1 \subseteq R_2 \subseteq \cdots \subseteq R_n \subseteq \cdots$$

in the following way: take $R_1 = R$, and suppose $R_n$ is defined. If there does not exist an immediate extension $S$ such that $R_n \subseteq S$ and $S \models \varphi_n$, then set $R_{n+1} = R_n$. Otherwise, set $R_{n+1} = S$. We now take the union of such extensions

$$R^{(1)} = \bigcup_{i<\omega} R_i.$$

Notice that if $\varphi$ is some existential sentence (with constants interpreted within $R$) that is true in some immediate extension $S$ such that $R^{(1)} \subseteq S$, then $\varphi$ is, in fact, true in $R^{(1)}$. This follows from the fact that $\varphi = \varphi_n$ for some $n \in \omega$, and so since $R_n \subseteq R^{(1)} \subseteq S$, and by construction, $\varphi_n$ is true in $R_{n+1}$, the truth of the existential sentence moves up the extension to $R^{(1)}$. We note further, that $R^{(1)}$ is, in fact, an immediate extension of $R$ – one can easily check that the conditions as laid out in Definition 3.1.39 are all satisfied. Indeed, the union of any ascending chain of immediate extensions (of bounded cardinality)[4] is again an immediate extension.

We now continue the process to construct $R^{(2)}$ by considering another ascending chain of immediate extensions. This time, we consider an enumeration of all the existential sentences with constants interpreted in $R^{(1)}$ and begin with $R_1^{(1)} = R^{(1)}$. We then take the union $R^{(2)} = \bigcup_{i<\omega} R_i^{(1)}$. Similarly, obtain $R^{(3)}$, and so on. In this way, we obtain another ascending chain

$$R \subseteq R^{(1)} \subseteq R^{(2)} \subseteq \cdots \subseteq R^{(n)} \subseteq \cdots .$$

[4] The condition on the cardinality is there so as to ensure that the union does not form a proper class.

We now let $R^{(\omega)} = \bigcup_{i<\omega} R^{(i)}$. By the same reasons as stated above, $R^{(\omega)}$ is an immediate extension that is e-closed. Further, note that if $R$ is countable, we could restrict our construction to countable immediate extensions and the unions of ascending chains of such countable immediate extensions would once again be a countable immediate extension. □

Suppose $R$ is a Prüfer ring of a multi-valued field $\langle K, R\rangle$, where $K = q(R)$. We say that $R$ **satisfies property** (**M**) if there does not exist any proper separable algebraic extension $K'$ of $K$ such that for any $R_i \in W(R)$, there exists a $K$-embedding of $K'$ into the Henselization $K^h$ of $K$ with respect to the valuation ring $R_i$. Note that property (M) corresponds exactly to the maximality property of the $W$-extension of $\mathbb{Q}$ that we had described above. We say that an immediate extension $R' \supseteq R$ of Prüfer rings with corresponding fields of fractions $K' = q(R')$ and $K = q(R)$ is a **lift** if $K'$ is a separable algebraic extension of $K$ and the Henselizations $(R'_i)^h$ and $(R'_i \cap K)^h$ of the rings $R'_i$ and $R'_i \cap K$ coincide under the natural embedding of $(R'_i \cap K)^h$ into $(R'_i)^h$ for any valuation ring $R'_i \in W(R')$. We point out that the relation "$R'$ is a lift of $R$" is inductive and transitive, and so by Zorn's lemma, we can conclude that for any Prüfer ring $R$, we can find a "maximal" lift $R'$, i.e. we can find a Prüfer ring $R'$ that is a lift of $R$ such that $R'$ does not have any proper lifts. If $R'$ is a lift of $R$ which satisfies property (M), we call $R'$ an **M-lift** of $R$. We now state the following proposition that appears in [Ers01a]:

**Proposition 3.2.6** (cf. Proposition 4 of [Ers01a])**.** *Let $R$ be a countable NB-ring such that its Jacobson radical $J(R)$ is trivial and the field of fractions $K = q(R)$ is dense in the Henselizations $\mathbb{H}_{R_i}(K)$ for every $R_i \in W(R)$. Then $R$ has an* M*-lift.*

We point out that if $R = \mathbb{Z}$, then $R$ satisfies the above conditions; indeed, $R$ is a countable NB-ring, with trivial Jacobson radical, and by virtue of Lemma 3.1.14, $\mathbb{Q} = q(\mathbb{Z})$ is dense in the Henselizations. The condition that the Jacobson radical $J(R)$ be trivial can be replaced by the condition that the family of valuation rings $W(R)$ be independent based on the following proposition established in [Ers01b] and the observation that follows:

**Proposition 3.2.7** (cf. Proposition 2.5.4 of [Ers01b])**.** *Suppose $R$ is an NB-ring and let $a, b \in R \setminus J(R)$ and $ab \in J(R)$. Then $R$ is a B-ring.*

A corollary of the above proposition is that if $R$ is an NB-ring that is not a B-ring, then $J(R)$ is a prime ideal. Indeed, if we suppose otherwise, then for some $x, y \in R$, $xy \in J(R)$ but $x, y \notin J(R)$. Since we then have that $x, y \in R \setminus J(R)$ and $xy \in J(R)$, then the conditions for the proposition are fulfilled and thus $R$ would be a B-ring, leading to a contradiction.

**Observation 3.2.8.** *Suppose $R$ is an NB-ring that is not a B-ring. If $J(R) \neq \{0\}$, then the family of valuation rings $W(R)$ of $R$ is dependent, i.e. not independent.*

Indeed, since $R$ is an NB-ring that is not a B-ring, $J(R)$ is a prime ideal and so there exists a maximal ideal $\mathfrak{m}$ such that $J(R) \subseteq \mathfrak{m}$. Thus, $R_{\mathfrak{m}} \subseteq R_{J(R)}$. But note that since $J(R)$ is the intersection of all maximal ideals of $R$, we must have that for every maximal ideal $\mathfrak{m}$ of $R$, $R_{\mathfrak{m}} \subseteq R_{J(R)}$, i.e. all valuation rings in $W(R)$ are, in fact, contained in the proper valuation ring $R_{J(R)}$ of the field $K = q(R)$. However, this implies that any pair of different valuation rings in $W(R)$ are dependent, and so $W(R)$ is dependent.

We further note that for our particular case, since $\mathbb{Z}$ is a (generalized) Dedekind ring, one can significantly streamline the proof of Proposition 3.2.6:

**Proposition 3.2.9.** *If $R$ is a generalized Dedekind ring, then $R$ has an $M$-lift.*

First note that since $R$ is a generalized Dedekind ring, $W(R)$ is independent and so the condition on the Jacobson radical is naturally satisfied in light of Observation (3.2.8). Furthermore, $R$ satisfies all the remaining conditions of Proposition 3.2.6 as well – the condition of being dense in its Henselization follows from Remark 3.1.15.

*Proof.* We aim to show that if $R$ is a generalized Dedekind ring such that it does not have any proper lifts, then $R$ must satisfy property (M). Assume, to the contrary, that there exists some proper finite (separable) extension $K'$ of $K = q(R)$ such

that $K'$ is $K$-embeddable in the field $q(R_i^h)$ for any $R_i \in W(R)$, i.e. $R$ does not satisfy property (M). Suppose $R^{ic}$ is the integral closure of $R$ in $K'$. By part (2) of Proposition 3.1.34, $R^{ic}$ is a generalized Dedekind ring. Since $K'$ is $K$-embeddable in the field $q(R_i^h)$ for any $R_i \in W(R)$, we can, for every $R_i \in W(R)$, find some $R_i^{ic} \in W(R^{ic})$ such that $R_i \subseteq R_i^{ic} \subseteq q(R_i^h)$. Denote by

$$W^{ic} = \{R_i^{ic} \mid R_i \in W(R),\ R_i \subseteq R_i^{ic} \subseteq q(R_i^h)\}.$$

Note that $W^{ic}$ is then a $\tau_1$-space, and thus is a compact subfamily of $W(R^{ic})$ by property (2) of $\tau_1$-spaces mentioned above. By Proposition 2.3.7 of [Ers01b], $W^{ic}$ is, in fact, affine. Now we have the following inclusion

$$R^{ic} = R_{W(R^{ic})} \subseteq R_{W^{ic}} \subseteq q(R) = K,$$

and by part (1) of Proposition 3.1.34, $R_{W^{ic}}$ is a generalized Dedekind ring. Further, by construction, we also note that $R_{W^{ic}}$ is, in fact, a proper lift of $R$. This contradicts the fact that $R$ does not have any proper lifts. □

We have thus seen that if we take $R = \mathbb{Z}$, a countable NB-ring, then $R$ has an M-lift. We now claim that a countable e-closed immediate extension of $\mathbb{Z}$ is the desired M-lift.

**Corollary 3.2.10.** *Let $R$ be a countable e-closed immediate extension of $\mathbb{Z}$. Then $R$ satisfies property* (M).

*Proof.* By Proposition 3.2.5, we know that such an $R$ does exist. Since $R$ is an immediate extension of $\mathbb{Z}$, by Proposition 3.1.41, we know that $R$ is an NB-ring and $W(R)$ is independent. Further, since the extension is immediate, the value group $\Gamma_{R_i}$ is isomorphic to $\mathbb{Z}$ for every $R_i \in W(R)$, and so by Lemma 3.1.14, we know that the field $K = q(R)$ is dense in the Henselizations $\mathbb{H}_{R_i}(K)$ for every $R_i \in W(R)$. Thus, $R$ satisfies all the conditions of Proposition 3.2.6, and hence has an M-lift. It suffices to show that $R$ does not have any proper lifts, but this follows from the definition of being e-closed. Indeed, if there were to exist a proper lift $R'$ of $R$, then in particular, $K' = q(R')$ would be a proper (separable) algebraic extension of

$K = q(R)$. However, since $R$ is e-closed, every existential sentence that is true in $K'$ is also true in $K$, and in particular, those existential sentences that purport the existence of elements in $K'$ would likewise purport the existence of elements in $K$. Hence, $K'$ cannot be a proper algebraic extension of $K$. □

We now turn our attention to dealing with the local-global principle. Suppose $R$ is a Prüfer ring with quotient field $K = q(R)$, and let $W(R)$ be the corresponding affine family of valuation rings of $K$. We say that $R$ possesses **property ($\mathtt{LG_A}$)** if any absolutely irreducible affine variety $V$ defined over $K$ has a $R$-rational point provided that $V$ has a simple $R_i^h$-rational point for any valuation ring $R_i \in W(R)$. It is not too hard to see that this indeed corresponds with the local-global principle as stated in the description of the $W$-extensions of $\mathbb{Q}$. We want to show that there exists some immediate extension of $\mathbb{Z}$ which satisfies property ($\mathtt{LG_A}$). Towards this end, we define the property ($\mathtt{HR}_{\leq}$). We say that a ring $R$ satisfies **property ($\mathtt{HR}_{\leq}$)** if the following conditions hold: Let $f \in R[x, y_0, y_1, \ldots, y_{n-1}]$ be an absolutely irreducible monic separable polynomial in the variable $x$, $h_i \in R[x, y_0, y_1, \ldots, y_{n-1}]$ for $i < k$, and $g \in R[y_0, y_1, \ldots, y_{n-1}] \setminus \{0\}$. If, for any $d \in R \setminus (U(R) \cup \{0\})$, there exist $a, \overline{b} \in R_d (= S_d^{-1}R,$ cf. Definition 3.1.31) such that

- $f'_x(a, \overline{b}) \neq 0$,
- $h_i(a, \overline{b}) \neq 0$ for $i < k$,
- $f(a, \overline{b}) \cdot f'_x(a, \overline{b})^{-2} \cdot \left( \prod_{i<k} h_i(a, \overline{b}) \right)^{-1} \in J(R_d)$, and
- there exists some $c_i \in R_d$ such that $g(\overline{b}) \cdot c_i = h_i(a, \overline{b})$ for $i < k$,

then there are $a, \overline{b} \in R$ such that

- $f(a, \overline{b}) = 0$,
- $f'_x(a, \overline{b}) \neq 0$,
- $\prod_{i<k} h_i(a, \overline{b}) \neq 0$, and

- there exists some $c_i \in R$ such that $g(\overline{b}) \cdot c_i = h_i(a, b)$ for $i < k$.

The following proposition then provides a criterion to ensure that a given NB-ring satisfies property ($\mathtt{LG_A}$):

**Proposition 3.2.11** (cf. Proposition 3.3.3 of [Ers01b])**.** *An NB-ring $R$ possesses property ($\mathtt{LG_A}$) if and only if $R$ is a Bézout ring, $W(R)$ is independent, and $R$ possesses property ($\mathtt{HR}_{\leq}$).*

Using this proposition, we can show the following:

**Corollary 3.2.12.** *Let $R$ be a countable e-closed immediate extension of $\mathbb{Z}$. Then $R$ satisfies property ($\mathtt{LG_A}$).*

*Proof.* We first note that, as before, $R$ is an NB-ring and we have that $W(R)$ is independent. That $R$ is a Bézout ring is established in part (1) of Theorem 1 of [Ers01a]. By Proposition 6 of [Ers09], we further know that the residue fields for the family $W(\mathbb{Z})$ are ample in infinity, and so by property (5) of 3.1.41, the residue fields for the family $W(R)$ are ample in infinity. The residue fields being ample in infinity then allows one to establish that $R$ does indeed satisfy property ($\mathtt{HR}_{\leq}$) as shown in the proof of Theorem 2 of [Ers01a]. Since all the conditions are satisfied, one concludes that $R$ satisfies property ($\mathtt{LG_A}$). □

As an immediate consequence of Corollary 3.2.10 and Corollary 3.2.12, we have the following:

**Corollary 3.2.13.** *There exist a countable $W$-extension of $\mathbb{Q}$.*

*Proof.* Indeed, since we have that $\mathbb{Z} = \bigcap_{p \in \mathbb{P}} \mathbb{Z}_{(p)}$ with $q(\mathbb{Z}) = \mathbb{Q}$, let us denote the (multi-valued) field $\mathbb{Q}$ by $\langle \mathbb{Q}, \mathbb{Z} \rangle$. By Corollary 3.2.10 and Corollary 3.2.12, we have that there exists some countable e-closed immediate extension of $\mathbb{Z}$, say $R$, which satisfies property ($\mathtt{M}$) and property ($\mathtt{LG_A}$). Denote by $K = q(R)$. Then $\langle K, R \rangle$ is a $W$-extension of $\langle \mathbb{Q}, \mathbb{Z} \rangle$. □

We note that given any countable $W$-extension $K$ of $\mathbb{Q}$, one can construct a proper countable extension $K' \supseteq K$ that is also a $W$-extension of $\mathbb{Q}$. The uniqueness of the embeddings of the $W$-extensions into $\mathbb{Q}_p$ for all primes $p$ (cf. Remark 3.2.2) would then naturally imply that $K$ and $K'$ are non-isomorphic, i.e. $W$-extensions of $\mathbb{Q}$ are not (algebraically) unique.

**Remark 3.2.14.** *In the most general setting, we can consider a multi-valued field $\langle K, R\rangle$ satisfying the following conditions:*

1. *$K$ is a field of characteristic zero;*
2. *$R$ is an NB-ring such that $K = q(R)$ is a field of fractions of $R$;*
3. *All valuation rings $R_i$ in $W(R)$ have locally bounded absolute ramification indices, i.e. for every prime $p$, there exists some positive integer $n_p$ such that for any $R_i \in W(R)$, the set $\{\gamma \in \Gamma_{R_i} \mid 0 \leq \gamma \leq \upsilon_{R_i}(p)\}$ has no more than $n_p$ elements;*
4. *Local elementary properties of the near-Boolean family $W(R)$ is near-continuous.*

*Note that, in general, the* ***absolute ramification index*** *for a valuation ring $R_i \in W(R)$ is defined as being equal to*

- *1 if the residue field of the valuation ring is of characteristic 0;*
- *the number of elements in the set $\{\gamma \in \Gamma_{R_i} \mid 0 < \gamma \leq \upsilon_{R_i}(p)\}$ if the residue field is of characteristic $p > 0$ and the set is finite;*
- *$\omega$ otherwise.*

*If we then take $\langle K, R\rangle$ as described above such that $W(R)$ is independent and the residue fields are ample in infinity, then $W$-extensions for $K$ exist. We construct such $W$-extensions by first finding a countable elementary substructure $K' \preccurlyeq K$. Note that $K'$ would also satisfy the conditions that $W(R')$ is independent and that the residue fields are ample in infinity (that these statements are indeed expressible in a first-order manner is established in Ershov's [Ers01b]). We then find a countable*

*e-closed extension $K^* \supseteq K'$ among the immediate extensions of $K'$. $K^*$ would then satisfy both Corollary 3.2.10 and Corollary 3.2.12, and would be a $W$-extension of $K'$. Note that $K$ is elementarily embeddable in a suitable ultrapower $(K')^I/\Omega$ of the multi-valued field $K'$. The induced embedding of $K$ in $(K^*)^I/\Omega$ is then the desired $W$-extension of $K$.*

In order to take into account the embedding into $\mathbb{R}$ to obtain a $W^+$-extension, we need to ensure that our multi-valued field $K$ satisfies some further properties. We first limit ourselves to dealing with only the real embedding for the moment (without any considerations of the $p$-adic valuations). Observe that in order to prove the existence of an immediate extension of $\langle K, R\rangle$ that satisfies property ($\mathtt{M}$), we needed the condition that $W(R)$ is independent, and that the field of fractions $K$ is dense in the Henselizations $\mathbb{H}_{R_i}(K)$ for every $R_i \in W(R)$. On the other hand, in order to prove the existence of an immediate extension $\langle K, R\rangle$ that satisfies property ($\mathtt{LG_A}$), we needed that $R$ is Bézout, $W(R)$ is independent, and that $R$ possesses property ($\mathtt{HR}_{\leq}$) (which in turn required that the residue fields of $W(R)$ be ample in infinity). We therefore aim to describe the analogues for all these stated properties when we are looking at orderings instead of valuations. Towards this end, we recall some details from the study of orderings. A set $L \subseteq K$ is a **linear order** of the field $K$ if the following conditions hold:

1. $L + L \subseteq L$;
2. $L \cdot L \subseteq L$;
3. $L \cup -L = K$;
4. $L \cap -L = \{0\}$.

These conditions imply that $L$ contains the set of all sums of squares of $K$. Denote the set of all orderings of $K$ by $\mathfrak{X}(K)$. One can turn this into a topological space by using the so-called Harrison topology: the family of sets $W_a = \{L \in \mathfrak{X}(K) \mid a \in L\}$ for all $a \in K \setminus \{0\}$ forms a subbase for the topology. Note that $\mathfrak{X}(K)$ is a Boolean space under this topology, i.e. it is compact, Hausdorff, and totally disconnected.

Let us denote by $\langle K, L\rangle$ the ordered field $K$, together with the ordering $L$. Every ordered field has a real closure and so for a given system $\langle K, L\rangle$ as above, we denote the corresponding system that represents the real closure by $\mathbb{R}_L(K) := \langle K^{rc_L}, L^{rc}\rangle$ where $K^{rc_L}$ is the real closure of the field $K$ with respect to the ordering $L$, and $L^{rc}$, its (unique) ordering.

We can generalise this notion of an ordering to that of a preordering: A proper subset $P \subsetneq K$ is a **preorder** of $K$ if the following conditions hold:

1. $P + P \subseteq P$;

2. $P \cdot P \subseteq P$;

3. $K^2 \subseteq P$.

Note in particular, that $-1 \notin P$ for otherwise, for any $k \in K$, we can write $k = x^2 - y^2$ where $x = \frac{1+k}{2}$ and $y = \frac{1-k}{2}$, and we would have that $k \in K^2 + P \cdot K^2 \subseteq P + P \cdot P \subset P$. Denote by $\mathfrak{X}(P)$ the set of all orderings $L$ of $K$ such that $L \supseteq P$, i.e.

$$\mathfrak{X}(P) = \{L \in \mathfrak{X}(K) \mid L \supseteq P\}.$$

We can similarly define a topology on $\mathfrak{X}(P)$: the family of sets $W_a^+ = \{L \in \mathfrak{X}(P) \mid a \in L\}$ for all $a \in K \setminus \{0\}$ forms a subbase for the topology. If $P$ is a proper preorder of a field $K$, we then call the system $\langle K, P\rangle$ a **preordered field**. We point out that while in our current setting, $\mathfrak{X}(P)$ plays the role performed by $W(R)$ in the "valuation" situation, there is one important distinction worth mentioning – $\mathfrak{X}(P)$ is a *Boolean space* in the Harrison topology while within the case that is most relevant in the study of $W$-extensions, $W(R)$ is a *near-Boolean space* in the Zariski topology. We also state that $\mathbb{R}_L(K)$ would now play the role of $\mathbb{H}_{R_i}(K)$ within this current context – indeed the analogous property to $K$ being dense in $\mathbb{H}_{R_i}(K)$ for every $R_i \in W(R)$ would now be that $K$ is dense in $\mathbb{R}_L(K)$ for every $L \in \mathfrak{X}(P)$.

**Remark 3.2.15.** *For the purposes of our study involving the wonderful extensions of $\mathbb{Q}$, this distinction between the linear orders and the preorders is lost – indeed, we are dealing with the "maximal" preordering $P_{\mathbb{Q}} := \{r \in \mathbb{Q} \mid r \geq 0\}$ and so the notions of preordering and (linear) ordering coincide, i.e. $P_{\mathbb{Q}} = L$. Further, $\mathfrak{X}(P_{\mathbb{Q}}) = \mathfrak{X}(\mathbb{Q}) = \{P_{\mathbb{Q}}\}$.*

The analogous property for the independence of $W(R)$ corresponds to the so-called Block Approximation Property. We say that the system $\langle K, P\rangle$ possesses **property (BAP)** if the following holds: Suppose $a_1, a_2, \ldots, a_n \in K\backslash\{0\}$ are such that $\mathfrak{X}(P) = \bigcup\limits_{1\leq i\leq n} W_{a_i}^+$ is a finite partition of $\mathfrak{X}(P)$ into compact subsets, $b_1, b_2, \ldots, b_n \in K$ and $\varepsilon_i \in P_{a_i} \setminus \{0\}$ for $1 \leq i \leq n$, where $P_{a_i} := P + a_iP = \{x + a_iy \mid x, y \in P\}$. Then there exists a $c \in K$ such that $\varepsilon_i \pm (c - b_i) \in P_{a_i}$ for $1 \leq i \leq n$. One can easily check that each $P_{a_i}$ satisfies the above-mentioned conditions of a preorder of the field $K$, and that

$$\mathfrak{X}(P_{a_i}) = \{L \in \mathfrak{X}(K) \mid L \supseteq P_{a_i}\} = \{L \in \mathfrak{X}(P) \mid a_i \in L\} = W_{a_i}^+ \subseteq \mathfrak{X}(P).$$

That the property (BAP) is indeed the analogous property for the independence of $W(R)$ is established in its full generality in Proposition 3 of [Ers94b]. Again, for the purposes of our investigation into the wonderful extensions of $\mathbb{Q}$, we note that this condition is automatically satisfied by virtue of the fact that there is only one element (i.e. only one ordering) in $\mathfrak{X}(P_{\mathbb{Q}}) = \mathfrak{X}(\mathbb{Q})$.

A preordered field $\langle K, P\rangle$ satisfies the **Strong Approximation Property** if the subbase $W_a^+$ for all $a \in K \setminus \{0\}$ is a multiplicative base, i.e. it satisfies the following condition: for all $a, b \in K \setminus \{0\}$, there exists a $c \in K \setminus \{0\}$ such that $W_a^+ \cap W_b^+ = W_c^+$. In such a case, we call $\langle K, P\rangle$ a **SAP field**. Note that the property of being SAP is analogous to the holomorphy ring $R$ being a Bézout ring (sum of any two principal ideals is a principal ideal). Furthermore, if $\langle K, P\rangle$ is a SAP field, then every clopen subset of $\mathfrak{X}(P)$ is precisely the sets of the form $W_a^+$ for $a \in K \setminus \{0\}$. Once again, focusing our attention to the case where $K = \mathbb{Q}$, and $P_{\mathbb{Q}} = \{r \in \mathbb{Q} \mid r \geq 0\}$, we see that $\langle \mathbb{Q}, P_{\mathbb{Q}}\rangle$ is a SAP field. Indeed, we have

three possible scenarios which can occur – either $a, b \in \mathbb{Q} \setminus \{0\}$ is such that both of them are in $L = P_{\mathbb{Q}}$, one of them is not in $L$, or both of them are not in $L$. In the first two cases, we can choose $c \in L$ since we either have $L \cap L = L = W_c^+$ or $L \cap \varnothing = L = W_c^+$. For the third scenario, choose $c \in \mathbb{Q} \setminus L$ since we then have that $\varnothing \cap \varnothing = \varnothing = W_c^+$.

We finally point out that the analogue of property ($\mathtt{HR}_{\leq}$) is the following property which we label as **property ($\mathtt{AHR}_{\leq}$)**: Let $f \in K[x, y_0, y_1, \ldots, y_{n-1}]$ be an absolutely irreducible monic separable polynomial in the variable $x$, and let $a, a', \overline{b} \in K$ such that $\Delta(f(\overline{b})) \neq 0$ and $-f(a, \overline{b})f(a', \overline{b}) \in P$. Then for any $g \in K[y_0, y_1, \ldots, y_{n-1}] \setminus \{0\}$, there exists $a, \overline{b} \in K$ such that $f(a, \overline{b}) = 0$ and $g(\overline{b}) \neq 0$. Here $\Delta(f(\overline{y}))$ refers to the discriminant of the polynomial $f$ regarded as a polynomial in $x$.

We also need to elucidate what we mean when we say that a preordered field is an immediate extension of another. As one would expect, we have that an extension of preordered fields $\langle K, P\rangle \leq \langle K', P'\rangle$ is **immediate** if the restriction mapping $\pi : \mathfrak{X}(P') \to \mathfrak{X}(P)$ with $\pi(L') = L' \cap K$ where $L' \in \mathfrak{X}(P')$ is a homeomorphism of the spaces $\mathfrak{X}(P')$ and $\mathfrak{X}(P)$ and, the field $K$ is cofinal in $\langle K', L'\rangle$ for all $L' \in \mathfrak{X}(P')$. We now describe the corresponding conditions for both the maximality property and the local-global principle in the current context. The corresponding condition for maximality is as follows: a preordered field $\langle K, P\rangle$ satisfies the **maximality property** if there exists no proper algebraic extension $K' \supseteq K$ such that for any $L \in \mathfrak{X}(P)$, there exists a $K$-embedding of the field $K'$ into $K^{rc_L}$. We say that a preordered field $\langle K, P\rangle$ is **regularly r-closed** if for any absolutely irreducible affine variety $V$ over the field $K$, $V$ has a simple $K$-rational point provided $V$ has a simple $K^{rc_L}$-rational point for any order $L \in \mathfrak{X}(P)$. Just as we had Proposition 3.2.11 for the "valuations" case, we have the following proposition in this situation:

**Proposition 3.2.16** (cf. Theorem 3 of [Ers02c]). *Suppose that a preordered field $\langle K, P\rangle$ is SAP, satisfies property* (BAP) *and that $K$ is dense in $\mathbb{R}_L(K)$ for all $L \in \mathfrak{X}(P)$. Then $K$ is regularly r-closed if and only if $K$ satisfies property* ($\mathtt{AHR}_{\leq}$).

We note that we did not require any analogous notion to the property of the residue fields of $W(R)$ being ample in infinity. This should not come as a surprise in light of Remark 3.1.36. We therefore get the following result:

**Corollary 3.2.17** (cf. Proposition 3 of [Ers02c]). *Suppose $K$ is a countable SAP field. Then there exists a countable immediate extension of $K$ that satisfies the maximality condition and is regularly r-closed.*

We can now combine the results from above and consider both the orderings and the valuations simultaneously. For the most part, the definitions and terminologies remain the same as above – for instance, we can consider the field $K$ being dense in $\mathbb{H}_{R_i}(K)$ and being dense in $\mathbb{R}_L(K)$ for all $R_i \in W(R)$ and $L \in \mathfrak{X}(P)$ "separately" without any confusion to what it might mean in the combined setting. We will, however, need to make some adjustments to accommodate property ($\mathtt{HR}_{\leq}$) and property ($\mathtt{AHR}_{\leq}$) since we note that in the case of property ($\mathtt{HR}_{\leq}$), the polynomial $f$ was taken over $R[x, y_0, y_1, \ldots, y_{n-1}]$ (where $R$ is the holomorphy ring obtained by intersecting all the valuation rings in $W(R)$) whereas in the case of property ($\mathtt{AHR}_{\leq}$), we did not place any such restrictions and simply took $f$ to be over $K[x, y_0, y_1, \ldots, y_{n-1}]$.

Suppose $R$ is a Prüfer ring of a preordered multi-valued field $\langle K, R, P\rangle$, where $K = q(R)$ and $P$ is a proper preorder of $K$. We say that the system $\langle K, R, P\rangle$ **satisfies property** ($\mathtt{M}^{+}$) if there does not exist any proper separable algebraic extension $K'$ of $K$ such that for any $R_i \in W(R)$, there exist an $K$-embedding of $K'$ into an Henselization $K^h$ of $K$ with respect to the valuation ring $R_i$, and for any $L \in \mathfrak{X}(P)$, there exists a $K$-embedding of $K'$ in $K^{rc_L}$. In a similar fashion, we say that the system $\langle K, R, P\rangle$ **satisfies property** ($\mathtt{LG}_{\mathtt{A}}^{+}$) if for any absolutely irreducible affine variety $V$ over $K$, $V$ has a simple $R$-rational point provided $V$

has a simple $R_i^h$-rational point for any valuation ring $R_i \in W(R)$, and $V$ has a simple $K^{rc_L}$-rational point for any $L \in \mathfrak{X}(P)$. Note that these correspond exactly to the local-global principle and maximality property as described in Definition 3.2.1, taking into account that in this particular situation, $P = P_{\mathbb{Q}}$.

We say that a ring $R$ satisfies **property ($\mathbf{HR}_{\leq}^{+}$)** if the following conditions hold: Let $f \in R[x, y_0, y_1, \ldots, y_{n-1}]$ be an absolutely irreducible monic separable polynomial in the variable $x$, $h_i \in R[x, y_0, y_1, \ldots, y_{n-1}]$ for $i < k$, and $g \in R[y_0, y_1, \ldots, y_{n-1}] \setminus \{0\}$ be such that there exists $a, a', \overline{b} \in K$ for which $\Delta(f(\overline{b})) \neq 0$ and $-f(a, \overline{b})f(a', \overline{b}) \in P$. If, for any $d \in R \setminus \{0\}$, there exist $a, \overline{b} \in R_d (= S_d^{-1}R$, cf. Definition 3.1.31) such that

- $f'_x(a, \overline{b}) \neq 0$,
- $h_i(a, \overline{b}) \neq 0$ for $i < k$,
- $f(a, \overline{b}) \cdot f'_x(a, \overline{b})^{-2} \cdot \left( \prod_{i<k} h_i(a, \overline{b}) \right)^{-1} \in J(R_d)$, and
- there exists some $c_i \in R_d$ such that $g(\overline{b}) \cdot c_i = h_i(a, \overline{b})$ for $i < k$,

then there are $a, \overline{b} \in R$ such that

- $f(a, \overline{b}) = 0$,
- $f'_x(a, \overline{b}) \neq 0$,
- $h_i(a, \overline{b}) \neq 0$ for $i < k$, and
- there exists some $c_i \in R$ such that $g(\overline{b}) \cdot c_i = h_i(a, b)$ for $i < k$.

The following theorem is the analogue of Proposition 3.2.11 when we take into consideration both the ordering and the valuations of $K$:

**Theorem 3.2.18** (cf. Theorem 5 of [Ers02c])**.** *Suppose $\langle K, R, P \rangle$ is a preordered multi-valued field such that*

- *$R$ is a Bézout ring and $\langle K, P \rangle$ is a SAP field,*

- *$W(R)$ is independent and $\langle K, P\rangle$ possesses property* ($\mathtt{BAP}$),
- *$K$ is dense in $\mathbb{H}_{R_i}(K)$ for any $R_i \in W(R)$ and $K$ is dense in $\mathbb{R}_L(K)$ for any $L \in \mathfrak{X}(P)$.*

*Then the system $\langle K, R, P\rangle$ satisfies property* ($\mathtt{LG}^+_{\mathtt{A}}$) *if and only if $R$ satisfies property* ($\mathtt{HR}^+_{\leq}$).

In a similar fashion, one can then establish that

**Theorem 3.2.19** (cf. Proposition 7 of [Ers02c])**.** *Suppose $\langle K, R, P\rangle$ is a countable preordered multi-valued field such that $R$ is an NB-ring, $W(R)$ is independent, and the residue field of the families $W(R)$ are ample in infinity. Suppose further that $\langle K, P\rangle$ is a SAP field. Then there exists a countable immediate extension $\langle K', R', P'\rangle$ of $\langle K, R, P\rangle$ such that the system $\langle K', R', P'\rangle$ satisfies property* ($\mathtt{LG}^+_{\mathtt{A}}$) *and property* ($\mathtt{M}^+$).

In particular, since $\langle \mathbb{Q}, P_{\mathbb{Q}}\rangle$ is indeed a SAP field as we had remarked earlier, we have that $W^+$-extensions (or wonderful extensions) of $\mathbb{Q}$ do indeed exist as required. Just as we were able to point out that there exists some countable e-closed immediate extension of $\mathbb{Z}$ which is a $W$-extension of $\mathbb{Q}$, we are able to describe what the appropriate wonderful extensions of $\mathbb{Q}$ actually look like. In order to do so, however, we must first be able to generalise the notion of e-closedness. In the most general setting, we begin with some class of algebraic systems $\mathfrak{C}$ with some transitive and reflexive relation $\trianglelefteq$ on these systems such that if $\mathfrak{M} \trianglelefteq \mathfrak{N}$, then $\mathfrak{M}$ is a subsystem of $\mathfrak{N}$. We then say that $\mathfrak{M} \in \mathfrak{C}$ is **e-closed** (in the class $\mathfrak{C}$) if for any $\mathfrak{N} \in \mathfrak{C}$ such that $\mathfrak{M} \trianglelefteq \mathfrak{N}$ we have that $\mathfrak{M} \preccurlyeq_1 \mathfrak{N}$. In order for there to be an e-closed system, one needs to ensure that the class $\mathfrak{C}$ in question is closed under unions of chains, i.e. for any system $\mathfrak{M}_i \in \mathfrak{C}$ with $i \in I$ such that $\mathfrak{M}_i \trianglelefteq \mathfrak{M}_j$ or $\mathfrak{M}_j \trianglelefteq \mathfrak{M}_i$ for all $i, j \in I$, the system $\mathfrak{M} := \bigcup_{i\in I} \mathfrak{M}_i \in \mathfrak{C}$ and $\mathfrak{M}_i \trianglelefteq \mathfrak{M}$ for all $i \in I$. Indeed, we see that immediate extensions of Prüfer rings form such a class, and the proof of Proposition 3.2.5 which shows that one could find a countable e-closed immediate extension of $\mathbb{Z}$ can be generalised to show that whenever the class is closed relative

to unions, one could always find a (countable) e-closed system within the class.

We now attempt to describe the appropriate class of multi-valued fields that would allow us to find a countable e-closed immediate extension of $\langle \mathbb{Q}, \mathbb{Z}, P_{\mathbb{Q}} \rangle$. Towards this end, we introduce the adele ring over the rational numbers.

**Definition 3.2.20.** *The* ***ring of integral adeles*** $\mathbb{A}_{\mathbb{Z}}$ *is the product of the profinite completion of the integers* $\widehat{\mathbb{Z}}$*, with the real numbers* $\mathbb{R}$*, i.e.* $\mathbb{A}_{\mathbb{Z}} = \mathbb{R} \times \widehat{\mathbb{Z}}$*. The* ***ring of adeles*** $\mathbb{A}_{\mathbb{Q}}$ *itself is the rationalisation of the ring of integral adeles, i.e.* $\mathbb{A}_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{A}_{\mathbb{Z}}$*.*

Since $\widehat{\mathbb{Z}} \cong \prod_{p \in \mathbb{P}} \mathbb{Z}_p$, we could also write $\mathbb{A}_{\mathbb{Z}}$ as

$$\mathbb{A}_{\mathbb{Z}} \cong \mathbb{R} \times \prod_{p \in \mathbb{P}} \mathbb{Z}_p,$$

and correspondingly $\mathbb{A}_{\mathbb{Q}}$ as

$$\mathbb{A}_{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \left( \mathbb{R} \times \prod_{p \in \mathbb{P}} \mathbb{Z}_p \right).$$

The advantage of studying the ring of adeles within the context of our investigation into the wonderful extensions of $\mathbb{Q}$ is that this ring allows us to simultaneously handle both the valuations and the (unique real) ordering on $\mathbb{Q}$ in light of the following observation which is derived as a specific instance of Theorem 5 of [Ers09]:

**Observation 3.2.21** (cf. Theorem 5 of [Ers09])**.** *Suppose* $K$ *is a countable subfield of* $\mathbb{A}_{\mathbb{Q}}$ *with* $\mathbb{Q} \subseteq K \subseteq \mathbb{A}_{\mathbb{Q}}$ *and* $K' = K(x)$ *be a field of rational functions in one variable over* $K$*. Since* $|\mathbb{Q}_p| = |\mathbb{R}| = 2^{\aleph_0}$*, we note that there exist embeddings* $\varepsilon_{(p)_R} : K' \to \mathbb{Q}_p$ *for maximal ideals* $(p)_R$ *of* $\mathbb{Z}$*, and* $\varepsilon_{P_{\mathbb{Q}}} : K' \to \mathbb{R}$ *such that*

- $\varepsilon_{(p)_R} \restriction K = \pi_{(p)_R} \restriction K$ *where* $\pi_{(p)_R}$ *is a projection of* $\mathbb{A}_{\mathbb{Q}}$ *onto* $\mathbb{Q}_p$*, and*
- $\varepsilon_{P_{\mathbb{Q}}} \restriction K = \pi_{P_{\mathbb{Q}}} \restriction K$ *where* $\pi_{P_{\mathbb{Q}}}$ *is a projection of* $\mathbb{A}_{\mathbb{Q}}$ *onto* $\mathbb{R}$*.*

*These satisfy all the assumptions as stated in Theorem 5 of [Ers09], and hence, we can conclude that there exists a* $K$*-embedding* $\varepsilon : K' \to \mathbb{A}_{\mathbb{Q}}$ *such that* $\pi_{P_{\mathbb{Q}}} \circ \varepsilon = \varepsilon_{P_{\mathbb{Q}}}$*.*

Now consider the following class of multi-valued fields which are immediate extensions of $\langle \mathbb{Q}, \mathbb{Z} \rangle$:

$$\mathfrak{C}_{\mathbb{Q}} := \{\langle K, R\rangle \mid \mathbb{Q} \subseteq K \subseteq \mathbb{A}_{\mathbb{Q}},\ R = K \cap \mathbb{A}_{\mathbb{Z}}\}.$$

Note that if $\langle K, R\rangle \in \mathfrak{C}_{\mathbb{Q}}$ then $R$ is a Dedekind ring by virtue of property (6) of Proposition 3.1.41. One can easily check that $\mathfrak{C}_{\mathbb{Q}}$ is indeed closed under union of ascending chains and hence there exists some (countable) e-closed immediate (field) extension – as before, we say that $\langle K, R\rangle \in \mathfrak{C}_{\mathbb{Q}}$ is e-closed if for any $\langle K', R'\rangle \in \mathfrak{C}_{\mathbb{Q}}$ such that $\langle K, R\rangle \leq \langle K', R'\rangle$, we have that $\langle K, R\rangle \preccurlyeq_1 \langle K', R'\rangle$. We further point out that we do not have to explicitly concern ourselves with the unique ordering of $K$ – Observation (3.2.21) ensures that this is always taken care of implicitly.

**Remark 3.2.22.** *By Theorem 2 of [Ers09], $\langle K, R\rangle$ is e-closed (in class $\mathfrak{C}_{\mathbb{Q}}$) if and only if $R$ is e-closed as a Prüfer ring in the sense as described in Proposition* 3.2.5.

One can then show that such a countable e-closed immediate extension of $\langle \mathbb{Q}, \mathbb{Z}\rangle$ (in the class $\mathfrak{C}_{\mathbb{Q}}$) would satisfy the analogues of Corollary 3.2.10 and Corollary 3.2.12 with very similar proofs, i.e. the countable e-closed immediate extension of $\langle \mathbb{Q}, \mathbb{Z}\rangle$ satisfies both property $(M^+)$ and property $(LG_A^+)$. This result is stated as Theorem 6 of [Ers09], and is based on the proofs of Corollary 1 and Theorem 2 of [Ers01a]. Thus, countable e-closed immediate extension fields within the class $\mathfrak{C}_{\mathbb{Q}}$ (i.e. e-closed fields which are countable subfields of $\mathbb{A}_{\mathbb{Q}}$) indeed are the desired wonderful extensions of $\mathbb{Q}$. More precisely, we have the following:

**Corollary 3.2.23.** *Suppose that $K$ is a countable extension of the field $\mathbb{Q}$ and $\lambda_r : K \longrightarrow \mathbb{R}$ and $\lambda_p : K \longrightarrow \mathbb{Q}_p$ with $p \in \mathbb{P}$ are embeddings such that the family $\{\lambda_p^{-1}(\mathbb{Z}_p) \mid p \in \mathbb{P}\}$ is near-Boolean. Then the field $K$ has a countable e-closed immediate extension, $K'$, being a wonderful extension of $\mathbb{Q}$, and the embeddings of $K'$ into $\mathbb{R}$ and $\mathbb{Q}_p$ for $p \in \mathbb{P}$ extend the embeddings $\lambda_r$ and $\lambda_p$ with $p \in \mathbb{P}$.*

Once again, we point out that wonderful extensions of $\mathbb{Q}$ are not unique. Indeed, for any given wonderful extension $K$ of $\mathbb{Q}$, one can construct a proper countable extension $K'$ of $K$ that is also a wonderful extension of $\mathbb{Q}$ with $K'$ not being

isomorphic to $K$ by virtue of the fact that the embeddings of wonderful extensions of $\mathbb{Q}$ into $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes $p$ are unique as remarked previously.

### 3.2.2 A Sketch of the Decidability of Wonderful Extensions of $\mathbb{Q}$

We now move on to the task of describing how one would go about showing that the theory of the wonderful extensions of $\mathbb{Q}$ is decidable. As we had done before, we first begin by showing the decidability of the $W$-extensions of $\mathbb{Q}$ before explaining how one could generalise this to the situation of $W^+$-extensions of $\mathbb{Q}$. There are two main steps involved in showing that the $W$-extensions are decidability – we aim to show that the theory of $W$-extensions of $\mathbb{Q}$ is complete and then argue that this theory can be recursively axiomatised. Notice that if we can show that the theory of $W$-extensions of $\mathbb{Q}$ is complete, then any two distinct $W$-extensions, $K$ and $K'$, of $\mathbb{Q}$ are "model-theoretically" equivalent, i.e. there is no first-order way of telling apart $K$ from $K'$, and hence, as far as first-order logic is concerned, $W$-extensions of $\mathbb{Q}$ are ("model-theoretically") unique. This is in stark contrast to the fact that "algebraically", $K$ and $K'$ are distinct (they are not isomorphic to one another) due to the uniqueness of the embeddings of $K$ and $K'$ into $\mathbb{Q}_p$ for all primes $p$ as mentioned previously.

We first point out that many of the properties that we had described in our exposition above are actually first-order expressible.

**Observation 3.2.24** (Some Elementary Statements)**.** *The following statements can be expressed in a first-order manner:*

1. *$R$ is a Prüfer ring;*
2. *$R$ is a Bézout ring;*
3. *$R$ is a B-ring;*
4. *$R$ is an NB-ring;*

5. *All valuation rings $R_i \in W(R)$ have an absolute ramification index less than or equal to $n$;*

6. *Local properties for a near-Boolean family $W(R)$ are near-continuous;*

7. *$K$ is dense in $\mathbb{H}_{R_i}(K)$ for any $R_i \in W(R)$;*

8. *The family $W(R)$ satisfies property $(\mathtt{LG_A})$ (similarly, property $(\mathtt{LG_A^+})$);*

9. *The family $W(R)$ satisfies property $(\mathtt{M}^+)$ (similarly, property $(\mathtt{M}^+)$).*

*Proof.*

1. That $R$ is a Prüfer ring can be expressed by the following statement:

$$\forall x_0\ \forall x_1\ \exists y_0\ \exists y_1\ \exists z\ \ \left(z = x_0y_0 + x_1y_1\ \wedge\ \left(\bigwedge_{i,j=0,1} \exists u\ (zu = x_iy_j)\right)\right).$$

2. It suffices to express the statement that any two-generated ideal is principal, and this can be done so:

$$\forall x\ \forall y\ \exists z\ \ (\forall w\ (\exists a\ \exists b\ \ (w = ax + by) \rightarrow \exists u\ (w = uz))).$$

3. We had seen that a Prüfer ring $R$ is a B-ring if the quotient $\overline{R} = R/J(R)$ is a von Neumann regular ring. Statement (1) above tells us we can express that $R$ is a Prüfer ring in a first-order way. We can define the Jacobson radical $J(R)$ of the ring $R$ (within $R$) in the following way: $m \in J(R)$ if and only if $\forall x\ (1 - mx) \in U(R)$, where $U(R)$ is the set of invertible elements of $R$. Note that $U(R)$ is also definable in $R$ – indeed $u \in U(R)$ if and only if $\exists v\ (u \cdot v) = (v \cdot u) = 1$. We are thus able to express the elements of the quotient ring $\overline{R}$ (and hence $\overline{R}$ is also definable). We need to say that $\overline{R}$ is a von Neumann regular ring and this statement is clearly elementary, expressed by $\forall x \in \overline{R}\ \ \exists y \in \overline{R}\ \ (x^2y = x)$.

4. Note that we can express the notion that $R$ is a valuation ring by saying that $R$ is a commutative ring such that $\forall a\ \forall b\ \exists c\,((a = b \cdot c) \vee (b = a \cdot c))$ (cf. property 3 of Observation (3.1.2)). If $R$ is not a valuation ring, then $R$ is an NB-ring if and only if $M(R) = R \setminus (U(R) \cup J(R)) \neq \varnothing$, and for all $a \in M(R)$, the ring $R_a = S_a^{-1}R$ is a B-ring. As we had seen $U(R)$ and $J(R)$ are both definable in $R$, so $M(R)$ is definable in $R$ too. The set $S_a$ is definable in $R$ using the parameter $a$ – indeed $b \in S_a$ if and only if $\exists x\ \exists y\ \ (a \cdot x + b \cdot y = 1)$ (cf. Definition 3.1.31). Hence $R_a$ is definable using the parameter $a$ and the statement that $R_a$ is a B-ring can be expressed in a first-order manner by statement 3 above.

5. This statement can be expressed by an infinite set of sentences: for every prime $p$,

$$\forall d\ \forall x\ \ \Big(d \in R\ \wedge\ d \neq 0\ \wedge\ x \in J(R_d) \longrightarrow x^n p^{-1} \in R_d\Big)\,,$$

where $R_d = S_d^{-1}R = R_{W_d}$ (cf. Remark 3.1.30) and $J(R_d)$ is the Jacobson radical for the ring $R_d$.

6. This is established via Theorem 4.6.1 of [Ers01b].

7. This is established via Proposition 1.6.1 of [Ers01b].

8. This is an immediate consequence of Proposition 3.2.11 after noting that the statements "$W(R)$ is independent" and "$R$ possesses property ($\mathtt{HR}_{\leq}$)" are elementary. Indeed, the statement "$W(R)$ is independent" can be expressed by the following (equivalent) statement: for any $s, t, \varepsilon \in R \setminus \{0\}$, if we have that the ideal generated by $s$ and $t$ is not proper, i.e. $(s,t)_R = R$, then there is an element $k \in K$ such that $(1-k)\varepsilon^{-1} \in R_s = S_s^{-1}R$ and $k\varepsilon^{-1} \in R_t = S_t^{-1}R$. "$R$ possesses property ($\mathtt{HR}_{\leq}$)" can be expressed by an (infinite) set of sentences $\varphi_{HR_{\leq,N}}$ for $N > 1$ where $\varphi_{HR_{\leq,N}}$ describes property ($\mathtt{HR}_{\leq}$) for polynomials $f, g, h_i, i < k, k \leq N, n \leq N$, such that the degree of the polynomials $f, g, h_i$ in each variable $x, y_0, \ldots, y_{k-1}$ does not exceed $N$ (cf. Theorem 3.3.1 of [Ers01b]).

9. This is established via Lemma 4.6.1 of [Ers01b].

□

As with the model-theoretic study of most classes of fields that satisfy a certain local-global principle, we now aim to classify these $W$-extensions of $\mathbb{Q}$ by certain invariants, notably those that encode the way in which the different topologies involved interact with one another. In order to make this precise, we will introduce the notion of an $E$-lattice – a certain distributive lattice with relative complements and a least element – and an enrichment of such lattices by a Boolean algebra (more precisely, by the Lindenbaum-Tarski algebra) called the $B$-enrichment of these $E$-lattices. As it turns out, the question of elementary equivalence of these enriched lattices (which are definable within the $W$-extensions) determines the elementary equivalence of the corresponding $W$-extensions and is considerably easier to deal with rather than having to directly deal with the question of the elementary equivalence of those $W$-extensions themselves. An analysis of such enriched lattices would then allow us to conclude that any two $W$-extensions of $\mathbb{Q}$ are elementarily equivalent, and hence, that the elementary theory of the class of all $W$-extensions of $\mathbb{Q}$ is, in fact, complete. One can then deduce the decidability of such $W$-extensions by showing that the axiomatisation of the theory of these extensions also happens to be recursive.

Let $W$ be a near-Boolean family of valuation rings and let the associated ***E*-lattice**, denoted by $E(W) := \{W_A \mid A \subseteq_{\text{finite}} R_W \setminus \{0\}\}$, be the set of all subsets of $W$ that are open-closed and compact in the Constructive topology (cf. Remark 3.1.30). Note that, in this case, $W_A$ is Boolean. If $R$ is an NB-ring and $W(R)$ is the corresponding near-Boolean family of valuation rings, then we use the notation $E(R)$ for brevity, instead of the notation $E(W(R))$, to refer to the associated $E$-lattice of the near-Boolean family of valuation rings. We first aim to show that $E(R)$ is indeed definable in $R$, and hence within the $W$-extension $\langle K = q(R), R\rangle$ itself.

**Lemma 3.2.25.** *Let $R$ be an NB-ring and $a, b, c \in R \setminus \{0\}$. Then there exists a $d \in R \setminus \{0\}$ such that $(a, b, c)_R = (c, d)_R$*

*Proof.* Let $R_c = S_c^{-1}R$. Since $R$ is an NB-ring, $R_c$ is a B-ring. Since every B-ring is a Bézout ring (cf. Proposition 2.4.4 of [Ers01b]), we have that $R_c$ is a Bézout ring as well. Hence, there is some element $d \in R_c \setminus \{0\}$ such that $(a, b)_{R_c} = (d)_{R_c}$. Since $d \in R_c \setminus \{0\}$, we can rewrite $d$ as $d = s^{-1}d_0$ for some $s \in S_c$ and $d_0 \in R \setminus \{0\}$. Thus we have that the principle ideal of $R_c$ generated by $d$ is the same as that generated by $d_0$, i.e. $(d)_{R_c} = (d_0)_{R_c}$, and so we can, without any loss of generality, simply assume that $d \in R \setminus \{0\}$.

Now, since $(a, b)_{R_c} = (d)_{R_c}$, we have $ua + vb = d$ for some $u, v \in R_c$. Pick an $s \in S_c$ such that $us, vs \in R$. Thus, $usa + vsb = ds \in (a, b)_R$. Given such an $s \in S_c$, we can find $m, n \in R$ such that $cm + sn = 1$. We thus have $d = (cm + sn)d = cmd + snd = cmd + (usa + vsb)n = (usn)a + (vsn)b + (md)c \in (a, b, c)_R$. We therefore have that $(c, d)_R \leq (a, b, c)_R$.

For the reverse inclusion, notice that since $(a, b)_{R_c} = (d)_{R_c}$, there exists some $u \in R_c$ such that $a = ud$. Let $s \in S_c$ be such that $us \in R$. Then $sa = usd \in (d)_R$. Again, since $s \in S_c$, there exist $m, n \in R$ such that $cm + sn = 1$, and so $a = (cm + sn)a = c(ma) + sa(n) \in (c, d)_R$. In a similar fashion, we get that $b \in (c, d)_R$. Thus, $(a, b, c)_R \leq (c, d)_R$. □

**Corollary 3.2.26.** *Suppose $R$ is an NB-ring. Then, for every finite subset $A \subseteq R \setminus \{0\}$, there are $a, b \in R \setminus \{0\}$ such that $W_A = W_{\{a,b\}}$.*

*Proof.* By Lemma 3.2.25, there exist $a, b \in R \setminus \{0\}$ such that $(A)_R = (a, b)_R$. We

thus have the following equalities:

$$\begin{aligned} W_A &= \{R_{\mathfrak{m}} \mid \mathfrak{m} \in m\mathrm{Spec}(R),\ A \subseteq \mathfrak{m}\} \\ &= \{R_{\mathfrak{m}} \mid \mathfrak{m} \in m\mathrm{Spec}(R),\ (A)_R \in \mathfrak{m}\} \\ &= \{R_{\mathfrak{m}} \mid \mathfrak{m} \in m\mathrm{Spec}(R),\ (a,b)_R \in \mathfrak{m}\} \\ &= \{R_{\mathfrak{m}} \mid \mathfrak{m} \in m\mathrm{Spec}(R),\ \{a,b\} \in \mathfrak{m}\} \\ &= W_{\{a,b\}}. \end{aligned}$$

□

**Proposition 3.2.27.** *Let $R$ be an NB-ring. Then the E-lattice, $E(R)$, is definable in $R$.*

*Proof.* Given $R$ an NB-ring, let us consider the corresponding family of valuation rings $W(R)$. Let $A = \{a_i \mid 1 \leq i \leq n\}$ be a finite subset of $R \setminus \{0\}$ and suppose that $S_A = \{s \mid s \in R,\ (A \cup \{s\})_R = R\} \subseteq R$. Note that in this case, we have that $W_A = \{R_i \in W(R) \mid A \subseteq \mathfrak{m}_{R_i}\}$. Let $s \in S_A$. Then since we have that $(A \cup \{s\})_R = R$, there exists $u, v_1, v_2, \ldots, v_n \in R$ such that $us + v_1a_1 + v_2a_2 + \cdots + v_na_n = 1$. Note that $s \notin \mathfrak{m}_{R_i}$ for any $R_i \in W_A$ for otherwise, since $A \subseteq \mathfrak{m}_{R_i}$, we will have that $1 = us + v_1a_1 + v_2a_2 + \ldots + v_na_n \in \mathfrak{m}_{R_i}$. Consequently, $s^{-1} \in R_i$ for all $R_i \in W_A$ (cf. Remark 3.1.30), and so $s^{-1} \in R_{W_A} = \bigcap\{R_i \mid R_i \in W_A\}$. We thus have that $S_A^{-1}R \subseteq R_{W_A}$.

Now suppose that $r \in R_{W_A}$, and consider the following set $I_r = \{t \in R \mid rt \in R\} \subseteq R$. Clearly, $I_r$ is an ideal of $R$. Consider the ideal $J = (I_r \cup A)_R$ of $R$ generated by the set $I_r \cup A$. If $J$ is not proper, then there exist $t \in I_r$, $u, v_1, v_2, \ldots, v_n \in R$ such that $ut + a_1v_1 + a_2v_2 + \cdots + a_nv_n = 1$, where $a_i \in A$. Thus, $t \in S_A$, and so we have that $r = t^{-1}(rt) \in S_A^{-1}R$. If, on the other hand, $J$ is proper, then let $\mathfrak{m}$ be a maximal ideal of $R$ containing $J$. Since $J$ is generated by $A \cup I_r$, we have that $A \subseteq J \subseteq \mathfrak{m}$ from whence we can conclude that $R_{\mathfrak{m}} \in W_A$. Thus, we have that $R_{W_A} \subseteq R_{\mathfrak{m}}$, and so $r \in R_{\mathfrak{m}}$. Hence, there exist $x \in R$, and $y \in R \setminus \mathfrak{m}$ such that $r = \frac{x}{y}$. We then have that $ry = x \in R$ and so $y \in I_r$. However, since $I_r \subseteq J \subseteq \mathfrak{m}$, we have that $y \in \mathfrak{m}$, a contradiction. Thus, $J$ cannot be proper, and so we have

that $R_{W_A} \subseteq S_A^{-1}R$. We can thus conclude that $R_{W_A} = S_A^{-1}R$.

We therefore have the following equivalence:

$$W_A \subseteq W_B \text{ if and only if } S_B^{-1}R \subseteq S_A^{-1}R \text{ if and only if } S_B \subseteq S_A.$$

By Corollary 3.2.26, we thus know that the families $W_{\{a,b\}}$ exhaust all possible elements of $E(R)$. We can therefore express $E(R)$ in terms of the pairs $\langle a, b\rangle$ and the relations $W_{\{a,b\}} \subseteq W_{\{c,d\}}$. Note that the latter relations are definable since they are equivalent to the relations $S_{\{c,d\}} \subseteq S_{\{a,b\}}$ which are easily definable. □

Note that if $(A)_R = (a)_R$ and $(B)_R = (b)_R$ for some finite subset $A$ and $B$ of $R \setminus \{0\}$ and $a, b \in R\setminus\{0\}$ – as it is in the case when $R$ is a Bézout ring – then we get that

$$W_a \subseteq W_b \text{ if and only if } S_b \subseteq S_a.$$

Here, we can define a transitive relation, $\sqsubseteq_R$, in the following manner:

$$a \sqsubseteq_R b \text{ if and only if } S_b \subseteq S_a.$$

Note that since $S_a = \{c \in R \mid (a, c)_R = R\}$, we can equivalently say that $a \sqsubseteq_R b$ if and only if the following statement holds:

$$\forall c\ (\exists x_1\ \exists y_1\ (bx_1 + cy_1 = 1) \to \exists x_2\ \exists y_2\ (ax_2 + cy_2 = 1))\,.$$

We can further define the relation $\equiv_R$ as follows:

$$a \equiv_R b \text{ if and only if } a \sqsubseteq_R b \text{ and } b \sqsubseteq_R a.$$

The relation $\sqsubseteq_R$ induces a partial order $\sqsubseteq$ on the quotient set $L_R = R/\equiv_R$.

**Remark 3.2.28.** *The relation $\sqsubseteq_R$ corresponds to the **radical relation** on $R$ defined by the family of maximal ideals, as introduced by Prestel and Schmid in [PS90]. Indeed, $a \sqsubseteq_R b$ holds in $R$ if and only if for any maximal ideal $\mathfrak{m}$ of $R$, if $a \in \mathfrak{m}$, then $b \in \mathfrak{m}$.*

*For suppose $a \sqsubseteq_R b$ holds in $R$ and for a maximal ideal $\mathfrak{m}$ of $R$, we have that $a \in \mathfrak{m}$. If $b \notin \mathfrak{m}$, then the smallest ideal containing both $b$ and $\mathfrak{m}$ is the whole ring. Hence, there exists a $c \in R$ such that $1 = bc + \mathfrak{m}$, i.e. there is some $m \in \mathfrak{m}$ such that $m = 1 - bc$. Thus, we have that $1 = bc + m$ and hence $m \in S_b$. Since $a \sqsubseteq_R b$, we have that $S_b \subseteq S_a$, and thus, $m \in S_a$ as well. However, since $a, m \in \mathfrak{m}$, the ideal generated by $a$ and $m$, $(a, m)_R \subseteq \mathfrak{m} \subsetneq R$ and hence $m \notin S_a$, a contradiction. Thus $b \in \mathfrak{m}$.*

*Conversely, suppose $\mathfrak{m}$ is any maximal ideal of $R$ and that if $a \in \mathfrak{m}$, we have that $b \in \mathfrak{m}$. We want to show that $S_b \subseteq S_a$. We thus suppose that $c \in S_b$. In this case, $(b, c)_R = R$. Suppose to the contrary that $(a, c)_R \neq R$. Then there exists some maximal ideal $\mathfrak{m}$ such that $(a, c)_R \subseteq \mathfrak{m} \subsetneq R$. Since we have that $a \in \mathfrak{m}$, we thus have that $b \in \mathfrak{m}$, and so $(b, c)_R \subseteq \mathfrak{m} \subsetneq R$ which implies that $c \notin S_b$, contradicting our assumption.*

Let $R$ be a Bézout ring and consider the lattice $\langle L_R, \sqsubseteq \rangle$. For any $a \in R$, let $[a]_R$ denote an element of $L_R$ containing $a$. Note that the lattice $\langle L_R, \sqsubseteq \rangle$ is, in fact, an upper semilattice, i.e. for any $[a]_R, [b]_R \in L_R$, $[a]_R \sqsubseteq [b]_R$ whenever $[a]_R \vee [b]_R = [b]_R$. By Remark 3.1.32, it is clear to see that $[1]_R = [u]_R$ if and only if $u \in U(R)$. We point out further that for any $[a]_R, [b]_R \in L_R$ the element $[ab]_R$ is indeed the least upper bound of the elements $[a]_R$ and $[b]_R$ in $\langle L_R, \sqsubseteq \rangle$, i.e. $[a]_R \vee [b]_R = [ab]_R$. It is clear to see that $[0]_R$ is the largest element and $[1]_R$ is the least element of $\langle L_R, \sqsubseteq \rangle$. Note that if $(c)_R = (a, b)_R$, we have that $[a]_R \wedge [b]_R = [c]_R$. We further point out that $S_a = \{b \in R \mid (a, b)_R = R = (1)_R\} = \{b \in R \mid [a]_R \wedge [b]_R = [1]_R\}$. By Proposition 2.3.11 of [Ers01b], it follows that $\langle L_R, \sqsubseteq \rangle$ is, in fact, isomorphic to $\mathbb{E}(R) := \langle E(R), \wedge, \vee, \perp \rangle$, where $E(R) = \{W_a \mid a \in R \setminus \{0\}\}$. We will henceforth refer to the structure $\mathbb{E}(R)$ as the $E$-lattice of the Bézout ring $R$.

Suppose $B$ is some Boolean algebra and $\mathbb{E}(R)$ an $E$-lattice. We call the system $\langle E(R), \wedge, \vee, \perp, T_b \mid b \in B \rangle$ a ***B*-enrichment of the *E*-lattice** if it satisfies the following conditions:

- for every $b \in B$, $T_b \subseteq E(R)$ is an ideal of the $E$-lattice;
- $T_0 = \{\bot\}$ where 0 is the least element of $B$;
- $T_1 = E(R)$ where 1 is the greatest element of $B$;
- for every $a, b \in B$, $T_{a \wedge b} = T_a \cap T_b$;
- for every $a, b \in B$, $T_{a \vee b} = T_a \vee T_b = \{c \vee d \mid c \in T_a,\ d \in T_b\}$.

Suppose $R$ is a Bézout ring and let $K = q(R)$ be the corresponding field of fractions of $R$. Denote by $K^{\text{alg}}$ the algebraic closure of the field $\mathbb{Q}$ in $K$, and let $A$ be the integral closure of the ring $\mathbb{Z}$ in $K^{\text{alg}}$. Let $\varphi(x_1, x_2, \ldots, x_n)$ be an arbitrary formula in $\mathscr{L}_{\text{ring}}$, $\psi(x_1, x_2, \ldots, x_n)$ be an arbitrary formula in the language of linearly ordered groups $\mathscr{L}_{\log} = \{0\ ;\ +, -\ ;\ \leq\}$, and suppose further that $a_1, a_2, \ldots, a_n \in A \setminus \{0\}$. We define the sets

$$T_{\varphi(\overline{x});\overline{a}} := \{[r]_R \mid r \in R \setminus \{0\},\ \forall R_i \in W_r\ (K_{R_i} \models \varphi(\overline{a} + \mathfrak{m}_{R_i}))\}$$

and

$$T_{\psi(\overline{x});\overline{a}} := \{[r]_R \mid r \in R \setminus \{0\},\ \forall R_i \in W_r\ (\Gamma_{R_i} \models \psi(\upsilon_{R_i}(\overline{a})))\}.$$

One can easily check that $T_{\varphi(\overline{x});\overline{a}}$ and $T_{\psi(\overline{x});\overline{a}}$ are ideals of the $E$-lattice $E(R)$ and that the following relations hold for any $\varphi_1(\overline{x}), \varphi_2(\overline{x})$ formulae in $\mathscr{L}_{\text{ring}}$ and $\psi_1(\overline{x}), \psi_2(\overline{x})$ formulae in $\mathscr{L}_{\log}$:

1. $T_{\varphi_1(\overline{x});\overline{a}} \cap T_{\varphi_2(\overline{x});\overline{a}} = T_{\varphi_1(\overline{x}) \wedge \varphi_2(\overline{x});\overline{a}}$, and similarly,
   $T_{\psi_1(\overline{x});\overline{a}} \cap T_{\psi_2(\overline{x});\overline{a}} = T_{\psi_1(\overline{x}) \wedge \psi_2(\overline{x});\overline{a}}$;
2. $T_{\varphi_1(\overline{x});\overline{a}} \vee T_{\varphi_2(\overline{x});\overline{a}} = T_{\varphi_1(\overline{x}) \vee \varphi_2(\overline{x});\overline{a}}$, and similarly,
   $T_{\psi_1(\overline{x});\overline{a}} \vee T_{\psi_2(\overline{x});\overline{a}} = T_{\psi_1(\overline{x}) \vee \psi_2(\overline{x});\overline{a}}$;
3. $T_{\varphi_1(\overline{x});\overline{a}} \cap T_{\neg\varphi_1(\overline{x});\overline{a}} = \{\bot\} = \{[1]_R\}$, and similarly,
   $T_{\psi_1(\overline{x});\overline{a}} \cap T_{\neg\psi_1(\overline{x});\overline{a}} = \{\bot\} = \{[1]_R\}$;
4. $T_{\varphi_1(\overline{x});\overline{a}} \vee T_{\neg\varphi_1(\overline{x});\overline{a}} = E(R)$, and similarly,
   $T_{\psi_1(\overline{x});\overline{a}} \vee T_{\neg\psi_1(\overline{x});\overline{a}} = E(R)$.

We can thus regard the system

$$\mathbb{E}_{A\setminus\{0\}}(K) := \langle \mathbb{E}(R), T_{\Phi(\overline{x}),\overline{a}} \mid \Phi(\overline{x}) \in \texttt{Formulae}_{\mathscr{L}_{\text{ring}}\cup\mathscr{L}_{\log}},\ \overline{a} \in (A\setminus\{0\})^n \rangle$$

as a $B$-enriched lattice where $B$ is the Lindenbaum-Tarski algebra. We will henceforth refer to the system $\mathbb{E}_{A\setminus\{0\}}(K)$ as the **$(A\setminus\{0\})$-expansion of $K$**.

**Remark 3.2.29.** *Given the above set-up, one can also say that the multi-valued field $\langle K, R\rangle$ is a $W$-extension of $\langle \mathbb{Q}, \mathbb{Z}\rangle$ if the extension $\langle \mathbb{Q}, \mathbb{Z}\rangle \leq \langle K, R\rangle$ induces an elementary embedding $\mathbb{E}_{\mathbb{Z}\setminus\{0\}}(\mathbb{Q}) \preccurlyeq \mathbb{E}_{\mathbb{Z}\setminus\{0\}}(K)$.*

The following theorem allows us to deduce the elementary equivalence of two multi-valued fields satisfying the conditions stated in Remark 3.2.14 based on the elementary equivalence of their corresponding $(A\setminus\{0\})$-expansions.

**Theorem 3.2.30** (cf. Theorem 5 of [Ers02a])**.** *Suppose $\langle K_1, R_1\rangle$ and $\langle K_2, R_2\rangle$ are two multi-valued fields satisfying conditions (1) to (4) of Remark* 3.2.14 *as well as the conditions that $W(R_j)$ satisfies property* ($\texttt{LG}_\texttt{A}$) *and property* (M) *for $j = 1, 2$. Suppose that $K$ is a common subfield of the fields $K_1$ and $K_2$, $K$ is algebraically closed in $K_1$, and that $R$ is a common subring of $R_1$ and $R_2$ such that $q(R) = K$. Suppose further that for any $R_{1,i} \in W(R_1)$, $R^* := R_{1,i} \cap K = R_{\mathfrak{m}_{R_{1,i}}\cap R}$, $K_{R_{1,i}}$ is a separable extension of $K_{R^*}$, and $\Gamma_{R^*}$ is a pure subgroup of $\Gamma_{R_{1,i}}$. If the $(R\setminus\{0\})$-expansions $\mathbb{E}_{R\setminus\{0\}}(K_1)$ and $\mathbb{E}_{R\setminus\{0\}}(K_2)$ are elementarily equivalent, then $\langle K_1, R_1\rangle$ and $\langle K_2, R_2\rangle$ are elementarily equivalent.*

Suppose that $\langle K_1, R_1\rangle$ and $\langle K_2, R_2\rangle$ are two $W$-extensions of $\mathbb{Q}$. We had noted earlier that $\mathbb{Q}$ is algebraically closed in $K_1$ (and $K_2$) by the maximality property. Thus, in this particular case, we have that $\text{Abs}(K_1) = \mathbb{Q}$. Let us therefore take $K = \mathbb{Q}$ and $R = \mathbb{Z}$. Notice that all the conditions of Theorem 3.2.30 are indeed satisfied – the condition on the elementary equivalence of the $(\mathbb{Z}\setminus\{0\})$-expansions of $K_1$ and $K_2$ is satisfied in light of Remark 3.2.29. Hence, any two $W$-extensions of $\mathbb{Q}$ are indeed elementarily equivalent.

**Remark 3.2.31.** *In fact, if $\langle K_1, R_1\rangle$ and $\langle K_2, R_2\rangle$ are two $W$-extensions of $\mathbb{Q}$ such that $\langle K_1, R_1\rangle \leq \langle K_2, R_2\rangle$, then the extension is elementary. We therefore have a means of constructing uncountable $W$-extensions of $\mathbb{Q}$ from our countable e-closed immediate extension of $\mathbb{Z}$ (cf. Corollary 3.2.13) via the Upward Löwenheim-Skolem Theorem.*

By virtue of these, we have the following:

**Corollary 3.2.32.** *The elementary theory of $W$-extensions of $\mathbb{Q}$ is complete.*

That the elementary theory of (the class of all) $W$-extensions of $\mathbb{Q}$ is decidable now follows from Corollary 3.2.32 and the following axiomatisation of the theory of a $W$-extension $\langle K, R\rangle$ of $\mathbb{Q}$, which by Theorem 2 of [Ers02b], is known to be recursively enumerable:

1. the theory of multi-valued fields with near-Boolean families of quasi-classical valuation rings satisfying a corresponding maximality condition – that this theory is decidable is the main theorem of [Ers02b];

2. the set of sentences

$$N(\mathbb{Q}) := \{\forall x\ (h(x) \neq 0) \mid h \in \mathbb{Z}[x] \text{ is a monic polynomial such that } \mathbb{Q} \models \forall x\ (h(x) \neq 0)\};\ \text{and}$$

3. the elementary characteristics $\chi(\varphi, \psi, \overline{a})$ for the ideals $T_{\varphi;\overline{a}} \cap T_{\psi;\overline{a}}$ of $E(R)$, where $\varphi(\overline{x}) \in \texttt{Formulae}_{\mathscr{L}_{\text{ring}}}$, $\psi(\overline{x}) \in \texttt{Formulae}_{\mathscr{L}_{\log}}$ and $\overline{a} \in \mathbb{Z} \setminus \{0\}$ – this is determined by asking, for any arbitrary sentence $\phi \in \mathscr{L}_{\text{ring}} \cup \{\mathcal{R}'\}$ where $\mathcal{R}'$ is a one place predicate distinguishing a valuation ring, whether the set

$$\mathscr{P}_\phi := \{p \mid p \text{ is a prime number and } \langle \mathbb{Q}_p, \mathbb{Z}_p\rangle \models \phi\}$$

is finite or infinite, and how many element it contains if the set is finite.

**Theorem 3.2.33.** *The elementary theory of the class of all $W$-extensions (alternatively, the elementary theory of an arbitrary $W$-extension) of $\mathbb{Q}$ is decidable.*

For the purposes of constructing a counterexample to answer Question (1.1.1) negatively, we point out that it suffices for us to simply consider $W$-extensions of $\mathbb{Q}$ as suitable base fields. We note that $W^+$-extensions, otherwise known as wonderful extensions, of $\mathbb{Q}$ would likewise make suitable base fields, and we briefly describe how one achieves a similar decidability result for them in what follows. In order to address the decidability of wonderful extensions of $\mathbb{Q}$, we will likewise need a theorem that establishes the fact that the elementary theory of $W^+$-extensions of $\mathbb{Q}$ is complete, and that the axiomatisation of such fields are indeed recursive. Just as we had introduced a $(A \setminus \{0\})$-expansion of a $W$-extension $K$ of $\mathbb{Q}$, we will need to introduce a Boolean lattice to deal with the preordering. Towards this end, recall that for a preordered field $\langle K, P\rangle$, and $a_i \in K\setminus\{0\}$, the set $P_{a_i} = \{x+a_iy \mid x, y \in P\}$ is a preorder of the field $K$ and $\mathfrak{X}(P_{a_i}) = W^+_{a_i} \subseteq \mathfrak{X}(P)$. We can then define an elementary preorder $\sqsubseteq^+$ on $K \setminus \{0\}$ as follows:

$$a \sqsubseteq^+ b \text{ if and only if } P_b \subseteq P_a \text{ if and only if } W^+_a \subseteq W^+_b.$$

For a SAP field $\langle K, P\rangle$, the factorisation $B(P) := \langle (K \setminus \{0\}) / \equiv^+, \sqsubseteq\rangle$ of the preordered set $\langle K \setminus \{0\}, \sqsubseteq^+\rangle$ modulo the equivalence relation $\equiv^+$ (which is defined as $a \equiv^+ b$ if and only if $a \sqsubseteq^+ b$ and $b \sqsubseteq^+ a$ for all $a, b \in K \setminus \{0\}$) is a Boolean lattice isomorphic to the Boolean lattice $B(\mathfrak{X}(P))$ of clopen subsets of the Boolean space $\mathfrak{X}(P)$.

Let $R$ be a NB-ring and $\langle K, R, P\rangle$ be a preordered multi-valued field in which the following condition ($\mathtt{PMV}_k$) holds: there exists some $k > 1$ a positive integer such that for any $R_i \in W(R)$,

$$\mathbb{H}_{R_i}(K) \models \forall x\, \exists y_1\, \exists y_2\, \ldots\, \exists y_k \left(x = \sum_{1\leq i\leq k} y_i^2\right).$$

The following theorem then establishes an analogue of Theorem 3.2.30:

**Theorem 3.2.34** (cf. Theorem 7 of [Ers02c])**.** *Suppose $\langle K_1, R_1, P_1\rangle$ and $\langle K_2, R_2, P_2\rangle$ are two preordered multi-valued fields satisfying condition ($\mathtt{PMV}_k$) for a suitable $k > 1$ such that $\langle K_1, R_1\rangle$ and $\langle K_2, R_2\rangle$ satisfy conditions (1) to (4) of Remark* 3.2.14*,*

*as well as the conditions that $W(R_j)$ satisfies property $(\mathtt{LG}_{\mathtt{A}}^{+})$ and property $(\mathtt{M}^{+})$ for $j = 1, 2$. Suppose that $K$ is a common subfield of the fields $K_1$ and $K_2$, $K$ is algebraically closed in $K_1$, and that $R$ is a common subring of $R_1$ and $R_2$ such that $q(R) = K$. Suppose further that for any $R_{1,i} \in W(R_1)$, $R^* := R_{1,i} \cap K = R_{\mathfrak{m}_{R_{1,i}} \cap R}$, $K_{R_{1,i}}$ is a separable extension of $K_{R^*}$, and $\Gamma_{R^*}$ is a pure subgroup of $\Gamma_{R_{1,i}}$. If the $(R \setminus \{0\})$-expansions $\mathbb{E}_{R\setminus\{0\}}(K_1)$ and $\mathbb{E}_{R\setminus\{0\}}(K_2)$ are elementarily equivalent and $B(P_1)$ is elementarily equivalent to $B(P_2)$, then $\langle K_1, R_1, P_1\rangle$ and $\langle K_2, R_2, P_2\rangle$ are elementarily equivalent.*

**Remark 3.2.35.** *Just as we had previously provided an alternate characterisation of $W$-extensions of $\mathbb{Q}$ in terms of the corresponding $(\mathbb{Z} \setminus \{0\})$-expansions (cf. Remark 3.2.29), one can also say that the preordered multi-valued field $\langle K, R, P\rangle$ is a wonderful extension of $\langle \mathbb{Q}, \mathbb{Z}, P_{\mathbb{Q}}\rangle$ if the extension $\langle \mathbb{Q}, \mathbb{Z}, P_{\mathbb{Q}}\rangle \leq \langle K, R, P\rangle$ induces an elementary embedding $\mathbb{E}_{\mathbb{Z}\setminus\{0\}}(\mathbb{Q}) \preccurlyeq \mathbb{E}_{\mathbb{Z}\setminus\{0\}}(K)$ and $B(P_{\mathbb{Q}}) \preccurlyeq B(P)$.*

Again, it is clear to see that all of the conditions of Theorem 3.2.34 are satisfied when we consider two wonderful extensions of $\mathbb{Q}$, and hence we can conclude that:

**Corollary 3.2.36.** *The elementary theory of $W^+$-extensions of $\mathbb{Q}$ is complete.*

The decidability of these $W^+$-extensions of $\mathbb{Q}$ then follows from Corollary 3.2.36, and the fact that the theory of $W^+$-extensions of $\mathbb{Q}$ is indeed recursively axiomatisable – this can be established analogously in a similar fashion as expressed above, taking into account the embedding into $\mathbb{R}$.

**Theorem 3.2.37** (cf. Theorem 3 of [Ers00])**.** *The elementary theory of the class of all wonderful extensions (alternatively, the elementary theory of an arbitrary wonderful extension) of $\mathbb{Q}$ is decidable.*

## 3.3 The Undecidability of Finite Extensions of Wonderful Extensions of $\mathbb{Q}$

Thus far, we have seen that $W$-extensions (and $W^+$-extensions) of $\mathbb{Q}$ are decidable. In this section, we will attempt to show that sufficiently saturated extensions of

such fields are indeed the kinds of fields that would allow us to provide a definitive solution to Question (1.1.1) in the negative, by constructing a finite extension of a sufficiently saturated extension of a $W$-extension (alternatively, a $W^+$-extension) that happens to be undecidable. As we had pointed out in Section 2.2.2, in order to show the undecidability of such finite extensions, it suffices to exhibit the existence of some appropriate Boolean independent set $\Upsilon$ that satisfies Criterion 2.2.2. We begin by first describing what this appropriate Boolean independent set should be.

Throughout this section, we fix the following convention: Let $R$ be an NB-ring and $K = q(R)$ be the corresponding field of fractions such that $\langle K, R\rangle$ is a sufficiently saturated extension of a $W$-extension of $\langle \mathbb{Q}, \mathbb{Z}\rangle$. Suppose further that $L$ is a quadratic extension of $K$. Now, since $K$ is a $W$-extension of $\mathbb{Q}$, we note that there exist embeddings $\lambda_p : K \to \mathbb{Q}_p$ for all $p \in \mathbb{P}$ which, in turn, induce unique valuations $\upsilon_p$ on $K$ for each $p \in \mathbb{P}$ – the corresponding valuation rings of $K$ being $R_p = \lambda_p^{-1}(\mathbb{Z}_p)$ for all (rational) primes $p$. For every $R_p$ a valuation ring of $K$, there exists at least one valuation ring $S_{\mathfrak{p}_i}$ of $L$ which **lies above** $R_p$, i.e. the ring $S_{\mathfrak{p}_i}$ dominates $R_p$. In this case, we also say that the prime $\mathfrak{p}_i$ of $L$ **lies above** the prime $p$ of $K$. For any quadratic extension $L$ of $K$, one of two situations can occur: for a fixed prime $p$, there can either be exactly one valuation ring $S_{\mathfrak{p}_1} = S_{\mathfrak{p}}$ of $L$ that dominates $R_p$ or two valuation rings $S_{\mathfrak{p}_1}$ and $S_{\mathfrak{p}_2}$ of $L$ that dominate $R_p$. Note that for a prime $q \neq p$, the number of valuation rings of $L$ that dominate $R_q$ is not dependent on the number of valuation rings of $L$ that dominate $R_p$ – indeed for $p \neq q$, we can either have that

1. there exists exactly one valuation ring $S_{\mathfrak{p}}$ of $L$ that dominates $R_p$ of $K$ and exactly one valuation ring $S_{\mathfrak{q}}$ of $L$ that dominates $R_q$ of $K$; or

2. there exists exactly one valuation ring $S_{\mathfrak{p}}$ of $L$ that dominates $R_p$ of $K$ while there are two valuation rings $S_{\mathfrak{q}_1}$ and $S_{\mathfrak{q}_2}$ of $L$ that dominate $R_q$; or

3. there exists exactly one valuation ring $S_{\mathfrak{q}}$ of $L$ that dominates $R_q$ of $K$ while there are two valuation rings $S_{\mathfrak{p}_1}$ and $S_{\mathfrak{p}_2}$ of $L$ that dominate $R_p$; or

4. there are two valuation rings $S_{\mathfrak{p}_1}$ and $S_{\mathfrak{p}_2}$ of $L$ that dominate $R_p$ and there are two valuation rings $S_{\mathfrak{q}_1}$ and $S_{\mathfrak{q}_2}$ of $L$ that dominate $R_q$.

This demonstrates that if we are able to express the statement "there exists exactly one valuation ring of $L$ that dominates $R_p$" for any prime $p$ as $\varphi_p$ in the language of rings, then we could take the set $\Upsilon = \{\varphi_p \mid p \in \mathbb{P}\}$ to be our desired Boolean independent set. Note that the negation of the above-mentioned statement would be that $L$ has two valuation rings dominating $R_p$ for any prime $p$, and the collection of these negated statements for all primes $p$ would equivalently be a(nother) Boolean independent set. In order to avoid any pathological issues which may arise because of the even prime, we will exclude the even prime and construct $\Upsilon$ with only the odd primes – note that $\Upsilon = \{\varphi_p \mid p \in \mathbb{P} \setminus \{2\}\}$ is still countably infinite and thus would nevertheless satisfy Criterion 2.2.2. In what follows, we will aim to express these statements in the language of rings from whence we can conclude that there exists some undecidable quadratic extension of $K$.

Suppose $K$ is a $W$-extension of $\mathbb{Q}$, $L$ a quadratic extension of $K$, and fix $p \in \mathbb{P} \setminus \{2\}$. Note that $K$ can be viewed as a $p$-valued field. We define the ***p*-adic Kochen operator** of $L$ over $K$ as

$$\gamma_p(x) := \frac{1}{p} \cdot \frac{x^p - x}{(x^p - x)^2 - 1}.$$

We point out that the $p$-adic Kochen operator $\gamma_p(x)$ is indeed expressible using the language of rings. Denote by $R_p[\gamma_p(L)]$ the subring of $L$ generated by $\gamma_p(L) \cup R_p$ where $R_p = \lambda_p^{-1}(\mathbb{Z}_p)$ is the valuation ring of $K$ associated with the prime $p$. The ***p*-adic Kochen ring**, $R^p_{\mathrm{Koc}}(L)$, of $L$ over $K$ is the subring of $L$ defined by

$$R^p_{\mathrm{Koc}}(L) := \left\{ \frac{t}{1 - ps} \;\middle|\; t, s \in R_p[\gamma_p(L)] \text{ and } 1 - ps \neq 0 \right\}.$$

For brevity, we will henceforth use the notation $R^p_{\mathrm{Koc}}$ instead of $R^p_{\mathrm{Koc}}(L)$ whenever it is clear from the context as to which extension of $K$ we are considering. By

Theorem 6.14 of [PR], we know that $R^p_{\text{Koc}}$ is the integral closure of $R_p$ in $L$ and is the intersection of all the valuation rings $S_{\mathfrak{p}_i}$ of $L$ which lie above $R_p$, i.e.

$$R^p_{\text{Koc}} = \bigcap_{R_p \sqsubseteq S_{\mathfrak{p}_i}} S_{\mathfrak{p}_i}.$$

From the above-mentioned theorem, we also know that $S_{\mathfrak{p}_i}$ is the localization of $R^p_{\text{Koc}}$ at some maximal ideal $\mathfrak{m}_i$ of $R^p_{\text{Koc}}$, i.e. $S_{\mathfrak{p}_i} = (R^p_{\text{Koc}})_{\mathfrak{m}_i}$. Hence, it is clear that if there are two distinct valuation rings $S_{\mathfrak{p}_1}$ and $S_{\mathfrak{p}_2}$ of $L$ that lie above $R_p$, then $R^p_{\text{Koc}}$ cannot be a valuation ring – indeed, a valuation ring is a local ring and thus must have a unique maximal ideal. On the other hand, if there is only one valuation ring $S_{\mathfrak{p}}$ of $L$ that lie above $R_p$, then $R^p_{\text{Koc}} = S_{\mathfrak{p}}$ is indeed a valuation ring. Hence, we find another way of expressing the statement "$L$ has only one valuation ring dominating $R_p$" – we simply say the following: "$R^p_{\text{Koc}}$ is a valuation ring". As we had pointed out in the proof of part (4) of Observation (3.2.24), the statement "$R$ is a valuation ring" can be expressed in a first-order manner using the language of rings. Hence, it suffices to define $R^p_{\text{Koc}}$ in $L$ using the language of rings since we would then be able to express the above-mentioned statement that $R^p_{\text{Koc}}$ is a valuation ring in a first-order way.

Towards this end, we begin by claiming that

$$R^p_{\text{Koc}}(L) := \{\gamma_p(x) + \gamma_p(y) + \gamma_p(z) \mid x, y, z \in L\}$$

which would, in turn, imply that $R^p_{\text{Koc}}$ is (existentially) definable in $L$ using the language $\mathscr{L}_{\text{ring}}$. Indeed,

$$l \in R^p_{\text{Koc}} \quad \Longleftrightarrow \quad \exists x\, \exists y\, \exists z \;\; (l = \gamma_p(x) + \gamma_p(y) + \gamma_p(z)).$$

We proceed to prove the claim asserting the above definition of $R^p_{\text{Koc}}$. For any $x, y, z \in L$, the fact that there exists some $l \in R^p_{\text{Koc}}$ such that

$$\gamma_p(x) + \gamma_p(y) + \gamma_p(z) = l$$

follows from Theorem 6.14 of [PR]. It therefore suffices to show that for any $l \in R^p_{\text{Koc}}$, we have the following:

$$l = \gamma_p(x) + \gamma_p(y) + \gamma_p(z) \quad \text{for some } x, y, z \in L.$$

In order to prove this direction, we modify Part C of the proof of Theorem 3.11 in Efrat and Jarden's *Free Pseudo p-adically Closed Fields of Finite Corank* (cf. [EJ90]). The above-mentioned Theorem 3.11 provides necessary and sufficient conditions for a field $K$ to be pseudo $p$-adically closed with $e$ $\Theta$-sites where $e \in \mathbb{N}$ – here, by a $\Theta$-site on a field $K$, we mean a pair $(\pi, \varphi)$ where $\pi$ is a $\mathbb{Q}_p$-place and on $K$ and $\varphi : K \setminus \{0\} \to \varprojlim \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^n$ is a homomorphism such that $\varphi(x) = \pi(x)$ whenever $x \in K \setminus \{0\}$ and $\pi(x) \neq 0, \infty$ (cf. page 134 of [EJ90]).

Let us begin by denoting the $p$-adic valuation of $K$ by $\upsilon_p$, and let us suppose that $\upsilon_{\mathfrak{p}_1}$ and $\upsilon_{\mathfrak{p}_2}$ are the two (possibly non-distinct) valuations of $L$ that extend the $p$-adic valuation of $K$ with valuation rings $S_{\mathfrak{p}_1}$ and $S_{\mathfrak{p}_2}$ respectively. Let us further suppose that $L^{\upsilon_{\mathfrak{p}_1}}$ and $L^{\upsilon_{\mathfrak{p}_2}}$ are the $p$-adic closures of $L$ under $\upsilon_{\mathfrak{p}_1}$ and $\upsilon_{\mathfrak{p}_2}$ respectively, and let their corresponding valuation rings be $\overline{S_{\mathfrak{p}_1}}$ and $\overline{S_{\mathfrak{p}_2}}$ respectively. For any $l \in R^p_{\text{Koc}}$, we have

$$\begin{aligned}
&\gamma_p(x) + \gamma_p(y) + \gamma_p(z) - l \\
&\quad = \frac{x^p - x}{p \cdot ((x^p - x)^2 - 1)} + \frac{y^p - y}{p \cdot ((y^p - y)^2 - 1)} + \frac{z^p - z}{p \cdot ((z^p - z)^2 - 1)} - l \\
&\quad = \frac{(x^p - x) \cdot ((y^p - y)^2 - 1) \cdot ((z^p - z)^2 - 1)}{p \cdot ((x^p - x)^2 - 1) \cdot ((y^p - y)^2 - 1) \cdot ((z^p - z)^2 - 1)} \\
&\qquad + \frac{((x^p - x)^2 - 1) \cdot (y^p - y) \cdot ((z^p - z)^2 - 1)}{p \cdot ((x^p - x)^2 - 1) \cdot ((y^p - y)^2 - 1) \cdot ((z^p - z)^2 - 1)} \\
&\qquad + \frac{((x^p - x)^2 - 1) \cdot ((y^p - y)^2 - 1) \cdot (z^p - z)}{p \cdot ((x^p - x)^2 - 1) \cdot ((y^p - y)^2 - 1) \cdot ((z^p - z)^2 - 1)} \\
&\qquad - \frac{p \cdot l \cdot ((x^p - x)^2 - 1) \cdot ((y^p - y)^2 - 1) \cdot ((z^p - z)^2 - 1)}{p \cdot ((x^p - x)^2 - 1) \cdot ((y^p - y)^2 - 1) \cdot ((z^p - z)^2 - 1)}
\end{aligned}$$

By Hensel's Lemma, we note that the following polynomial has a zero in $\overline{S_{\mathfrak{p}_1}}$ and $\overline{S_{\mathfrak{p}_2}}$:

$$f(X) = p \cdot l \cdot \Big((X^p - X)^2 - 1\Big) - X^p + X.$$

Let $x_1$ and $x_2$ be those zeros in $\overline{S_{\mathfrak{p}_1}}$ and $\overline{S_{\mathfrak{p}_2}}$ respectively. Denote by $G(X,Y,Z)$ the numerator of $\gamma_p(X)+\gamma_p(Y)+\gamma_p(Z)-l$, i.e.

$$\begin{aligned} G(X,Y,Z) = (x^p-x)\cdot\Big((y^p-y)^2-1\Big)\cdot\Big((z^p-z)^2-1\Big) \\ +\Big((x^p-x)^2-1\Big)\cdot(y^p-y)\cdot\Big((z^p-z)^2-1\Big) \\ +\Big((x^p-x)^2-1\Big)\cdot\Big((y^p-y)^2-1\Big)\cdot(z^p-z) \\ -p\cdot l\cdot\Big((x^p-x)^2-1\Big)\cdot\Big((y^p-y)^2-1\Big)\cdot\Big((z^p-z)^2-1\Big) \end{aligned}$$

In *Reducibility of Polynomials in Several Variables II*, Schinzel proves that if $K$ is a field of characteristic 0, $n\geq 3$, and $f_i\in K(x_i)\setminus K$, where $i\in\{1,2,\ldots,n\}$, then $\sum_{i=1}^n f_i$ is irreducible over $K$ (cf. Corollary 1 of [Sch85]). Using this result, we can conclude that $G(X,Y,Z)$ is indeed absolutely irreducible. Note that since $x_1$ is a zero in $\overline{S_{\mathfrak{p}_1}}$, we have that $(x_1,0,0)$ is a $L^{\upsilon_{\mathfrak{p}_1}}$-rational point of $G(X,Y,Z)$. Similarly, $(x_2,0,0)$ is a $L^{\upsilon_{\mathfrak{p}_2}}$-rational point of $G(X,Y,Z)$. We further note that $(x_1,0,0)$ is, in fact, a simple $L^{\upsilon_{\mathfrak{p}_1}}$-rational point of the variety $V(G)$ since

$$\frac{\partial G}{\partial X}(x_1,0,0)\equiv -1 \mod p\overline{S_{\mathfrak{p}_1}}.$$

Note that the same holds, correspondingly, for $(x_2,0,0)$.

We now point out that since $K$ is a wonderful extension of $\mathbb{Q}$ (and therefore satisfies the Local-Global principle as stated in Definition 3.2.1), if we consider the family $S$ of all prolongations of all $p$-adic valuations of $K$ to $L$, then $L$ still satisfies the Local-Global principle for rational points with respect to this family $S$. We point out that for an odd prime $q\neq p$, every element of the $q$-adic completion of $L$ does lie in $R^p_{\mathrm{Koc}}$. Hence, we can conclude that $V(G)$ does, in fact, have an $L$-rational point, say, $(x,y,z)$. Since the denominator of the $p$-Kochen operator does not vanish on a formally $p$-adic field, we must have that $\gamma_p(x)+\gamma_p(y)+\gamma_p(z)-l=0$, from whence we have that

$$R^p_{\mathrm{Koc}}(L)=\{\gamma_p(x)+\gamma_p(y)+\gamma_p(z)\mid x,y,z\in L\}.$$

By defining the $p$-Kochen ring within $L$ in a first-order manner using $\mathscr{L}_{\text{ring}}$, we are able to effectively write a first-order statement to say that "$R^p_{\text{Koc}}$ is a valuation ring". Let $\varphi_p$ be such a statement, i.e. $\varphi_p$ be the sentence in $\mathscr{L}_{\text{ring}}$ that asserts that $R^p_{\text{Koc}}$ is a valuation ring. Now consider the following set $\Upsilon = \{\varphi_p \mid p \in \mathbb{P} \setminus \{2\}\}$. One can readily see that $\Upsilon$ is indeed a Boolean independent set that is realisable in quadratic extensions of a sufficiently saturated extension of $K$, where $K$ is a $W$-extension (alternatively, a $W^+$-extension) of $\mathbb{Q}$. This, in turn, enables us to state the following theorem:

**Theorem 3.3.1.** *There exists a finite extension of a sufficiently saturated extension of a $W$-extension (alternatively, a wonderful extension) of $\mathbb{Q}$ that is undecidable.*

The above theorem therefore allows us to conclude that there is an example of a decidable field which admits an undecidable finite extension. We highlight that we exploited the following facts about $W$-extensions (alternatively, a wonderful extensions) of $\mathbb{Q}$ that allowed us to make this conclusion:

- ***$W$-extensions (alternatively, a wonderful extensions) of $\mathbb{Q}$ are decidable fields***

  As pointed out in Chapter 1, it was necessary to first find a "non-classical" decidable field.

- ***a $W$-extension (alternatively, a wonderful extension) of $\mathbb{Q}$ is a multi-valued field with a family of countably infinitely many valuation rings***

  If one were to take a quadratic extension of a field that admits a valuation ring, then in the extension field, there are either one or two distinct valuation rings that lie above that particular valuation ring. Since $W$-extensions (alternatively, a wonderful extension) of $\mathbb{Q}$ admit countably infinitely many valuation rings, we see that there are essentially $2^{\aleph_0}$ many different possibilities which can arise (two possibilities for each valuation ring of the $W$-extension/ wonderful extension of $\mathbb{Q}$). Further, note that how one prime ramifies in the extension

is not determined by how another distinct prime ramifies, and so these events are clearly independent. Thus, within a sufficiently saturated extension of the $W$-extension/ wonderful extension of $\mathbb{Q}$, one can ensure that all the $2^{\aleph_0}$ many possibilities are realised – i.e. a sufficiently saturated extension of the $W$-extension/ wonderful extension of $\mathbb{Q}$ would admit uncountably many different quadratic extensions, with any quadratic extension differing from another in the way a certain rational odd prime ramifies in them.

- ***the difference between any two quadratic extensions as obtained from the discussion above can be expressed in a first-order manner*** By being able to define the $p$-adic Kochen ring in the language of rings, we were able to express the statement that the $p$-adic Kochen ring is a valuation ring. Depending on how the rational odd prime $p$ ramifies in the extension, this statement would either be true or false in the quadratic extension. This allows us to distinguish any two different quadratic extensions of a sufficiently saturated extension of a $W$-extension/ wonderful extension of $\mathbb{Q}$ in a first-order way – being pairwise elementarily inequivalent means that the uncountably many quadratic extensions result in uncountably many different theories, only countably many of whom can be decidable.

Indeed, in light of our discussions in Subsection 2.2.2, the Cantor-esque counting argument invoked indicates that most of the quadratic extensions of a sufficiently saturated extension of a $W$-extension (or $W^+$-extension) of $\mathbb{Q}$ are undecidable. Notice, however, that while we have shown that such undecidable finite extensions of a decidable field do exist, we had not explicitly provided a concrete example of one such undecidable finite extension. We now aim to provide an explicit construction using the main ideas borrowed from our treatise above.

Let $\mathbb{P}_{\text{nr}}$ be a non-recursive subset of $\mathbb{P} \setminus \{2\}$. Let $K$ be a sufficiently saturated extension of a $W$-extension (alternatively, $W^+$-extension) of $\mathbb{Q}$ such that $\alpha \in K$

realises the type $\varrho(x)$ defined in the following manner:

$$\varrho(x) := \{R^p_{\mathrm{Koc}}(K(\sqrt{x})) \text{ is a valuation ring} \mid p \in \mathbb{P}_{\mathrm{nr}}\} \cup \{R^p_{\mathrm{Koc}}(K(\sqrt{x})) \text{ is not a valuation ring} \mid p \in \mathbb{P} \setminus (\mathbb{P}_{\mathrm{nr}} \cup \{2\})\}.$$

Note that for a prime $q \neq p$, the number of valuation rings of the quadratic extension that dominate $R_q$ is not dependent on the number of valuation rings of quadratic extension that dominate $R_p$. Hence, whether $R^p_{\mathrm{Koc}}(K(\sqrt{x}))$ is a valuation ring is not affected by whether $R^q_{\mathrm{Koc}}(K(\sqrt{x}))$ is a valuation for $p \neq q$, with $p, q \in \mathbb{P} \setminus \{2\}$. Let $L = K(\sqrt{\alpha})$. Then clearly $L$ is an undecidable finite extension of $K$, for otherwise, one would be able to determine the membership of the non-recursive set of primes by checking for which primes the corresponding $p$-adic Kochen ring is a valuation ring. Since $K$ is a sufficiently saturated extension of a $W$-extension (alternatively, a $W^+$-extension) of $\mathbb{Q}$, $K$ is decidable by our exposition in Subsection 3.2.2. Hence, we have constructed an explicit example of a decidable field which has a finite extension that is undecidable, answering Question (1.1.1) in the negative.

*Well, some mathematics problems look simple, and you try them for a year or so, and then you try them for a hundred years, and it turns out that they're extremely hard to solve. There's no reason why these problems shouldn't be easy, and yet they turn out to be extremely intricate.*

— Andrew Wiles

# 4

# Attempts at Constructing a PAC Counterexample

## Contents


**4.1 Modifying Known Counterexamples . . . . . 100**
**4.2 Coding "Undecidability" . . . . . 106**
4.2.1 Addressing Question 1 . . . . . 107
4.2.2 Addressing Question 2 . . . . . 122


While, on hindsight, the choice of $W$-extensions (and, indeed, $W^+$-extensions) of $\mathbb{Q}$ as suitable starting points to investigate in order to construct counterexamples to answer Question (1.1.1) negatively appears rather natural in light of the properties of those fields which we had highlighted at the end of the previous chapter, the path taken to arrive at this result had not always been that straightforward. In this brief final chapter, we aim to outline some of the avenues that were pursued in order to construct a counterexample that would answer Question (1.1.1) negatively.

As was pointed out by Observation (1.2.4), in order for a field $K$ to act as a suitable base field to answer Question (1.1.1) negatively, it must, at the very least, be a decidable "non-classical" field. We had, earlier in this thesis, seen that the class of pseudo alegbraically closed (PAC) fields (cf. Subsection 2.1.2) happen

to be one such class of "non-classical" fields which admit an easily describable decidability criterion (cf. Theorem 2.1.6) – the decidability of a PAC field $K$ is completely determined by the isomorphism types of the field $K^{\mathrm{alg}}$ (which, in turn, is determined by the set of polynomials in $\mathbb{Z}[X]$ with a root in $K$) and of the restriction map $\mathbf{G}_K \longrightarrow \mathbf{G}_{K^{\mathrm{alg}}}$ (considered as morphism in the category of profinite groups). Thus, a PAC field $K$ is decidable if and only if the theory of the algebraic part of $K$ is decidable (in the language $\mathscr{L}_{\mathrm{ring}}$) and its absolute Galois group is decidable (in the language $\mathscr{L}_{\mathrm{CSIS}}$). Furthermore, given that it was within this class of PAC fields that counterexamples to Abraham Robinson's original question (cf. Question (1.1.2) and Question (1.1.4)) were produced, we had naturally considered PAC fields as promising candidates to help us arrive at a similar negative answer to Question (1.1.1). While we have ultimately been unsuccessful in constructing one such PAC counterexample, exploring this avenue has provided us with some insights and has raised some interesting questions in the flavour of Question (1.1.1) that appear to be worth investigating in their own rights.

## 4.1 Modifying Known Counterexamples

In Chapter 2, we had noted that by a result of Lubotzky and van den Dries (cf. Proposition 4.8 of [LD81]), a profinite group is projective if and only if it is isomorphic to the absolute Galois group of some PAC field. We recall further that finite extensions of PAC fields correspond to taking open subgroups of the associated absolute Galois groups, i.e. if $L$ is a finite field extension of a PAC field, $K$, then $\mathbf{G}_L$ is an open subgroup of $\mathbf{G}_K$. Now, suppose we are looking to find a PAC counterexample to Question (1.1.1). In order to find such a counterexample, we would, in essence, have to answer the following question negatively in light of Theorem 2.1.6:

**Question 4.1.1.** *Is an open subgroup of a decidable projective profinite group always decidable?*

If we are able to find a decidable projective profinite group, $\mathcal{G}$, which admits an undecidable open subgroup $\mathcal{H}$, then the PAC field $K$ with absolute Galois group, $\mathbf{G}_K \cong \mathcal{G}$, and algebraic part, $K^{\text{alg}} = \widetilde{\mathbb{Q}}$, would be a decidable field which admits an undecidable finite extension $L$ which has absolute Galois group, $\mathbf{G}_L \cong \mathcal{H}$, and algebraic part, $L^{\text{alg}} = \widetilde{\mathbb{Q}}$. Our aim for the rest of the paper is to try and find a suitable PAC counterexample to Question (1.1.1). Towards this end, we will primarily focus on attempting to address Question (4.1.1). Note that the counterexample that we had constructed in Chapter 3 would not be able to solve the above question definitively – $W$-extensions (and similarly, $W^+$-extensions) of $\mathbb{Q}$ are not PAC fields and their absolute Galois groups are not *projective* profinite groups. However, since absolute Galois groups are indeed profinite groups, it is extremely likely that the following question does have a negative solution:

**Question 4.1.2.** *Is an open subgroup of a decidable profinite group always decidable?*

Again, we appeal to our $W$-extension (alternatively, $W^+$-extension) of $\mathbb{Q}$ counterexample from the previous chapter which does appear to hint at this negative solution: The countably infinite Boolean independent set $\Upsilon$ we had described in Section 3.3 shows us that a (sufficiently saturated extension of a) $W$-extension (and similarly, a $W^+$-extension) of $\mathbb{Q}$ has uncountably many pairwise elementarily inequivalent extensions $L_i$'s such that for every $\varphi \in \Upsilon$, $\varphi$ is satisfied by infinitely many of the $L_i$'s and not satisfied by infinitely many other $L_i$'s. Notice that these pairwise elementarily inequivalent extensions were obtained by considerations of the *residue fields* rather than through their *absolute Galois groups*. By Theorem 4.1 of [Koe95], we know that if the absolute Galois group of $L_i$ is $p$-adic – i.e. $\mathbf{G}_{L_i} \cong \mathbf{G}_{F_i}$ for some finite extension $F_i$ of $\mathbb{Q}_p$ – then $L_i$ is $p$-adically closed, i.e. $L_i$ is elementarily equivalent to some finite extension of $\mathbb{Q}_p$. Since this fits within the framework we are considering, we can in some sense "convert this story" to address the absolute Galois groups of each of the $L_i$'s instead. Indeed, for $i \neq j$, note that since $L_i \not\equiv L_j$, $L_i$ and $L_j$ cannot both be elementarily equivalent to the same finite extension of $\mathbb{Q}_p$ for some fixed prime $p$, so we have that $\mathbf{G}_{L_i} \ncong \mathbf{G}_{L_j}$.

However, as demonstrated, our set-up only allows us to conclude that the absolute Galois group of the $L_i$'s are all pairwise non-isomorphic. While we suspect that the absolute Galois group of these $L_i$'s would also be pairwise elementarily inequivalent (and possibly be such that one can, in addition, find some other countably infinite Boolean independent set $\Upsilon'$ with the property that whenever $\psi \in \Upsilon'$, then $\psi$ is true in infinitely many $\mathbf{G}_{L_i}$'s and false in infinitely many other $\mathbf{G}_{L_i}$'s), at the moment of this writing, we do not yet have a convincing argument for this assertion.

On the other hand, in light of Observation (1.2.6) and our exposition following Remark 2.1.11, we do have partial answers to the above questions based on the following lemma – the proof of which follows in exactly the same way as that of Observation (1.2.6):

**Lemma 4.1.3.** *If $K$ is a decidable field with small absolute Galois group and of finite degree of imperfection, then every finite extension of $K$ is decidable. In particular, if $K$ is a decidable PAC field whose absolute Galois group $\mathbf{G}_K$ (which is a projective profinite group) is small, then every open subgroup of $\mathbf{G}_K$ is also decidable.*

While Question (4.1.1) and Question (4.1.2) do remain open for the most part, it is worth noting that there are, in fact, undecidable projective profinite groups, $\mathcal{G}$, which have decidable open subgroups. Indeed, the construction of an undecidable PAC field, $K$, such that all proper finite extensions of $K$ are (isomorphic and) decidable as provided by Cherlin, van den Dries, and Macintyre in [CDM80a] give us one such example of a projective profinite group $\mathcal{G}$:

**Example 4.1.1** ("C-D-M" Example)**.** Let $f$ be a non-recursive function from the set of finite simple non-abelian groups to $\omega$. We then take $\mathcal{G}$ to be the closed normal subgroup of $\widehat{F}_\omega$ such that for any set $S$, $f(S)$ is the largest $k$ such that $S^k$ is a continuous image of $\mathcal{G}$. That such a closed normal subgroup exists follows from Theorem 3.3 of [Mel78]. $\mathcal{G}$ is clearly undecidable in $\mathscr{L}_{\mathrm{CSIS}}$ by virtue of its

construction. On the other hand, if $\mathcal{H}$ is a proper open subgroup of $\mathcal{G}$, then $\mathcal{H} \cong \widehat{F}_\omega$, and $\widehat{F}_\omega$ is known to be decidable.

We provide another, more illuminating, example of an undecidable (projective) profinite group which has a decidable open subgroup which would also form the basis of yet another counterexample to Robinson's original question:

**Example 4.1.2** ("Semi-Direct Product" Example)**.** Suppose $\mathbb{P}_{\text{nr}}$ is a non-recursive set of odd primes, and

$$\mathcal{G} := \prod_{p \text{ odd primes}} \mathbb{Z}_p \rtimes_\phi \mathbb{Z}_2,$$

where $\mathbb{Z}_p$ is the ring of $p$-adic integers. Let $\alpha$ be a generator of $\mathbb{Z}_2$ such that the action of $\mathbb{Z}_2$ on $\prod_{p \text{ odd prime}} \mathbb{Z}_p$ is given as follows:

$$\phi_\alpha = \begin{cases} \text{Identity on } \mathbb{Z}_p & \text{if } p \in \mathbb{P}_{\text{nr}}, \\ \text{Inversion on } \mathbb{Z}_p & \text{if } p \notin \mathbb{P}_{\text{nr}}. \end{cases}$$

Note that $\mathcal{G}$ is undecidable (in the language $\mathscr{L}_{\text{CSIS}}$) since we can essentially identify the non-recursive set $\mathbb{P}_{\text{nr}}$ in the following manner:

$$p \in \mathbb{P}_{\text{nr}} \iff \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ is a finite quotient of } \mathcal{G}.$$

On the other hand, let

$$\mathcal{H} := \prod_{p \text{ odd primes}} \mathbb{Z}_p \rtimes_\phi 2\mathbb{Z}_2.$$

Note further that $(\mathcal{G} : \mathcal{H}) = 2$ and that the (induced) action of $2\mathbb{Z}_2$ on $\prod_{p \text{ odd prime}} \mathbb{Z}_p$ is simply the identity on $\mathbb{Z}_p$ for all odd primes $p$. Thus,

$$\mathcal{H} = \prod_{p \text{ odd primes}} \mathbb{Z}_p \rtimes_\phi 2\mathbb{Z}_2 = \prod_{p \text{ odd primes}} \mathbb{Z}_p \times 2\mathbb{Z}_2 \cong \prod_{p \in \mathbb{P}} \mathbb{Z}_p \cong \widehat{\mathbb{Z}},$$

which is known to be decidable.

Earlier attempts to modify the above-mentioned examples to construct a decidable projective profinite group with an undecidable open subgroup proved to be tricky. The main objective in all these attempts was to "mask" some sort of undecidability which would be expressed only within an open subgroup of the

constructed projective profinite group. In the example provided by Cherlin, van den Dries and Macintyre, properties of $\widehat{F}_\omega$ were exploited in order to get an undecidable projective profinite group (an undecidable closed normal subgroup of $\widehat{F}_\omega$) with an open subgroup that was decidable – indeed, any open subgroup of the constructed projective profinite group was isomorphic to $\widehat{F}_\omega$ and that was known to be decidable. The specificity of this example made it difficult to be generalised to suit our needs.

On the other hand, the second example provided above involving the semi-direct products (cf. Example 4.1.2) appeared to be a little more susceptible to generalisations: For suppose

$$\mathcal{G} := \prod_{p \text{ odd prime}} \mathbb{Z}_p \ \rtimes_\phi \ (\mathbb{Z}_2 \ \coprod_2 \ \mathbb{Z}_2)$$

where $\mathbb{Z}_p$ is the group of $p$-adic integers, and $\coprod_2$ is the free pro-2 product. Note that $(\mathbb{Z}_2 \ \coprod_2 \ \mathbb{Z}_2)$ is, in fact, a free pro-2 group of two generators, say $\alpha$ and $\beta$ – for brevity of notation, henceforth, we will denote the group $(\mathbb{Z}_2 \ \coprod_2 \ \mathbb{Z}_2)$ by $\hat{F}_2(2)$. We further note that $\mathcal{G}$ is indeed a projective profinite group since, for every prime $p$, the Sylow $p$-subgroups of $\mathcal{G}$ are free pro-$p$ groups. Now suppose $\mathbb{P}_{\text{nr}}$ is a non-recursive set of odd primes as above. We define the action of $\hat{F}_2(2)$ on $\prod_{p \text{ odd prime}} \mathbb{Z}_p$ as follows:

$$\phi_\alpha = \begin{cases} \text{Identity on } \mathbb{Z}_p & \text{if } p \in \mathbb{P}_{\text{nr}}, \\ \text{Inversion on } \mathbb{Z}_p & \text{if } p \notin \mathbb{P}_{\text{nr}}. \end{cases}$$

$$\phi_\beta = \begin{cases} \text{Identity on } \mathbb{Z}_p & \text{if } p \notin \mathbb{P}_{\text{nr}}, \\ \text{Inversion on } \mathbb{Z}_p & \text{if } p \in \mathbb{P}_{\text{nr}}. \end{cases}$$

This complementary action of $\hat{F}_2(2)$ on $\prod_{p \text{ odd prime}} \mathbb{Z}_p$ was defined in such a way that attempted to "mask" the non-recursive set from being expressed within $\mathcal{G}$. We first aim to show that the following open subgroup

$$\mathcal{H} := \prod_{p \text{ odd prime}} \mathbb{Z}_p \ \rtimes_\phi \ \ker(\psi)$$

of $\mathcal{G}$ is undecidable. Here,

$$\psi : \ \hat{F}_2(2) \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

is an epimorphism such that $\psi(\alpha) = s$ and $\psi(\beta) = \psi(\alpha^2) = 1$ where $\mathbb{Z}/2\mathbb{Z} = \{1, s\}$ with $s^2 = 1$. Clearly, we have that $\left(\hat{F}_2(2) : \ker(\psi)\right) = 2$. We point out that $\ker(\psi)$ is, in fact, the normal closure of the subgroup generated by the set $\{\alpha^2, \beta\}$ in $\hat{F}_2(2)$. Further, by the Nielsen-Schrier formula, we have that the rank – i.e. the minimum number of topological generators – of $\ker(\psi)$ is 3. It is clear that both $\alpha^2$ and $\beta$ are generators of $\ker(\psi)$. Notice that

$$\psi(\alpha^{-1}\beta\alpha) = s^{-1} \cdot 1 \cdot s = 1$$

and so $\alpha^{-1}\beta\alpha \in \ker(\psi)$. Thus, let $\ker(\psi) = \langle \alpha^2, \beta, \alpha^{-1}\beta\alpha \rangle$. The (induced) action of $\ker(\psi)$ on $\prod_{p \text{ odd prime}} \mathbb{Z}_p$ is then given as follows:

$$\phi_{\alpha^2} = \text{ Identity on } \mathbb{Z}_p \text{ for all odd primes } p.$$

$$\phi_\beta = \phi_{\alpha^{-1}\beta\alpha} = \begin{cases} \text{Identity on } \mathbb{Z}_p & \text{if } p \notin \mathbb{P}_{\text{nr}}, \\ \text{Inversion on } \mathbb{Z}_p & \text{if } p \in \mathbb{P}_{\text{nr}}. \end{cases}$$

Now, one can show that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is indeed a finite quotient of $\ker(\psi)$. Thus, we would be able to express the complement of the non-recursive set $\mathbb{P}_{\text{nr}}$ (which, itself, is yet another non-recursive set of odd primes) in the following way:

$$p \notin \mathbb{P}_{\text{nr}} \iff \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ is a finite quotient of } \mathcal{H}.$$

Indeed, if $p \in \mathbb{P}_{\text{nr}}$, then the action is non-trivial on $\mathbb{Z}_p$ and hence we cannot have a direct product. If, on the other hand, $p \notin \mathbb{P}_{\text{nr}}$, then the action is indeed trivial on $\mathbb{Z}_p$ and so the semi-direct product in our formulation is just the direct product. This implies that $\mathcal{H}$ is undecidable.

However, as it turns out, the non-recursive set $\mathbb{P}_{\text{nr}}$ was already "visible" within $\mathcal{G}$, albeit in a rather convoluted way: For suppose we fix some odd prime $p \in \mathbb{Q}$. Note that we know that either $p \in \mathbb{P}_{\text{nr}}$ or $p \notin \mathbb{P}_{\text{nr}}$. Now, we could ask whether, for any odd prime $q \neq p$, the group action on $\mathbb{Z}_q$ is the same as that on $\mathbb{Z}_p$. This, in essence, allows us to partition the set of odd primes into two classes – those odd primes $q \neq p$ for which the group action on $\mathbb{Z}_q$ is the same as that on $\mathbb{Z}_p$, and

those odd primes $q \neq p$ for which the group action on $\mathbb{Z}_q$ is different from that on $\mathbb{Z}_p$. One of these classes corresponds to the non-recursive set $\mathbb{P}_{\text{nr}}$ (while the other corresponds to its complement), and the above exposition demonstrates that one could essentially reference either of the non-recursive sets ($\mathbb{P}_{\text{nr}}$ or its complement) within $\mathcal{G}$, implying that $\mathcal{G}$ had to, itself, be undecidable, for otherwise, one would be able to effectively determine the membership of a non-recursive set of odd primes.

Note that pushing Example 4.1.2 to further generalisations by constructing $\mathcal{G}$ as

$$\mathcal{G} := \prod_{p \text{ odd prime}} \mathbb{Z}_p \rtimes_\phi \left( \underbrace{\mathbb{Z}_2 \amalg \mathbb{Z}_2 \amalg \cdots \amalg \mathbb{Z}_2}_{n \text{ copies}} \right) = \prod_{p \text{ odd prime}} \mathbb{Z}_p \rtimes_\phi \hat{F}_n(2)$$

where $\hat{F}_n(2)$ denotes the free pro-2 group of $n$ generators formed by a free pro-2 product of $n$ copies of $\mathbb{Z}_2$, would not yield a counterexample that is very much more different from the one with just two copies of $\mathbb{Z}_2$ as constructed above – indeed, in this case, one would simply have to take $(n-1)$ distinct odd primes (instead of just one odd prime, as was the case for $\hat{F}_2(2)$), and ask whether the action of $\mathbb{Z}_q$ for any odd prime $q$ that is distinct from the pre-selected $(n-1)$ odd primes is the same as the action of $\mathbb{Z}_p$ for any one of the primes $p$ among the $(n-1)$ primes chosen. Thus, the constructed $\mathcal{G}$ in all these situations has to be undecidable as well, thereby making them unsuitable to be potential candidates to answer Question (4.1.1) negatively.

## 4.2 Coding "Undecidability"

As alluded to in the previous section, the main strategy that we had attempted to employ in order to find a negative solution to Question (1.1.1) was to "mask" some undecidability within a projective profinite group that would be expressed only within one of its open subgroups. Two main questions naturally arise during the implementation of this strategy:

1. How can one "code" some undecidability within a projective profinite group?

2. What would this "undecidability" be?

In this section, we aim to address these two questions partially and provide an insight into the thought process surrounding the above-mentioned strategy.

### 4.2.1 Addressing Question 1

Taking inspiration from the works of Cherlin, van den Dries, and Macintyre (cf. [CDM80a]; [CDM80b]), we believed that one way of tackling the first question was by coding the undecidability within graph structures. The above-mentioned manuscripts then provide the technical means by which one could construct projective profinite groups based on the given graph structures that, in turn, interpret the underlying graph structure from which the group was constructed from. For the sake of being self-contained, we describe in some detail the set-up and this C-D-M Construction of a projective profinite group from a given graph, elaborating Section 7.3 of [CDM80a]. We further refer one to Section 6 to 10 of Chapter 28, in the encyclopedic volume of Michael D. Fried and Moshe Jarden (cf. [FJ08]) which cover this technical means of coding graphs in projective profinite groups in much greater detail. As it was pointed out to us after the submission of this thesis, the materials covered especially in Section 8 to 10 appear to resolve Question 1.

Throughout this section, we fix two distinct odd primes $p$ and $q$. Let us suppose that $V$ is a vector space over $\mathbb{F}_2$. Suppose further that $\mathcal{H}$ and $\mathcal{I}$ are families of linear subspaces of $V$ of codimension 1, $A$ is a vector space over $\mathbb{F}_p$ by taking $(a_H)_{H\in\mathcal{H}}$ as a basis, and $B$ is a vector space over $\mathbb{F}_q$ by taking $(b_I)_{I\in\mathcal{I}}$ as a basis. We define an action of the additive group $V$ on the additive group $A \oplus B$ in the following way: for any $v \in V$,

$$a_H^v = \begin{cases} a_H & \text{if } v \in H \\ -a_H & \text{if } v \notin H \end{cases} \qquad\qquad b_I^v = \begin{cases} b_I & \text{if } v \in I \\ -b_I & \text{if } v \notin I \end{cases}$$

Let us suppose that $\phi : V \to \mathrm{Aut}(A \oplus B)$ is a homomorphism such that $\phi_v(a_H) = a_H^v$ and $\phi_v(b_I) = b_I^v$, and define $G := (A \oplus B) \rtimes_\phi V$. We now try and identify all normal subgroups $N$ of $G$ such that

(i) $G/N \cong \mathbb{F}_2$;

(ii) $G/N \cong D_p = \langle r, s \mid r^p = s^2 = 1,\ s^{-1}rs = r^{-1} \rangle$;

(iii) $G/N \cong D_q = \langle r, s \mid r^q = s^2 = 1,\ s^{-1}rs = r^{-1} \rangle$

In order to accomplish (i), we consider an epimorphism $\varphi : G \to \mathbb{F}_2$ and aim to show that $A \oplus B \subseteq \ker(\varphi)$, i.e. $\varphi(a, b, e_V) = e_{\mathbb{F}_2}$ for any $a \in A$ and $b \in B$. Suppose to the contrary that $\varphi(a, b, e_V) \neq e_{\mathbb{F}_2}$. Then $\varphi(a, b, e_V) = n$ for some $n \in \mathbb{F}_2 \setminus \{e_{\mathbb{F}_2}\}$. Recall that for $G = (A \oplus B) \rtimes_\phi V$, the external semi-direct product has the multiplication given by the following rule:

$$(a_1, b_1, v_1) *_G (a_2, b_2, v_2) = (a_1 *_A \phi_{v_1}(a_2),\ b_1 *_B \phi_{v_1}(b_2),\ v_1 *_V v_2),$$

where $*_A$, $*_B$, and $*_V$ are the group operations for $A$, $B$, and $V$ respectively. Now consider

$$\begin{aligned}
\varphi(a, b, e_V)^p &= \underbrace{\varphi(a, b, e_V) \cdot \varphi(a, b, e_V) \cdot \cdots \cdot \varphi(a, b, e_V)}_{p \text{ times}} \\
&= \varphi\left((a, b, e_V) *_G \cdots *_G (a, b, e_V)\right) \\
&= \varphi\left(\underbrace{a *_A \cdots *_A a}_{p \text{ times}},\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ \underbrace{e_V *_V \cdots *_V e_V}_{p \text{ times}}\right) \\
&= \varphi\left(e_A,\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ e_V\right).
\end{aligned}$$

Note further that $\varphi(a, b, e_V)^p = n^p$. Since $n \in \mathbb{F}_2 \setminus \{e_{\mathbb{F}_2}\}$, we have that $n^2 = e_{\mathbb{F}_2}$. Further, since $p$ is an odd prime, $p \equiv 1 \mod 2$, and so $n^p = n^{2k+1} = n^{2k} \cdot n = n$. We therefore have that

$$\varphi\left(e_A,\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ e_V\right) = \varphi(a, b, e_V)^p = n.$$

Now consider

$$\begin{aligned}
\varphi\left(e_A,\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ e_V\right)^q &= \underbrace{\varphi\left(e_A,\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ e_V\right) \cdot \cdots\cdot \varphi\left(e_A,\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ e_V\right)}_{q \text{ times}} \\
&= \varphi\left(\underbrace{(e_A,\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ e_V) *_G \cdots *_G (e_A,\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ e_V)}_{q \text{ times}}\right) \\
&= \varphi\left(\underbrace{e_A *_A \cdots *_A e_A}_{q \text{ times}},\ \underbrace{b *_B \cdots *_B b}_{pq \text{ times}},\ \underbrace{e_V *_V \cdots *_V e_V}_{q \text{ times}}\right) \\
&= \varphi\left(e_A,\ \underbrace{e_B *_B \cdots *_B e_B}_{p \text{ times}},\ e_V\right) \\
&= \varphi\left(e_A, e_B, e_V\right) \\
&= e_{\mathbb{F}_2}.
\end{aligned}$$

Note that $\varphi\left(e_A,\ \underbrace{b *_B \cdots *_B b}_{p \text{ times}},\ e_V\right)^q = n^q$ and since $n \in \mathbb{F}_2 \setminus \{e_{\mathbb{F}_2}\}$, we have that $n^2 = e_{\mathbb{F}_2}$. Further, since $q$ is an odd prime, $q \equiv 1 \mod 2$, and so $n^q = n^{2k+1} = n^{2k} \cdot n = n$. However, as we had mentioned, $n \neq e_{\mathbb{F}_2}$ and so it must be the case that $A \oplus B \subseteq \ker(\varphi)$.

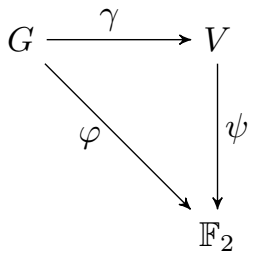
Now we consider the following exact sequence:

$$0 \longrightarrow A \oplus B \longrightarrow G \longrightarrow V \longrightarrow 0.$$

Correspondingly, we also have the following:

$$0 \longrightarrow \ker(\varphi) \longrightarrow G \xrightarrow{\varphi} \mathbb{F}_2 \longrightarrow 0.$$

Now consider the following:




Since $G/(A \oplus B) \cong V$, we get $(a, b, v) \overset{\gamma}{\mapsto} (e_A, e_B, v)$. As such, we have that

$$\begin{aligned}\psi(e_A, e_B, v) &= \varphi(a, b, v) \\ &= \varphi\left((a, b, e_V) *_G (e_A, e_B, v)\right)\end{aligned}$$

since $\phi_{e_V}(e_A) = e_A$ and $\phi_{e_V}(e_B) = e_B$. Therefore, we have that

$$\begin{aligned}\psi(e_A, e_B, v) &= \varphi\left((a, b, e_V) *_G (e_A, e_B, v)\right) \\ &= \varphi(a, b, e_V) \cdot \varphi(e_A, e_B, v) \\ &= e_{\mathbb{F}_2} \cdot \varphi(e_A, e_B, v) \\ &= \varphi(e_A, e_B, v).\end{aligned}$$

So we have that $\psi = \varphi$ and so

$$0 \longrightarrow \ker(\psi) \longrightarrow V \xrightarrow{\psi} \mathbb{F}_2 \longrightarrow 0.$$

We thus have that

$$\begin{aligned}& V/\ker(\psi) \cong \mathbb{F}_2 \\ \Rightarrow\quad & V/\ker(\varphi) \cong \mathbb{F}_2 \\ \Rightarrow\quad & \dim_{\mathbb{F}_2}\left(V/\ker(\varphi)\right) = \dim_{\mathbb{F}_2}(\mathbb{F}_2) = 1 \\ \Rightarrow\quad & \dim_{\mathbb{F}_2}(V) - \dim_{\mathbb{F}_2}\left(\ker(\varphi)\right) = 1 \\ \Rightarrow\quad & \operatorname{codim}\left(\ker(\varphi)\right) = 1.\end{aligned}$$

Note that $\ker(\varphi)$ thus corresponds to those normal subgroups $N$ of $G$ such that $G/N \cong \mathbb{F}_2$. This concludes (i).

We now attempt to address (ii), i.e. find all normal subgroups $N$ of $G$ such that $G/N \cong D_p$. Towards this end, consider an epimorphism $\varphi : G \to D_p$. We first aim to show that $B \subseteq \ker(\varphi)$, i.e. $\varphi(e_A, b, e_V) = e_{D_p}$ for all $b \in B$. For notation convenience, let us denote the identity $e_{D_p}$ of $D_p$ by 1. Suppose $\varphi(e_A, b, e_V) = r^m s^n$ for $1 \leq m \leq p$ and $1 \leq n \leq 2$. Now consider

$$\begin{aligned}
\varphi(e_A, b, e_V)^q &= \underbrace{\varphi(e_A, b, e_V) \cdot \cdots \cdot \varphi(e_A, b, e_V)}_{q \text{ times}} \\
&= \varphi\left(\underbrace{(e_A, b, e_V) \ *_G \ \cdots \ *_G \ (e_A, b, e_V)}_{q \text{ times}}\right) \\
&= \varphi\left(\underbrace{e_A *_A \cdots *_A e_A}_{q \text{ times}}, \underbrace{b *_B \cdots *_B b}_{q \text{ times}}, \underbrace{e_V *_V \cdots *_V e_V}_{q \text{ times}}\right) \\
&= \varphi(e_A, e_B, e_V) \\
&= 1
\end{aligned}$$

Now, note also that

$$\begin{aligned}
\varphi(e_A, b, e_V)^q &= (r^m s^n)^q \\
&= r^{mq} s^{nq}.
\end{aligned}$$

Thus, given that $\varphi(e_A, b, e_V)^q = 1$, we must have that $r^{mq} = 1$ and $s^{nq} = 1$, i.e.

$$mq \equiv 0 \mod p \quad \text{and} \quad nq \equiv 0 \mod 2.$$

Since $p$ and $q$ are distinct odd primes, we must have that

$$m \equiv 0 \mod p \quad \text{and} \quad n \equiv 0 \mod 2.$$

Given that $1 \leq m \leq p$ and $1 \leq n \leq 2$, we can conclude that $m = p$ and $n = 2$. Thus, we have that $\varphi(e_A, b, e_V) = r^p s^2 = 1$ and so $B \subseteq \ker(\varphi)$.

Note that $\varphi(A, e_B, e_V) = \langle r \rangle$ and $\varphi(e_A, e_B, V) = \langle s \rangle$. Now let us take $H_0 \in \mathcal{H}$ such that $\varphi(a_{H_0}, e_B, e_V) \neq 1$. We aim to show that

$$\ker(\varphi) = (\langle a_H \mid H \neq H_0 \rangle \oplus B) \rtimes H_0.$$

Towards this end, we first show that for all $v \in H_0$, $\varphi(e_A, e_B, v) = 1$. Note that $\phi_v(a_{H_0}) = a_{H_0}$. Now consider

$$\begin{aligned}\varphi(e_A, e_B, v)^2 &= \varphi(e_A, e_B, v) \cdot \varphi(e_A, e_B, v) \\ &= s^n \cdot s^n \\ &= s^{2n} \\ &= 1\end{aligned}$$

We point out that if $(a, b, v) \in G$, then we have that

$$(a, b, v)^{-1} = \left(\phi_{v^{-1}}(a^{-1}),\ \phi_{v^{-1}}(b^{-1}),\ v^{-1}\right).$$

Consider the following

$$\varphi(e_A, e_B, v)^{-1} \ \cdot\ \varphi(a, e_B, e_V) \ \cdot\ \varphi(e_A, e_B, v).$$

Note that $\varphi(e_A, e_B, v)^{-1} = \varphi\left((e_A, e_B, v)^{-1}\right)$. Now,

$$\begin{aligned}&\varphi\left((e_A, e_B, v)^{-1} \ *_G\ (a, e_B, e_V) \ *_G\ (e_A, e_B, v)\right) \\ &= \varphi\left(\left(\phi_{v^{-1}}(e_A^{-1}),\ \phi_{v^{-1}}(e_B^{-1}),\ v^{-1}\right) \ *_G\ (a, e_B, e_V) \ *_G\ (e_A, e_B, v)\right) \\ &= \varphi\left((e_A, e_B, v^{-1}) \ *_G\ (a, e_B, e_V) \ *_G\ (e_A, e_B, v)\right) \\ &= \varphi\left(\left(\phi_{v^{-1}}(a), e_B, v^{-1}\right) \ *_G\ (e_A, e_B, v)\right) \\ &= \varphi\left(\phi_{v^{-1}}(a), e_B, e_V\right).\end{aligned}$$

Now note that since $\phi_{e_V}(a_H) = a_H$, we have that $\phi_{v^{-1}}(a_H) = \phi_v(a_H)$, for otherwise, we would have that

$$\phi_{v^{-1}}(a_H) = \begin{cases} a_H & \text{if } v \notin H \\ -a_H & \text{if } v \in H \end{cases}$$

If $v \in H$, we would have that $\varphi_{v^{-1}}\left(\phi_v(a_H)\right) = \phi_{v^{-1}}(a_H) = -a_H$. But, $\varphi_{v^{-1}}\left(\phi_v(a_H)\right) = \phi_{v^{-1}.v}(a_H) = \phi_{e_V}(a_H) = a_H$, a contradiction. We thus have that $\phi_{v^{-1}}(a) = \phi_v(a)$. Hence,

$$\varphi(e_A, e_B, v)^{-1} \cdot \varphi(a, e_B, e_V) \cdot \varphi(e_A, e_B, v) = \varphi(\phi_v(a), e_B, e_V).$$

Let us suppose that $a = a_{H_0}$. In this case,

$$\varphi(e_A, e_B, v)^{-1} \cdot \varphi(a_{H_0}, e_B, e_V) \cdot \varphi(e_A, e_B, v) = \varphi(\phi_v(a_{H_0}), e_B, e_V).$$

Since $v \in H_0$,

$$\begin{aligned}\varphi(e_A, e_B, v)^{-1} \cdot \varphi(a_{H_0}, e_B, e_V) \cdot \varphi(e_A, e_B, v) &= \varphi(\phi_v(a_{H_0}), e_B, e_V) \\ &= \varphi(a_{H_0}, e_B, e_V).\end{aligned}$$

Now suppose that $\varphi(a_{H_0}, e_B, e_V) = r^m$ where $1 \leq m < p$ (since $\varphi(a_{H_0}, e_B, e_V) \neq 1$). Suppose $\varphi(e_A, e_B, v) = s \neq 1$. Note that $\varphi(e_A, e_B, V) = \langle s \rangle$, with $s^2 = 1$. So, we have that

$$s^{-1} \cdot r^m \cdot s = r^m.$$

We also have that $s^{-1} \cdot r \cdot s = r^{-1}$. Now,

$$\begin{aligned}& s^{-1} \cdot r \cdot s \cdot r^{m+1} = r^m = s^{-1} \cdot r^m \cdot s \\ \Rightarrow \quad & r \cdot s \cdot r^{m+1} = r^m \cdot s \\ \Rightarrow \quad & s \cdot r^{m+1} = r^{m-1} \cdot s \\ \Rightarrow \quad & r^{m+1} = s^{-1} \cdot r^{m-1} \cdot s.\end{aligned}$$

Then,

$$\begin{aligned}& r^{m+1} = s^{-1} \cdot r \cdot s \cdot r^{m+2} = s^{-1} \cdot r^{m-1} \cdot s \\ \Rightarrow \quad & r \cdot s \cdot r^{m+2} = r^{m-1} \cdot s \\ \Rightarrow \quad & s \cdot r^{m+2} = r^{m-2} \cdot s \\ \Rightarrow \quad & r^{m+2} = s^{-1} \cdot r^{m-2} \cdot s.\end{aligned}$$

Continuing this process, we eventually arrive at

$$\begin{aligned}& r^{2m-1} = s^{-1} \cdot r \cdot s = r^{-1} \\ \Rightarrow \quad & r^{2m-1} = r^{-1} \\ \Rightarrow \quad & r^{2m} = 1.\end{aligned}$$

Since $r \neq 1$, $r^{2m} = 1$ holds if and only if $2m \equiv 0 \mod p$ (since $r^p = 1$). Given that $p$ is an odd prime, $2m \equiv 0 \mod p$ implies that $m \equiv 0 \mod p$. However, we had earlier noted that $1 \leq m < p$, so $m \not\equiv 0 \mod p$. Hence, it must be the case $\varphi(e_A, e_B, v) = 1$ for all $v \in H_0$. We therefore have that $H_0 \subseteq \ker(\varphi)$.

Note that $H_0$ is a subspace of $V$ of codimension 1. Now, for $H \in \mathcal{H}$, $H \neq H_0$, we take $v \in H_0 \setminus H$. In this instance, we point out that $\phi_v(a_H) = -a_H$. We aim to show that $\varphi(a_H, e_B, e_V)^{-1} = \varphi(a_H, e_B, e_V)$. Consider

$$\begin{aligned}\varphi(a_H, e_B, e_V)^{-1} &= \varphi\left((a_H, e_B, e_V)^{-1}\right) \\ &= \varphi\left(\phi_{e_v^{-1}}(-a_H), \phi_{e_v^{-1}}(e_B), e_V\right) \\ &= \varphi\left(-a_H, e_B, e_V\right).\end{aligned}$$

Now,

$$\begin{aligned}\varphi(e_A, e_B, v) \cdot \varphi(-a_H, e_B, e_V) &= \varphi\left((e_A, e_B, v) *_G (-a_H, e_B, e_V)\right) \\ &= \varphi\left(a_H, e_B, v\right).\end{aligned}$$

Since $\varphi(e_A, e_B, v) = 1$ for all $v \in H_0$, we have that

$$\begin{aligned}\varphi(a_H, e_B, v) &= \varphi\left((a_H, e_B, e_V) *_G (e_A, e_B, v)\right) \\ &= \varphi(a_H, e_B, e_V) \cdot \varphi(e_A, e_B, v) \\ &= \varphi(a_H, e_B, e_V).\end{aligned}$$

We therefore have shown that $\varphi(a_H, e_B, e_V)^{-1} = \varphi(a_H, e_B, e_V)$ as required.

Now suppose $\varphi(a_H, e_B, e_V) = r^m$ for some $1 \leq m \leq p$. Since we have that $\varphi(a_H, e_B, e_V)^{-1} = \varphi(a_H, e_B, e_V)$,

$$\begin{aligned}&\Rightarrow \quad (r^m)^{-1} = r^m \\ &\Rightarrow \quad r^{-m} = r^m \\ &\Rightarrow \quad r^{2m} = 1.\end{aligned}$$

Since $r \neq 1$ and $r^p = 1$, we know that $2m \equiv 0 \mod p$. Again, since $p$ is an odd prime, we get that $m \equiv 0 \mod p$ and so $m = p$. Thus, $\varphi(a_H, e_B, e_V) = r^p = 1$ from whence we get that $\langle a_H \mid H \neq H_0 \rangle \subseteq \ker(\varphi)$. We can therefore conclude that

$$\ker(\varphi) = (\langle a_H \mid H \neq H_0 \rangle \oplus B) \rtimes H_0.$$

So if $H_0 \in \mathcal{H}$, take

$$N = (\langle a_H \mid H \in \mathcal{H} \setminus \{H_0\} \rangle \oplus B) \rtimes H_0.$$

$N$ is then a normal subgroup of $G$ such that $G/N \cong D_p$. This concludes (ii).

To address (iii), one merely repeats the steps in (ii) by modifying it accordingly to address the prime $q$ instead of the prime $p$. This leads us to the following:

$$\ker(\varphi) = (A \oplus \langle b_I \mid I \neq I_0 \rangle) \rtimes I_0,$$

and if $I_0 \in \mathcal{I}$, take

$$N = (A \oplus \langle b_I \mid I \in \mathcal{I} \setminus \{I_0\} \rangle) \rtimes I_0.$$

This $N$ is a normal subgroup of $G$ such that $G/N \cong D_q$, concluding (iii).

### Coding Graphs from Profinite Groups and Vice-Versa

With the above set-up, we now show that given a projective profinite group $\mathcal{G}$, we can construct a graph $\Gamma(\mathcal{G})$. Note that $\mathcal{G}$ plays the role of $G$ from above. Again, suppose that $p$ and $q$ are distinct odd primes. We take the set of vertices of $\Gamma(\mathcal{G})$ to be the set of open normal subgroups $N$ of $\mathcal{G}$ such that $\mathcal{G}/N \cong D_p$. We point out that from our set-up above, we can identify $\mathcal{H}$ with the underlying set of $\Gamma(\mathcal{G})$ via the map

$$H_0 \mapsto (\langle a_H \mid H \in \mathcal{H} \setminus \{H_0\} \rangle \oplus B) \rtimes H_0.$$

Now, for every normal subgroup $N$ with $\mathcal{G}/N \cong D_p$, we note that there exists a unique open normal subgroup $N'$ such that $N' \supseteq N$ with $\mathcal{G}/N' \cong \mathbb{F}_2$. We define the edge relation, $E$, in the following way: "vertices" $N_1$ and $N_2$ are adjacent if and only if

- $N_1 \neq N_2$ and
- there exists an open normal subgroup $M$ such that $M \supseteq N_1' \cap N_2'$ with $\mathcal{G}/M \cong \mathbb{F}_2$ such that there is an open normal subgroup $N$ with $N \subseteq M$ and $\mathcal{G}/N \cong D_q$.

This coding allows us to identify the vertices as the family $\mathcal{H}$, and the graph relation by the following: If $H_1, H_2 \in \mathcal{H}$, then $(H_1, H_2) \in E$ (i.e. $H_1$ and $H_2$ are adjacent) if and only if $H_1 \neq H_2$ and there exists $I \in \mathcal{I}$ with $H_1 \cap H_2 \subseteq I$.

Thus far, we have seen how, given a projective profinite group $\mathcal{G}$, we can construct a graph $\Gamma(\mathcal{G})$. Now, we show that given a graph $\Gamma$, we can construct a projective profinite group $\mathcal{G}$ such that $\Gamma \cong \Gamma(\mathcal{G})$. By an abuse of notation, let us denote the set of vertices of $\Gamma$ by $\Gamma$, and let the set of edges be denoted by $E$. We say that $(v_1, v_2) \in E$ whenever $v_1$ and $v_2$ are adjacent (in the graph-theoretic sense). Let $V$ denote a vector space over $\mathbb{F}_2$ with basis $(v_\gamma)_{\gamma \in \Gamma}$, and let

$$H_\gamma = \langle v_\delta \mid \delta \neq \gamma \rangle.$$

Note that $H_\gamma$ is a linear subspace of $V$ of codimension 1. Let

$$\mathcal{H} = \{H_\gamma \mid \gamma \in \Gamma\}.$$

For $\gamma \neq \delta$, let

$$I(\gamma, \delta) = \langle v_\gamma + v_\delta \rangle \oplus \langle v_\lambda \mid \lambda \neq \gamma,\ \lambda \neq \delta \rangle.$$

Note that $I(\gamma, \delta)$ is also a linear subspace of $V$ of codimension 1. Let

$$\mathcal{I} = \{I(\gamma, \delta) \mid (\gamma, \delta) \in E\}.$$

We can then construct the projective profinite group by taking

- $A$ to be a vector space over $\mathbb{F}_p$ with basis $(a_H)_{H \in \mathcal{H}}$
- $B$ to be a vector space over $\mathbb{F}_q$ with basis $(b_I)_{I \in \mathcal{I}}$.

Let the additive group $V$ act on the additive group $A \oplus B$ by

$$a_H^v = \begin{cases} a_H & \text{if } v \in H \\ -a_H & \text{if } v \notin H \end{cases} \qquad b_I^v = \begin{cases} b_I & \text{if } v \in I \\ -b_I & \text{if } v \notin I \end{cases}$$

Taking $\phi : V \to \mathrm{Aut}(A \oplus B)$ to be the corresponding homomorphism, we construct $\mathcal{G}$ as

$$\mathcal{G} = (A \oplus B) \rtimes_\phi V.$$

We are thus able to identify the set of elements in $\Gamma(\mathcal{G})$ with those in $\Gamma$, and so also with those in $\mathcal{H}$. The edge relation $E$ of $\Gamma(\mathcal{G})$ holds between $H_\gamma$ and $H_\delta$ if and only if $\gamma \neq \delta$ and for some $\gamma'$, $\delta'$ with $\gamma' \neq \delta'$ and $(\gamma', \delta') \in E$ we have that $I(\gamma', \delta') \supseteq H_\gamma \cap H_\delta$.

Note, however, that there are exactly three subspaces of $V$ of codimension 1 containing $H_\gamma \cap H_\delta$, namely

1. $H_\gamma$;
2. $H_\delta$;
3. $I(\gamma, \delta)$.

Clearly $\mathcal{H} \cap \mathcal{I} = \varnothing$. So we must have that $(H_\gamma, H_\delta) \in E$ holds if and only if $I(\gamma', \delta') = I(\gamma, \delta)$ for some $\gamma', \delta'$ with $(\gamma', \delta') \in E$. But then, this would imply that $\{\gamma, \delta\} = \{\gamma', \delta'\}$ and so $(\gamma, \delta) \in E$. Thus, we have that $(H_\gamma, H_\delta) \in E$ if and only if $(\gamma, \delta) \in E$. We can thus conclude that $\Gamma(\mathcal{G}) \cong \Gamma$.

We now aim to justify our claim that the profinite group $\mathcal{G}$ constructed is indeed projective. Towards this end, we recall the following definitions:

**Definition 4.2.1** (Essential Epimorphism)**.** *An essential epimorphism $\rho : \mathcal{G}_1 \to \mathcal{G}_2$ is a surjective homomorphism of profinite groups such that there is no proper closed subgroup $\mathcal{G}_0$ of $\mathcal{G}_1$ with $\rho(\mathcal{G}_0) = \mathcal{G}_2$.*

**Definition 4.2.2** (Projective Cover)**.** *A projective cover of a profinite group $\mathcal{G}_2$ is an essential epimorphism $\rho : \mathcal{G}_1 \to \mathcal{G}_2$ such that $\mathcal{G}_1$ is projective, i.e. a closed subgroup $\mathcal{G}_0$ of $\mathcal{G}_1$ is equal to $\mathcal{G}_1$ if and only if $\rho(\mathcal{G}_0) = \mathcal{G}_2$.*

By a result of Banaschewski, we note that every profinite group has a projective cover that is unique up to isomorphism (cf. Proposition 22.6.1 of [FJ08]). For notational convenience, if $\rho : \mathcal{G}_1 \to \mathcal{G}_2$ is a projective cover of $\mathcal{G}_2$, we denote the projective cover of $\mathcal{G}_2$ as $\rho^*(\mathcal{G}_2)$. We will also, by an abuse of notation, sometimes refer to $\mathcal{G}_1$ as the projective cover and use $\mathcal{G}_1$ and $\rho^*(\mathcal{G}_2)$ interchangeably depending on the situation.

**Remark 4.2.3.** *Note that the term* ***universal Frattini covers*** *is frequently used to refer to projective covers.*

In order to justify our claim that the profinite group thus constructed is indeed projective, it suffices for us to show that for any profinite group $\mathcal{G}$, we have that $\Gamma(\mathcal{G}) \cong \Gamma(\rho^*(\mathcal{G}))$. This therefore allows us to assume without any loss of generality that $\mathcal{G}$ itself is a projective profinite group as we had done above. Towards this end, let

$$\rho : \rho^*(\mathcal{G}) \to \mathcal{G}$$

be the projective cover of $\mathcal{G}$ and $H$ an open normal subgroup of $\rho^*(\mathcal{G})$ such that one of the following conditions holds:

1. $\rho^*(\mathcal{G})/H \cong \mathbb{F}_2$; or
2. $\rho^*(\mathcal{G})/H \cong D_p$; or
3. $\rho^*(\mathcal{G})/H \cong D_q$.

Consider the induced epimorphism

$$\theta : \rho^*(\mathcal{G})/H \to \mathcal{G}/\rho(H).$$

We aim to show that $\theta$ is an essential epimorphism, i.e. $\theta$ is an epimorphism such that there is no proper closed subgroup $F$ of $\rho^*(\mathcal{G})/H$ with $\theta(F) = \mathcal{G}/\rho(H)$. Suppose that $F$ is a subgroup of $\rho^*(\mathcal{G})/H$ with $\theta(F) = \mathcal{G}/\rho(H)$, and let

$$\phi : \rho^*(\mathcal{G}) \to \rho^*(\mathcal{G})/H$$

be an epimorphism. Consider the following commutative diagram:

$$\begin{array}{ccc} \rho^*(\mathcal{G}) & \xrightarrow{\phi} & \rho^*(\mathcal{G})/H \\ \Big\downarrow{\scriptstyle \rho} & & \Big\downarrow{\scriptstyle \theta} \\ \mathcal{G} & \xrightarrow[\psi]{} & \mathcal{G}/\rho(H) \end{array}$$

Identifying $H$ with $\ker(\phi)$, we have

$$\theta\left(\phi\left(\phi^{-1}(F)\right)\right) = \mathcal{G}/\rho(H) \quad \text{and} \quad \psi\left(\rho\left(\phi^{-1}(F)\right)\right) = \mathcal{G}/\rho(H).$$

Thus, we have that

$$\begin{aligned} & \rho\left(\phi^{-1}(F)\right) = \mathcal{G} \\ \Rightarrow \quad & \phi^{-1}(F) = \rho^*(\mathcal{G}) \\ \Rightarrow \quad & F = \phi\left(\rho^*(\mathcal{G})\right) = \rho^*(\mathcal{G})/H. \end{aligned}$$

Therefore, $\theta$ is indeed an essential epimorphism. Since $\theta$ is an essential epimorphism, we have that $\rho^*(\mathcal{G})/H \cong \mathcal{G}/\rho(H)$. Now, since $\mathcal{G}/N \cong \rho^*(\mathcal{G})/\rho^{-1}(N)$ for every open normal subgroup $N$ of $\mathcal{G}$, we have that

$$H = \rho^{-1}\left(\rho(H)\right).$$

Thus, $\Gamma(\mathcal{G})$ and $\Gamma(\rho^*(\mathcal{G}))$ are naturally isomorphic as sets via

$$N \mapsto \rho^{-1}(N).$$

One can further check that this map is also an isomorphism of $\Gamma(\mathcal{G})$ and $\Gamma(\rho^*(\mathcal{G}))$ as graphs, thereby justifying our assumption that the constructed profinite group $\mathcal{G}$ from a graph using the C-D-M Construction can indeed be taken to be a projective.

**Remark 4.2.4.** *We point out that there are indeed several other ways of constructing groups from graph structures, and we had earlier also attempted to construct groups from graphs using the so-called Mekler's Construction (cf. [Mek81] and Appendix A.3 of [Hod93]) in order to come up with a counterexample to answer Question* (1.1.1) *negatively. We briefly describe this Mekler's construction and explain the reason behind ultimately favouring the C-D-M Construction over Mekler's Construction.*

**Definition 4.2.5** (Nilpotent Group of Class 2 and Prime Exponent $p$)**.** *Let $G$ be a group, and denote by $[a, b]$ the commutator of group elements $a, b \in G$, where $[ab, b] = a^{-1}b^{-1}ab$. Denote by $Z(G) := \{a \in G \mid \text{ for } b \in G, \ [a, b] = 1\}$ the centre of the group $G$.*

- *The commutator subgroup of $G$ is the group generated by $[a, b]$ for $a, b \in G$;*
- *$G$ is nilpotent of class 2 (nil-2) if the commutator subgroup of $G$ is contained in $Z(G)$;*
- *$G$ is of exponent $p$ if for all $g \in G$, $g^p = 1$.*

*Some properties of a nilpotent group $G$ of class 2 include: for all $x, y, z \in G$*

- $[[x, y], z] = 1$;
- $[x \cdot y, z] = [x, z] \cdot [y, z]$;
- $[x, y \cdot z] = [x, y] \cdot [x, z]$.

*Denote by $\mathfrak{N}_2^p$ the variety of nilpotent groups of class 2 and exponent $p$. For a graph $\Gamma = (V, E)$, we aim to define a group $G(\Gamma)$ in the variety $\mathfrak{N}_2^p$ by the following presentation: the generators of the group $G(\Gamma)$ are the vertex of $\Gamma$, the relations are the equations $[a, b] = 1$ where $a, b \in V$ with $(a, b) \in E$, i.e. if two vertices $a$ and $b$ are connected in the graph $\Gamma$, then we make sure that the corresponding elements $a^*$*

*and $b^*$ of the group commute. In order for the properties of the graph to "transfer" over to the group, we need a way of essentially "talking" about the graph within the group. This is where the Mekler Construction comes in handy; it asserts that if the graph $\Gamma$ is **nice**, then the graph is $\varnothing$-interpretable in the group.*

**Definition 4.2.6** (Nice Graph)**.** *A graph $\Gamma = (V, E)$ is nice if*

*(i) for each $a, b \in V$ distinct, there is a $c \in V$ such that $(a, c) \in E$ and $(b, c) \notin E$;*

*(ii) any 2 vertices are adjacent to at most 1 vertex in common;*

*(iii) if 2 vertices are adjacent, then there is no third vertex to which they are both adjacent to.*

*(i) basically ensures that there are more than 2 vertices such that for any 2 distinct vertices, you can always find a third vertex which is joined to one but not the other. (ii) asserts that no squares can occur in a nice graph, while (iii) assert that no triangles can occur in a nice graph.*

*We point out that any graph can be made to be nice by the subdivision of an edge. Let $\Gamma' = (V', E')$ be any graph, then it could indeed be made into a nice graph $\Gamma = (V, E)$ in the following way: Take $V = V' \cup \{v_i\}_{i \in |E'|}$ by inserting a new vertex $v_i$ into each edge $(a, b) \in E'$ such that $(a, b) \in E'$ is divided into $(a, v_i) \in E$ and $(v_i, b) \in E$.*

*Now let $F$ be the free nilpotent group of class 2 and exponent $p$ on the free generators $x_0, x_1, \ldots$ (note that $0, 1, \ldots$ correspond to the vertices on the graph $\Gamma$). By a result of MacHenry, we have that the centre, $Z(F)$, of $F$ is an abelian group of exponent $p$ that is freely generated by $[x_r, x_s]$ for $r \neq s$ and $r < s$ (cf. [Mac60]). Given a graph $\Gamma$, denote the group formed using Mekler's construction as $G(\Gamma)$. Then,*

$$G(\Gamma) = F/N$$

*where* $N = \langle [x_r, x_s] \mid (r,s) \in E \rangle$. *In [Mek81], Mekler shows that for any two nice graphs* $\Gamma_1$ *and* $\Gamma_2$, *we have that* $\Gamma_1 \cong \Gamma_2$ *if and only if* $G(\Gamma_1) \cong G(\Gamma_2)$. *Mekler further provides a first-order interpretation (without parameters) which allows one to interpret the underlying graph* $\Gamma$ *from the constructed group* $G(\Gamma)$.

*While Mekler's Construction in its original form only associates to each symmetric, irreflexive nice graph a(n abstract) nilpotent group of class 2 and prime exponent p, a recent paper by André Nies (cf. Section 7 of [Nie16]) asserts that one can generalise this construction to form, instead, a profinite group – namely, one can construct the profinite completion* $\hat{G}(\Gamma)$ *of* $G(\Gamma)$ *with respect to a suitable basis of neighbourhoods of the identity. Nies further shows that just as there was an interpretation of the graph* $\Gamma$ *from the abstract group* $G(\Gamma)$, *Mekler's interpretation also carries through to this profinite setting, i.e. one can recover the nice graph* $\Gamma$ *from the profinite group* $\hat{G}(\Gamma)$ *via essentially the same interpretation that Mekler used to interpret* $\Gamma$ *from* $G(\Gamma)$.

*This may indeed be another way of coding graphs into profinite groups. However, what is lacking within this construction as compared to the C-D-M Construction is the fact that the resulting profinite group obtained through this construction need not necessarily be a* projective *profinite group. Thus, in order to address Question* (4.1.1), *one would first have to "move up" to a projective cover* $\rho^*\left(\hat{G}(\Gamma)\right)$ *of the resulting group* $\hat{G}(\Gamma)$, *and this move might introduce some additional concerns such as whether one could still interpret the nice graph within the projective cover etc. It is for such technical concerns that the C-D-M Construction was eventually preferred over Mekler's Construction.*

### 4.2.2 Addressing Question 2

Thus far, we have seen that one could construct a projective profinite group from a (simple) graph (i.e. a graph with no multiple edges) in which the said-graph is interpretable. This implies that if we are to find a negative solution to Question (4.1.1),

we must find a decidable simple graph, $\Gamma$, (in the graph language $\mathscr{L}_{\text{graph}} := \{\mathcal{E}\}$ where $\mathcal{E}$ is a binary relation symbol expressing the edge relation) from which we could obtain an undecidable subgraph, $\Gamma'$, such that the relationship between the graph and the subgraph translates correspondingly to the relationship between the projective profinite group and the open subgroup. This highlights a major difficulty in addressing Question 2 – other than trying to find the "right kind" of undecidability that we want to "mask" in the graph that is only to be revealed in the subgraph, we must also have a notion that naturally translates to the projective profinite group/open subgroup relationship. For the moment, we focus on constructing an undecidable graph, $\Gamma'$, and checking whether we could expand this graph by adding finitely many vertices and (possibly countably many) edges to $\Gamma'$ to obtain a decidable graph, $\Gamma$.

In the study of decidability of a structure $\mathfrak{M}$, very often an undecidability result is obtained in one of two ways: either arithmetic (or a related theory)[1] is interpretable/definable within $\mathfrak{M}$, or alternatively, there is some way of describing a non-recursive set within $\mathfrak{M}$. The former approach is used whenever the structure $\mathfrak{M}$ is already given (and we want to show that it is undecidable), whereas the latter technique is often employed in the construction of structures which we dictate to be undecidable (as we have done for the most part throughout this thesis). In what follows, we will show that while we can obtain an undecidable graph $\Gamma'$ using both the above-mentioned techniques, masking the undecidability in the graph extension $\Gamma$ proves to be quite a challenge.

We provide an example of a constructed graph $\Gamma'$ in which the ring of natural numbers can be interpreted. We will do this construction in stages. We first claim that within the structure $\langle \mathbb{N}; R, 0, 1, 2\rangle$ – where $R$ is a suitably defined binary

[1] Throughout the rest of this chapter, we will use the term "arithmetic" to mean the ring structure of the natural numbers. By "a related theory" we specifically mean the Robinson arithmetic, **Q**, which is a finitely axiomatised fragment of first-order Peano arithmetic that is both recursively incompletable and essentially undecidable.

relation symbol, and 0, 1, 2, are constant symbols – one could interpret the rational numbers together with the operations of addition and multiplication. We will construct a lattice of height 3 (i.e. every maximal chain of the lattice consists of 4 elements) that is isomorphic to our structure, and show that in that lattice, we could interpret the rationals (together with the addition and multiplication operations).

Consider the (rational) affine plane $\mathscr{A}$ over the field of rational numbers, $\mathbb{Q}$. We denote by $\mathscr{P}$ a non-empty set of elements called points, and by $\mathscr{L}$ a non-empty collection of subsets of $\mathscr{P}$ called lines.

$$\mathscr{P} = \mathbb{Q}^2 = \{(x, y) \mid x, y \in \mathbb{Q}\},$$

$$l \in \mathscr{L} \text{ if and only if } l = \{(x, y) \mid ax + by = c\},$$

where $a, b, c \in \mathbb{Q}$, $a^2 + b^2 \neq 0$. Note that since we are considering an affine plane, the following properties hold:

1. If $P$ and $Q$ are distinct points, then there is a unique line $l$ such that $P \in l$ and $Q \in l$ (we denote this line by $l(P, Q)$);

2. If $P$ is a point not contained in the line $l$, then there is a unique line $m$ such that $P \in m$ and $m \cap l = \varnothing$ (so $l$ is parallel to $m$, denoted $l \mathbin{/\!/} m$);

3. There are at least two points on each line.

Now consider the lattice $\mathtt{L}$ consisting of the points $\mathscr{P}$, the lines $\mathscr{L}$, the whole plane $\mathscr{A}$, and the empty set, partially ordered by inclusion (so we think of the language of lattice as one containing simply the binary relation symbol "$\prec$" satisfying the axiom that it is a partial order, and the axioms claiming the existence of the meet and the join of two points of the lattice). Note that we can define the element of the lattice which corresponds to the whole affine plane $\mathscr{A}$ by saying that it is the "largest" element of the lattice:

$$e \in \mathtt{L} \text{ corresponds to } \mathscr{A} \text{ if and only if } \forall x \in \mathtt{L} \; x \prec e.$$

Similarly,

$$e \in \mathtt{L} \text{ corresponds to } \varnothing \text{ if and only if } \forall x \in \mathtt{L}\ e \prec x.$$

For convenience, we let `Max` and `Min` denote the greatest and the smallest element of the lattice corresponding to $\mathscr{A}$ and $\varnothing$ respectively. Further, we can define the set of elements of the lattice that corresponds to the set of points $\mathscr{P}$:

$$p \in \mathscr{P} \iff (\mathtt{Min} \prec e_p) \wedge \forall e\ (e \neq \mathtt{Min} \rightarrow e \not\prec e_p).$$

Denote this set by $\mathtt{E}_{\mathscr{P}}$. Note that here, $e_p$ is the element of the lattice that corresponds to the point $p \in \mathscr{P}$.

In a similar fashion, we could also define the set of elements of the lattice that corresponds to the set of lines $\mathscr{L}$:

$$l \in \mathscr{L} \iff (e_l \prec \mathtt{Max}) \wedge \forall e\ (e \neq \mathtt{Max} \rightarrow e_l \not\prec e).$$

Again, $e_l$ is an element of the lattice which corresponds to the line $l \in \mathscr{L}$. Denote this set of elements of the lattice by $\mathtt{E}_{\mathscr{L}}$.

Distinct parallel lines in the affine plane are characterised by the property that they do not intersect (i.e. no common point lies on the lines). In our lattice ordered by inclusion, this is characterised by the property that their meet is $\varnothing$. From the discussion above, we can see that the property of parallel lines can also be expressed within the lattice:

$$(l \mathbin{/\!\!/} m) \wedge (l \neq m)$$

$$\iff$$

$$e_l, e_m \in \mathtt{E}_{\mathscr{L}}\ \ ((e_l \neq e_m) \wedge \nexists e \in \mathtt{E}_{\mathscr{P}}\ ((e \prec e_l) \wedge (e \prec e_m))).$$

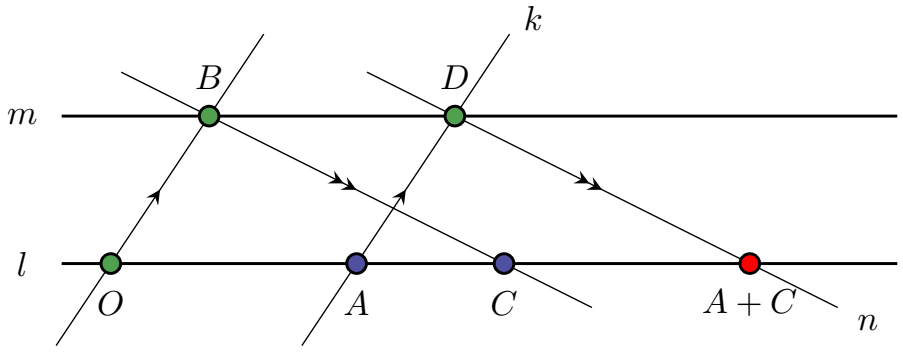
Now let the constants $0, 1, 2$ correspond to the three points $(0,0), (1,0), (0,1)$ to determine the coordinate system (affine transformations have 6 degrees of freedom on a plane, so we need 3 distinct points). We now choose a bijection $g : \mathbb{N} \rightarrow \mathtt{L}$ which maps the constants 0, 1 and 2 onto the points $(0,0), (1,0)$, and $(0,1)$ respectively.

We can then use $g$ to "transfer" the order of the lattice onto $\mathbb{N}$, and this obtained order will be the relation $R$.

Since it is easier to work with the lattice than with the structure described above, we first show that we can interpret the rational numbers, and the arithmetical operations in the lattice. Then the bijection $g$ would allow us to interpret the same within our structure $\langle \mathbb{N}; R, 0, 1, 2 \rangle$. We will employ techniques from Affine Geometry to essentially define these arithmetical operations. We first note that in Affine Geometry, we can only talk about addition and multiplication of points that lie on a common line. So let us identify any rational number $x$ with the point $(x, 0)$. Then we can define "geometrically" the addition and multiplication of the points of this form since they all lie on the common line, $y = 0$.

We recall the definition of addition in any affine plane $(\mathscr{P}, \mathscr{L})$. For a fixed line $l \in \mathscr{L}$, pick a point $O \in l$. Then for points $A, C \in l$, we define $A + C$ as follows:

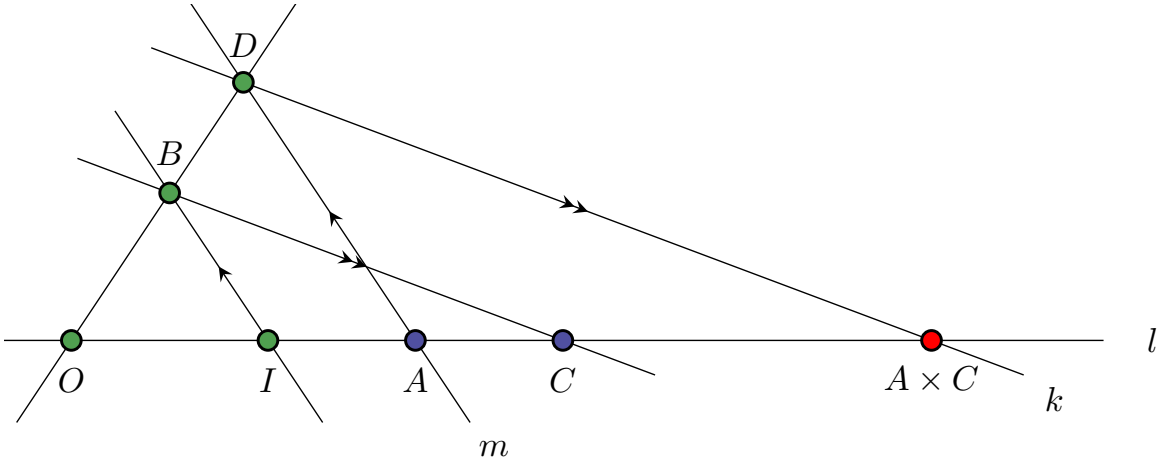
1. Select a point $B$ that is not on $l$;
2. Let $m$ be the line passing through $B$ and parallel to $l$;
3. Let $k$ be the line through $A$ parallel (or equal) to $l(O, B)$;
4. Let $D = m \cap k$;
5. Let $n$ be the line through $D$ parallel (or equal) to $l(B, C)$;
6. $A + C$ is defined to be $n \cap l$.



Since this description of addition only involves concepts of lines, points, parallel lines and intersection of lines, all of which, as we had seen above, are readily "transferable" to the lattice, we can effectively talk about the addition of points on the line $y = 0$. Note that the addition operation as defined by these steps on the line $y = 0$ gives rise to the coordinate-wise addition as we would expect. Also note that we needed to originally name the point $O$ for the addition to be defined; here our constants allow us to identify and name one such point immediately.

For the definition of multiplication, again take $(\mathscr{P}, \mathscr{L})$ as the affine plane. For a fixed line $l$ and $O$ as above, pick another fixed point $I$ different from $O$. For points $A$ and $C$ in $l$, multiply $A$ and $C$ as follows:

1. Select $B$ not in $l$;
2. Let $m$ be the line containing $A$ and parallel (or equal) to $l(I, B)$;
3. Let $D = m \cap l(O, B)$;
4. Let $k$ be the line containing $D$ and parallel (or equal) to $l(B, C)$;
5. $A \times C$ is defined to be $k \cap l$.



In this way, we can define multiplication on the line $y = 0$. Again, the constants allow us to name a second point $I$ immediately.

For a well-defined addition to satisfy the associative and commutative laws, and for a well-defined multiplication to satisfy the associative law, Desargues' Theorem is needed:

**Theorem 4.2.7** (Desargues' Theorem)**.**

1. *Suppose that $A, B, C$ are distinct non-collinear points with*

$$l(A, A') \mathbin{/\!/} l(B, B') \mathbin{/\!/} l(C, C'),$$
$$l(A, B) \mathbin{/\!/} l(A', B'), \text{ and}$$
$$l(A, C) \mathbin{/\!/} l(A', C').$$

   *Then $l(B, C) \mathbin{/\!/} l(B', C')$.*

2. *Suppose that $A, B, C$ are distinct non-collinear points with*

$$l(A, A') \cap l(B, B') \cap l(C, C') = P,$$
$$l(A, B) \mathbin{/\!/} l(A', B'), \text{ and}$$
$$l(A, C) \mathbin{/\!/} l(A', C').$$

   *Then $l(B, C) \mathbin{/\!/} l(B', C')$.*

For multiplication to be commutative, Pappus' Theorem is needed:

**Theorem 4.2.8** (Pappus' Theorem)**.** *Let $l \cap m = O$, with $P, Q$, and $R$ in $l$ and $S, T$, and $U$ in $m$. Suppose also that $l(P, T) \mathbin{/\!/} l(Q, U)$ and $l(Q, S) \mathbin{/\!/} l(R, T)$. Then $l(P, S) \mathbin{/\!/} l(R, U)$.*

We note that our affine plane over $\mathbb{Q}$ satisfies both the above theorems (a result in Affine Geometry) and as such, the addition and multiplication that we have defined on a line satisfy all the necessary properties as we should expect from the usual operations. Further, it suffices to define addition and multiplication on a single line since we have the following theorem in Affine Geometry:

**Theorem 4.2.9.** *Let $(\mathscr{P}, \mathscr{L})$ be an affine plane. Suppose $l, r \in \mathscr{L}$. Then there exists a bijective map $f : l \to r$. That is, there exists a bijective correspondence between the points of $l$ and the points of $r$.*

So if we think of the points $(x, 0)$ where $x \in \mathbb{Q}$ as the new "rational numbers", we have a corresponding addition and multiplication operation based on Affine Geometry as described above. Now we can define a bijection between the elements of the lattice $\mathtt{L}$ and these new "rational numbers", which will in turn allow us to interpret arithmetic within the structure $\langle \mathbb{N}; R, 0, 1, 2 \rangle$.

We next show that we can modify this argument by removing the dependence of the constants, thereby allowing us to show that $\langle \mathbb{N}; R \rangle$ is also undecidable. Recall that we needed the constants in order to name three non-collinear points so as to be able to establish the coordinate system. The constants also were necessary to help us define the addition and multiplication operations by identifying what were essentially the additive and multiplicative identities. Thus, if three non-collinear points could be defined and identified on our lattice, then the need for the constants would disappear.

The idea is to use additional elements in order to distinguish some points of the lattice. Let us begin with the lattice $\mathtt{L}$ from above, and suppose

$$X = \{(0, 1)\} \quad \cup \quad \{(x, 0) \mid x \in \mathbb{N}\}.$$

For every $x \in X$, we add a new point, $x'$ such that $e_x \prec e_{x'}$ in our lattice, and $x'$ is incomparable with all lines and all points that are distinct from $x$. Denote the resulting lattice by $\mathtt{L}^*$. Note that the definition of $\mathtt{E}_{\mathscr{P}}$ as described above still picks out the "old points" of $\mathtt{L}^*$, i.e. those elements of the lattice $\mathtt{L}$ that corresponded with the old points. We can now define the set $\mathtt{E}_{X'}$ corresponding to the set $X'$ in $\mathtt{L}^*$ in the following way:

$$x' \in X' \quad \iff \quad e_{x'} \in \mathtt{L}^* \;\; \exists!\, e \in \mathtt{E}_{\mathscr{P}} \;\; (e \prec e_{x'}).$$

So the set of elements of the lattice $\mathtt{L}^*$ that corresponds to the "points" of the affine plane is now given by the set $\mathtt{E}_{\mathscr{P}} \cup \mathtt{E}_{X'}$. It is worth pointing out that the definition of the set $\mathtt{E}_{\mathscr{L}}$ no longer identifies the set of lines of the affine plane in the new lattice $\mathtt{L}^*$; indeed $\mathtt{E}_{\mathscr{L}} \backslash \mathtt{E}_{X'}$ now corresponds to the set of lines.

Since we can identify the set $X'$ in the lattice $\mathtt{L}^*$ as $\mathtt{E}_{X'}$, we are able to identify the set $X$ too as $\mathtt{E}_X$ – these correspond to the set of elements that represent the points of the new lattice that are "related" to the elements in $\mathtt{E}_{X'}$. We can then identify the elements corresponding to $(0,1)$, $(0,0)$, and $(1,0)$ in the following manner:

- Since all the elements of $X$ except $(0,1)$ lie on the line $y = 0$,

$$x = (0,1)$$
$$\iff$$
$$e_x \in \mathtt{E}_X \ \wedge \ \exists l \in \mathtt{E}_{\mathscr{L}} \backslash \mathtt{E}_{X'} \ \left((e_x \not\prec l) \ \wedge \ (\forall e_y \in \mathtt{E}_X \ \ (e_y \neq e_x) \longrightarrow (e_y \prec l))\right).$$

  Denote this element by $e_{(0,1)}$.

- The midpoint of a line segment joining points $P$ and $Q$ is the point $M = \frac{1}{2}(P+Q)$. We can rewrite this as saying that $M$ is the midpoint of the line segment connecting $P$ and $Q$ if and only if $M + M = P + Q$. Now the point $(0,0)$ can be distinguished from the other points of the set $X \backslash \{(0,1)\}$ by saying that it is not the centre of any segment with endpoints in $X \backslash \{(0,1)\}$:

$$z = (0,0) \iff z \in X \backslash \{(0,1)\} \ \wedge \ \forall x, y \in X \backslash \{(0,1)\} \ \ (z + z \neq x + y).$$

  Since each point on the affine plane corresponds to some element in the lattice, the element corresponding to the point $(0,0)$ can be identified. We denote this element of the lattice by $e_{(0,0)}$.

- In a similar fashion, the point $(1,0)$ can be identified as the centre of exactly one such line segment:

$$z = (1,0) \iff z \in X \backslash \{(0,1)\} \ \wedge \ \exists! \ \ x, y \in X \backslash \{(0,1)\} \ \ (z + z = x + y).$$

  We denote this element of the lattice by $e_{(1,0)}$.

Note that the lattice $\mathtt{L}^*$ is still of height 3. With the three distinguished points, we can then define the binary relation $R$ for this lattice $\mathtt{L}^*$ as we had done before for $\mathtt{L}$.

Now we construct a graph, $\Gamma'$, based on the above construction of the lattice $\mathtt{L}^*$. We obtain the graph by considering the Hasse diagram (so transitivity relations are excluded from the graph) and removing `Max` and `Min` from the lattice $\mathtt{L}^*$ (and all the "edges" incident with them). Furthermore, we disregard the direction of the edges that is inherited from the lattice (note that in the lattice, inclusion was not a symmetric relation). We thus get a bipartite graph with one sort being formed by the set $\mathtt{E}_{\mathscr{P}}$, and the other formed by the set $\mathtt{E}_{\mathscr{L}}$ (the "new" points and the lines are part of the same sort). Note that we could identify the set $\mathtt{E}_{X'}$ in this graph since these are the elements of the graph that have degree 1 – every other vertex of this graph has infinite degree. Thus the set $\mathtt{E}_X$ can also be identified – those vertices that are adjacent to the elements in the set $\mathtt{E}_{X'}$. The set of vertices corresponding to the points $\mathscr{P}$ of the affine plane, together with the additional points that were added to the lattice $\mathtt{L}$ to get $\mathtt{L}^*$, can be identified by the following description: Vertex $v$ corresponds to a point if and only if either

1. $v \in \mathtt{E}_X$; or
2. $v \in \mathtt{E}_{X'}$; or
3. $\exists v_1, v_2$ with $v_1 \neq v_2$, $v_1 \in \mathtt{E}_X$ and $v_2 \notin \mathtt{E}_X$ such that $(v_1, v_2) \in R$ and $(v_2, v) \in R$

Denote this set of vertices by $V_{\mathscr{P}}$. Note that, in addition, for all $v_1, v_2 \in V_{\mathscr{P}} \backslash \mathtt{E}_{X'}$, we have that $(v_1, v_2) \notin R$ and if there exists $v_1, v_2 \in V_{\mathscr{P}}$ such that $(v_1, v_2) \in R$, then either $v_1 \in \mathtt{E}_X$ and $v_2 \in \mathtt{E}_{X'}$ or $v_2 \in \mathtt{E}_X$ and $v_1 \in \mathtt{E}_{X'}$. The set of vertices corresponding to the lines of the affine plane can then be identified by the following description: Vertex $v$ corresponds to a line in $\mathscr{L}$ if and only if $v \notin V_{\mathscr{P}}$. Denote this set by $V_{\mathscr{L}}$. So essentially these two sets, $V_{\mathscr{P}}$ and $V_{\mathscr{L}}$, can be identified by their "distances" away from the elements of the set $\mathtt{E}_X$. Note that the universe of the

graph $V = V_{\mathscr{P}} \cup V_{\mathscr{L}}$. In this way, we can interpret the rational numbers and the operations on them by "identifying the affine structure" that allowed us to interpret these sets and operations, thereby getting an undecidable graph.

In what follows, we provide an example of a graph $\Gamma$ such that when a vertex is removed, the resulting subgraph $\Gamma'$ interprets some non-recursive subset of $\mathbb{N}$. We will, however, also show that within this context, the non-recursive subset was already interpretable within $\Gamma$ itself. Let us begin by having a disconnected graph that contains countably many connected components, each connected component is a complete graph of precisely size $n$ for each $n \in \mathbb{N}$. Let $S$ be a non-recursive subset of $\mathbb{N}$ such that there is an extra vertex $s$ connected to all those components corresponding to the numbers in $S$, i.e. if the number 3 is in $S$, then the additional vertex $s$ is adjacent to all the vertices in the connected component of 3 elements. Suppose further that there is another vertex $t$ such that $t$ is connected to all those components corresponding to the numbers in the complement of $S$, i.e. if the number 5 is not in $S$, then the vertex $t$ is adjacent to all the vertices in the connected component of 5 elements. Let us denote the resulting graph by $\Gamma$. Notice that if we remove the vertex $t$ and all its adjacent edges, then the induced subgraph $\Gamma'$ is undecidable – indeed, the non-recursive subset $S$ becomes "visible" in $\Gamma'$ since membership of $S$ can be determined by looking at the neighbourhood relationship of the vertex $s$ (which is definable as being the only vertex that has infinitely many neighbours).

However, we point out that, in this case, $\Gamma$ itself must already be undeciable since $S$ is again "visible" within $\Gamma$: as with the situation in our attempted modification of Example 4.1.2, we know that, say, the complete graph of 3 elements is adjacent to either $s$ or $t$. We can thus ask whether the complete graph of $n$ elements is adjacent to the same vertex (that has infinitely many neighbours) as the complete graph of 3 elements. Depending on whether 3 is in $S$ or its complement, we would thus be able to identify either $S$ or its complement, noting that in either case, both sets are

non-recursive. The graph $\Gamma$ would therefore need to be undecidable as well.
We now provide a brief example of a decidable graph, $\Gamma$, that becomes undecidable when a finite number of vertices are removed. Let

$$S := \{m + nc \mid m, n \in \mathbb{Q},\ c \in \mathbb{R} \text{ realises an undecidable Dedekind cut}\}.$$

Taking addition as being component-wise, $S$ can be viewed as an ordered group in the language $\mathscr{L} := \{+, <\ ;\ 0, 1\}$. Here, we also take the language $\mathscr{L}$ to be relational by interpreting "+" as a ternary relation symbol and interpreting "<" as a binary relation symbol. Note that despite $S$ containing "undecidable" elements – namely, those elements that realise undecidable Dedekind cuts – the theory of $S$ in $\mathscr{L}$ is itself decidable; indeed, we are able to effectively axiomatise the full theory of $S$ by saying how any two elements in $S$ are related. On the other hand, if the element $c \in S$ is removed from the set, then we would, in particular, be able to define the element $2c \in S$ – it is the only element in $S \setminus \{c\}$ which is not the sum of two identical elements of $S \setminus \{c\}$, i.e. there is no $x \in S \setminus \{c\}$ such that $x + x = 2c$. Note that the element $2c$ also realises an undecidable Dedekind cut. Thus, we see that the theory of $S \setminus \{c\}$ would be undecidable. By coding the group $S$ into a suitable graph (within which we can still interpret the original group), we would be able to produce a decidable graph with an undecidable subgraph. It is, however, still relatively unclear whether the projective profinite groups that could be obtained from these graphs would respect the projective profinite group/open subgroup relationship that we expect in order to construct a counterexample to Question (4.1.1).

We end this paper with the following related question:

**Question 4.2.10.** *If $L$ is a finite extension of $K$ such that the Robinson Arithmetic, $\mathbf{Q}$, is interpretable in $L$ using $\mathscr{L}_{ring}$ (without any parameters), then is $\mathbf{Q}$ already be interpretable in $K$ using $\mathscr{L}_{ring}$ (without any parameters)?*

By modifying the above example, it appears that at least the "graph analogue" of Question (4.2.10) could be answered negatively – that there is a graph $\Gamma'$ and a "finite" extension graph $\Gamma$ (in the sense as described above) such that the ring structure of the natural numbers is interpretable in $\Gamma'$ but not in $\Gamma$. However, as of this moment, we are unsure whether this can be "generalised" to the field setting as laid out in Question (4.2.10).

*If I have seen further it is by standing on the shoulders of giants.*

— Sir Isaac Newton

# References


[AK65] Ax, James and Kochen, Simon. "Diophantine Problems Over Local Fields II: A Complete Set of Axioms for $p$-adic Number Theory". In: *American Journal of Mathematics* 87.3 (1965), pp. 631–648.

[Ax68] Ax, James. "The Elementary Theory of Finite Fields". In: *Annals of Mathematics* 88.2 (1968), pp. 239–271.

[Can67] Cantor, Georg. "De Aequationibus Secundi Gradus Indeterminatis". In: *Berolini, typis C. Schultzii* (1867). Doctoral Thesis, `https://hdl.handle.net/2027/njp.32101075302172`.

[CDM80a] Cherlin, Gregory, Dries, Lou van den, and Macintyre, Angus. "The Elementary Theory of Regularly Closed Fields (Version I)". In: *Preprint* (1980).

[CDM80b] Cherlin, Gregory, Dries, Lou van den, and Macintyre, Angus. "The Elementary Theory of Regularly Closed Fields (Version II)". In: *Preprint* (1980).

[CDM81] Cherlin, Gregory, Dries, Lou van den, and Macintyre, Angus. "Decidability and Undecidability Theorems for PAC-Fields". In: *Bulletin (New Series) of the American Mathematical Society* 4.1 (1981), pp. 101–104.

[Cha84] Chatzidakis, Zoé. "Model Theory of Profinite Groups". In: *Dissertation, Yale University* (1984).

[CK12] Chang, Chen Chung and Keisler, Jerome. *Model Theory*. 3rd. Vol. 73. Studies in Logic and the Foundations of Mathematics. Dover Publications, 2012.

[EJ90] Efrat, Ido and Jarden, Moshe. "Free Pseudo $p$-adically Closed Fields of Finite Corank". In: *Journal of Algebra* 133 (1990), pp. 132–150.

[Ers00] Ershov, Yuri L. “On Surprising Extensions of the Field of Rationals”. In: *Doklady Mathematics* 62.1 (2000), pp. 8–9.

[Ers01a] Ershov, Yuri L. “Immediate Extensions of Prüfer Rings”. In: *Algebra and Logic* 40.3 (2001), pp. 144–158.

[Ers01b] Ershov, Yuri L. *Multi-Valued Fields.* Kluwer Academic, 2001.

[Ers02a] Ershov, Yuri L. “Multi-Valued Fields II”. In: *Algebra and Logic* 41.6 (2002), pp. 374–390.

[Ers02b] Ershov, Yuri L. “Nice Local-Global Fields IV”. In: *Siberian Mathematical Journal* 43.3 (2002), pp. 418–427.

[Ers02c] Ershov, Yuri L. “Preordered Multivalued Fields”. In: *Doklady Mathematics* 65.1 (2002), pp. 75–79.

[Ers09] Ershov, Yuri L. “Subfields of the Adele Ring”. In: *Algebra and Logic* 48.6 (2009), pp. 418–425.

[Ers65] Ershov, Yuri L. “On the Elementary Theory of Maximal Normed Fields (Russian)”. In: *Algebra i Logika* 4.3 (1965), pp. 31–70.

[Ers94a] Ershov, Yuri L. “Fields with Continuous Local Elementary Properties I”. In: *Algebra and Logic* 33.6 (1994), pp. 351–365.

[Ers94b] Ershov, Yuri L. “RC*-Fields”. In: *Algebra and Logic* 33.4 (1994), pp. 205–215.

[ES09] Eisenträger, Kirsten and Shlapentokh, Alexandra. “Undecidability in Function Fields of Positive Characteristic”. In: *International Mathematics Research Notices* 2009.21 (2009), pp. 4051–4086.

[FHV93] Fried, Michael D., Haran, Dan, and Völklein, Helmut. “The Absolute Galois Group of the Totally Real Numbers”. In: *C. R. Acad. Sci. Paris Sér. I Math.* 317.11 (1993), pp. 995–999.

[FHV94] Fried, Michael D., Haran, Dan, and Völklein, Helmut. “Real Hilbertianity and the Field of Totally Real Numbers”. In: *Arithmetic Geometry – Conference on Arithmetic Geometry with an Emphasis on Iwasawa Theory Held at Arizona State Univeristy, March 15-18, 1993 (Contemporary*

*Mathematics, Vol. 174)*. Ed. by Nancy Childress and John W. Jones. American Mathematical Society, 1994, pp. 1–34.

[FJ08] Fried, Michael D. and Jarden, Moshe. *Field Arithmetic*. 3rd. Vol. 11. A Series of Modern Surveys in Mathematics. Springer-Verlag Berlin Heidelberg, 2008.

[FV92] Fried, Michael D. and Völklein, Helmut. "The Embedding Problem Over a Hilbertian PAC-Field". In: *Annals of Mathematics* 135 (1992), pp. 469–481.

[FV94] Fried, Michael D. and Völklein, Helmut. "The Absolute Galois Group of a Hilbertian PRC Field". In: *Israel Journal of Mathematics* 85 (1994), pp. 85–101.

[Goe29] Goethe, Johann Wolfgang von. *Wilhelm Meisters Wanderjahre oder die Entsagenden*. de. Cotta, 1829.

[GPR95] Green, Barry, Pop, Florian, and Roquette, Peter. "On Rumely's Local-Global Principle". In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 97 (1995), pp. 43–74.

[Har09] Harbater, David. "On Function Fields With Free Absolute Galois Group". In: *Journal für die reine und angewandte Mathematik* 2009.632 (2009), pp. 85–103.

[Har95] Harbater, David. "Fundamental Groups and Embedding Problems in Characteristic $p$". In: *Recent Developments in the Inverse Galois Problem – A Joint Summer Research Conference on Recent Developments in the Inverse Galois Problem Held at University of Washington, Seattle, July 17-23, 1993 (Contemporary Mathematics, Vol. 186)*. Ed. by Michael D. Fried et al. American Mathematical Society, 1995, pp. 353–369.

[Hod93] Hodges, Wilfrid. *Model Theory*. Vol. 42. Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 1993.

[Iwa53] Iwasawa, Kenkichi. "On Solvable Extensions of Algebraic Number Fields". In: *Annals of Mathematics, Second Series* 58.3 (1953), pp. 548–572.

[Jar72] Jarden, Moshe. "Elementary Statements Over Large Algebraic Fields". In: *Transactions of the American Mathematical Society* 164 (1972), pp. 67–91.

[Jar80] Jarden, Moshe. “An Analogue of Čebotarev Density Theorem for Fields of Finite Corank”. In: *Journal of Mathematics of Kyoto University* 20.1 (1980), pp. 141–147.

[Jar82] Jarden, Moshe. “The Elementary Theory of Large $e$-fold Ordered Fields”. In: *Acta Mathematica* 149.1 (1982), pp. 239–260.

[Jar95] Jarden, Moshe. “On Free Profinite Groups of Uncountable Rank”. In: *Recent Developments in the Inverse Galois Problem – A Joint Summer Research Conference on Recent Developments in the Inverse Galois Problem Held at University of Washington, Seattle, July 17-23, 1993 (Contemporary Mathematics, Vol. 186)*. Ed. by Michael D. Fried et al. American Mathematical Society, 1995, pp. 371–383.

[JK75] Jarden, Moshe and Kiehne, Ursel. “The Elementary Theory of Algebraic Fields of Finite Corank”. In: *Inventiones Mathematicae* 30 (1975), pp. 275–294.

[JL89] Jensen, Christian U. and Lenzing, Helmut. *Model Theoretic Algebra With Particular Emphasis on Fields, Rings, Modules*. Vol. 2. Algebra, Logic and Applications Series. Gordon and Breach Science Publishers, 1989.

[Koc97] Koch, Helmut. *Algebraic Number Theory*. Springer-Verlag Berlin Heidelberg, 1997.

[Koe16] Koenigsmann, Jochen. “On a Question of Abraham Robinson’s”. In: *Israel Journal of Mathematics* 214 (2016), pp. 931–943.

[Koe95] Koenigsmann, Jochen. “From $p$-rigid Elements to Valuations (with a Galois-Characterization of $p$-adic Fields)”. In: *Journal für die reine und angewandte Mathematik* 465 (1995), pp. 165–182.

[Lam04] Lam, Tsit Yuen. *Introduction to Quadratic Forms Over Fields*. Vol. 67. Graduate Studies in Mathematics. American Mathematical Society, 2004.

[LD81] Lubotzky, Alexander and Dries, Lou van den. “Subgroups of Free Profinite Groups and Large Subfields of $\widetilde{\mathbb{Q}}$”. In: *Israel Journal of Mathematics* 39.1–2 (1981), pp. 25–45.

[Let06] Lettl, Günter. "Finitely Arithmetically Fixed Elements of a Field". In: *Archiv der Mathematik* 87.6 (2006), pp. 530–538.

[Mac60] MacHenry, Trueman. "The Tensor Product and the 2nd Nilpotent Product of Groups". In: *Mathematische Zeitschrift* 73 (2 1960), pp. 134–145.

[Mek81] Mekler, Alan H. "Stability of Nilpotent Groups of Class 2 and Prime Exponent". In: *The Journal of Symbolic Logic* 46 (1981), pp. 781–788.

[Mel78] Mel'nikov, O. V. "Normal Subgroups of Free Profinite Groups". In: *Mathematics of the USSR-Izvestiya* 12.1 (1978), pp. 1–20.

[Nie16] Nies, André. "The Complexity of Isomorphism Between Countably Based Profinite Groups". In: *eprint arXiv:1604.00609* (2016).

[NS03] Nikolov, Nikolay and Segal, Dan. "Finite Index Subgroup in Profinite Groups". In: *Comptes Rendus Mathematique* 337.5 (2003), pp. 303–308.

[Pop84] Popescu, Nicolae. "On a Class of Prüfer Domains". In: *Revue Roumaine de Mathématique Pures et Appliquées* 29 (1984), pp. 777–786.

[Pop93a] Pop, Florian. "Hilbertian Fields with a Universal Local-Global Principle". In: *Reihe Arithmetik* 7 (1993). Preprint, `https://www.math.upenn.edu/~pop/Research/files-Res/HFLGP.pdf`.

[Pop93b] Pop, Florian. "The Geometric Case of a Conjecture of Shafarevich – $\mathbf{G}_{\tilde{\kappa}(t)}$ is Profinite Free". In: *Reihe Arithmetik* 8 (1993). Preprint, `https://www.math.upenn.edu/~pop/Research/files-Res/GeomSC.pdf`.

[Pop96] Pop, Florian. "Embedding Problems Over Large Fields". In: *Annals of Mathematics* 144.1 (1996), pp. 1–34.

[PR] Prestel, Alexander and Roquette, Peter. *Formally p-adic Fields*. Lecture Notes in Mathematics. Springer-Verlag Berlin Heidelberg.

[Pre81] Prestel, Alexander. "Pseudo Real Closed Fields". In: *Set Theory and Model Theory: Proceedings of an Informal Symposium Held at Bonn, June 1-3, 1979 (Lecture Notes in Mathematics, Vol. 872)*. Ed. by Ronald Björn Jensen and Alexander Prestel. Springer-Verlag Berlin Heidelberg, 1981, pp. 127–156.

[Prü32] Prüfer, Heinz. "Untersuchungen über die Teilbarkeitseigenschaften in Körpern". In: *Journal für die reine und angewandte Mathematik* 168 (1932), pp. 1–36.

[PS90] Prestel, Alexander and Schmid, J. "Existentially Closed Domains with Radical Relations – An Axiomatization of the Ring of Algebraic Integers". In: *Journal für die reine und angewandte Mathematik* 407 (1990), pp. 178–201.

[Rob59] Robinson, Julia. "The Undecidability of Algebraic Rings and Fields". In: *Proceedings of the American Mathematical Society* 10.6 (1959), pp. 950–957.

[Rob64] Robinson, Raphael M. "The Undecidability of Pure Transcendental Extensions of Real Fields". In: *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik MLQ - Math. Log. Quart.* 10.18 (1964), pp. 275–282.

[Rob65] Robinson, Abraham. "Formalism 64". In: *Logic, Methodology and Philosophy of Science: Proceedings of the 1964 International Congress (Studies in Logic and the Foundations of Mathematics)*. Ed. by Yehoshua Bar-Hillel. North-Holland Publishing Company Amsterdam, 1965, pp. 228–246.

[Rob73] Robinson, Abraham. "Metamathematical Problems". In: *The Journal of Symbolic Logic* 38.3 (1973), pp. 500–516.

[RZ10] Ribes, Luis and Zalesskii, Pavel. *Profinite Groups*. 2nd. Vol. 40. A Series of Modern Surveys in Mathematics. Springer-Verlag Berlin Heidelberg, 2010.

[Sch00] Schinzel, Andrzej. *Polynomials With Special Regard to Reducibility*. Vol. 77. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2000.

[Sch85] Schinzel, Andrzej. "Reducibility of Polynomials in Several Variables II". In: *Pacific Journal of Mathematics* 118.2 (1985), pp. 531–563.

[Tar51] Tarksi, Alfred. *A Decision Method for Elementary Algebra and Geometry*. Berkeley: University of California, 1951.

[Tys06] Tyszka, Apoloniusz. "A Discrete Form of the Theorem that Each Field Endomorphism of $\mathbb{R}(\mathbb{Q}_p)$ is the Identity". In: *Aequationes Mathematicae* 71.1-2 (2006), pp. 100–108.

[Whe79] Wheeler, William H. "Model-Complete Theories of Pseudo-Algebraically Closed Fields". In: *Annals of Mathematical Logic* 17.3 (1979), pp. 205–226.

[Zaf86] Zafrullah, Muhammad. "On Generalized Dedekind Domains". In: *Mathematika* 33 (2 1986), pp. 285–295.

# Index


$B$-Enrichment, 84
$E$-Lattice, 80, 84
$W$-Extension, 59, 86
$W^+$-Extension, 59, 89
$(A \setminus \{0\})$-expansion of $K$, 86
$p$-adic Kochen Operator, 91
$p$-adic Kochen Ring, 91

Absolute Ramification Index, 67
Affine, 49
Ample in Infinity, 54

B-Ring, 51
Bézout Ring, 46
Boolean, 49
Boolean Independent Set, 28

C-D-M Construction, 107
Complete Inverse System, 20

Dense, 40

e-closed, 60, 74
Essential Epimorphism, 117
Essentially Undecidable, 132
Existentially Closed, 59

Field
  $\omega$-free PAC, 22
  Ample, 54
  Decidable, 2
  Multi-Valued Field, 49
  Preordered Field, 69
  Pseudo Algebraically Closed, 13
  SAP Field, 70
  Valued Field, 35
Finite Embedding Problem, 14

Generalized Dedekind Ring, 52
Geometric Extension, 55
Graph
  Nice Graph, 120
  Simple Graph, 122

Henselization, 40
Holomorphy Ring, 48

Immediate Extension, 37, 55
Independence, 48

Language
  Graph, 122
  Complete Stratified Inverse Systems, 19
  Rings, 2
Lie Above, 90
Lift, 62
  M-Lift, 62
Linear Order, 68
Localization, 41

Mekler's Construction, 120

NB-ring, 51
Near-Boolean, 50

Prüfer Ring, 45
Preorder, 69
Profinite Group
  Projective, 13
  Small, 21
Projective Cover, 117
Property
  Property (BAP), 70
  Property ($\mathtt{HR}^+_<$), 73
  Property ($\mathtt{HR}_<$), 65
  Property ($\mathtt{LG}^+_\mathtt{A}$), 72
  Property ($\mathtt{LG}_\mathtt{A}$), 65
  Property ($\mathtt{M}^+$), 72
  Property (M), 62

Quotient Field, 32

Radical Relation, 83
Regularly r-closed, 71
Ring of Adeles of $\mathbb{Q}$, 75
Ring of Integral Adeles of $\mathbb{Q}$, 75
Robinson Arithmetic, 123

Strong Approximation Property, 70

Topology
  $\tau_1$-space, 53
  Constructive Topology, 50

Universal Frattini Cover, *see* Projective Cover

Valuation, 34
Valuation Ring, 32
    Henselian, 39
Valuation Rings
    Domination, 37

Wonderful Extension of $\mathbb{Q}$, *see also* $W^+$-Extension