Decoding Arithmetic Structure from Absolute Galois Groups



Benedikt Stock

St Peter's College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Michaelmas 2025

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Jochen Koenigsmann, for his exceptional guidance, generosity, and unwavering support throughout my time at Oxford. His mentorship extended far beyond the sharing of mathematical ideas, as he created a warm and stimulating environment for his students by inviting us to dinners, organising conferences, and encouraging us in countless other ways. Without his wisdom, enthusiasm, and the many stimulating discussions we shared, this thesis would not have been possible.

I am also profoundly grateful to Franziska Jahnke, who generously sponsored two research visits to the University of Münster and provided many fresh ideas and invaluable discussions that have shaped this work. Her insight, encouragement, and kindness have greatly enriched this thesis. I would also like to thank Sylvy Anscombe, Philip Dittmann, and Kostas Kartas for their many constructive conversations and for sharing their ideas and perspectives over the years. My gratitude extends to all members of the Oxford Logic Group, whose thoughtful questions and feedback have been a continual source of inspiration. In particular, I am indebted to Leo Gitin, a dear friend during our shared time at Oxford, for countless mathematical and non-mathematical conversations, as well as for his thoughtful comments and feedback on my work.

I feel very fortunate to have found such close friendships in Oxford. The warmth, kindness, and companionship of my friends made both the Mathematical Institute and St Peter's College truly feel like home. In particular, I would like to thank Álvaro, Atticus, Brian, Paweł, Finn, Robert, and Wojciech for their friendship, support, and countless stimulating discussions. I am also grateful to the following Oxford institutions for their significant contribution to my well-being: Formosan, Pepper's, and Edamame (in that order); the Oxford Philharmonic Orchestra; and the Oxford University Handball Club.

Finally, I owe my deepest gratitude to my family for their unwavering love, patience, and support throughout these years and beyond. To Camila, Linus, and my parents — thank you for being part of my mathematical journey. You are the foundation of everything I do; your love and encouragement make it all worthwhile.

Abstract

This thesis investigates how the arithmetic and model–theoretic properties of fields are encoded in their absolute Galois group. The guiding question throughout is: to what extent does the absolute Galois group of a field determine its arithmetic structure and properties?

The thesis consists of the following three projects addressing this theme.

An elementary proof of the local Kronecker–Weber theorem. We develop a new, elementary, and self–contained proof of the local Kronecker–Weber theorem that entirely avoids the machinery of class field theory and Galois cohomology. The argument relies only on valuation theory, Kummer theory, and fundamental results from infinite Galois theory, and yields an explicit construction of a cyclotomic extension containing the abelian one.

A new proof of the Galois characterisation of p–adically closed fields. We present a modern, simplified, and self–contained proof of the result by Koenigsmann and Efrat that a field is p–adically closed if and only if its absolute Galois group is isomorphic to that of $\mathbb{Q}_p$. Drawing on novel techniques in the theory of valued fields developed over the last 25 years, the proof is elementary in that it avoids reliance on local class field theory or Galois cohomology.

A cohomological approach to fields elementarily characterised by their absolute Galois group. We revisit the unresolved "Case 4" in Koenigsmann's classification of fields that are elementarily characterised by their absolute Galois group. By connecting this case to cohomological dimension and local–global principles in Galois cohomology, we obtain a conditional elimination result: Case 4 is empty under the assumption that $\mathbb{F}_p(t)^{\mathrm{solv}}$ is pseudo–algebraically closed (PAC). This establishes a new link between the model–theoretic classification problem and an open question in field arithmetic.

Contents

1 Introduction **1**

1.1 Motivation 1

1.2 Goals and results 6

1.3 Structure of this thesis 8

2 An elementary proof of the local Kronecker–Weber theorem **10**

2.1 Some facts about local number fields 11

2.1.1 Cyclotomic extensions of local fields 11

2.1.2 Residues and generators in $\mathbb{Q}_p$ 13

2.2 Proof of the local Kronecker–Weber theorem 18

2.2.1 The tame case 18

2.2.2 The wild case 20

3 Galois characterisation of p-adically closed fields **34**

3.1 Methods in valuation theory 36

3.1.1 Valuations, valuation rings, and places 37

3.1.1.1 Ordered abelian groups 37

3.1.1.2 Valuations and valuation rings 37

3.1.1.3 Places 39

3.1.1.4 Extensions of valuations 40

3.1.2 Structure theory 42

3.1.2.1 General ramification theory 43

3.1.2.2 Henselianity 48

3.1.2.3 p-henselianity 50

3.1.3 Coarsenings and decomposition 51

3.1.3.1 Composition of places 53

3.1.3.2 Standard Decomposition 54

3.1.3.3 Canonical henselian valuation 55

3.1.3.4 "Henseling down" . . . 58
3.1.4 Creation of valuations . . . 60
3.1.4.1 Creating valuations from rigid elements . . . 61
3.1.4.2 Creating valuations from p-rigid elements . . . 65
3.1.5 First-order languages for valued fields . . . 67
3.2 Valuations and absolute Galois groups . . . 68
3.2.1 The explicit structure of $\mathbb{Q}_p$ . . . 68
3.2.1.1 Cyclotomic extensions . . . 68
3.2.1.2 Counting in $\mathbb{Q}_p$ . . . 70
3.2.2 Fields with finite p-rank . . . 76
3.2.3 Distinguishing characteristics of fields . . . 77
3.2.4 Transfer of Galois groups between different characteristics . . . 82
3.2.5 Galois characterisation of henselianity . . . 87
3.3 Proof of the Galois characterisation of p-adically closed fields . . . 97

4 Towards eliminating Case 4 **107**
4.1 Local–global principles in Galois cohomology . . . 107
4.1.1 Review of Galois cohomology . . . 107
4.1.1.1 Definitions and examples . . . 108
4.1.1.2 Cohomological dimension . . . 117
4.1.1.3 The Albert–Brauer–Hasse–Noether Theorem . . . 121
4.1.2 Modern cohomological local–global principles . . . 123
4.1.2.1 Degree $n = 1$ . . . 123
4.1.2.2 Degree $n = 2$ . . . 125
4.1.2.3 Higher dimensions . . . 129
4.1.2.4 Extending to non-finitely generated fields . . . 132
4.2 Cohomological local–global approach to eliminate Case 4 . . . 134
4.2.1 Cohomological conjectures and Case 4 . . . 135
4.2.2 Reducing Case 4 to weaker conjecture . . . 138
4.2.3 Attempts to resolve weaker conjecture . . . 140
4.3 Related work and discussion . . . 143

Bibliography **146**

Chapter 1

Introduction

1.1 Motivation

This thesis is motivated by the observation that Galois groups encode surprisingly rich arithmetic information about their underlying fields. By definition, a Galois group consists of those permutations of the roots of a separable polynomial that preserve all algebraic relations among them. Despite the simplicity of this definition, these symmetries carry a remarkable amount of information about the arithmetic of the underlying field.

The origins of this insight trace back to one of the oldest problems in algebra, spanning from the Renaissance to the beginning of the modern era: the quest to solve polynomial equations using radicals. Solutions were known for equations of degrees $n = 1, 2, 3, 4$, but all attempts to extend these methods to the quintic ultimately failed. In the early nineteenth century, Ruffini, Abel, and finally Galois provided the definitive explanation: no such formula can exist in general for equations of degree five or higher. Galois's breakthrough lay in shifting the perspective from the roots themselves to the symmetries among them, leading to the study of the corresponding Galois group. What began as an investigation into explicit formulas for equations thus evolved into a deep connection between field theory and group theory. In particular, Galois's main theorem established that a polynomial is solvable by radicals if and only if its Galois group is a solvable group.

Since its inception, Galois theory has developed far beyond the study of solving polynomials by radicals. Its ideas now permeate much of modern mathematics, from algebraic geometry to number theory. A striking illustration of this connection is the *Kronecker–Weber theorem* in number theory, which asserts that every finite

abelian extension of the rational numbers is contained in a cyclotomic field—that is, a field obtained by adjoining roots of unity. In other words, if the Galois group of a polynomial with rational coefficients is abelian, we can express its roots as linear combinations of roots of unity with rational coefficients.

From the insolubility of the quintic to the classification of abelian extensions, Galois theory reveals a consistent theme: *Galois groups encode many aspects of the arithmetic of their underlying field.* Naturally, the question arises if we can be more precise and quantify how much arithmetic information Galois groups encode. This is the guiding principle for this thesis.

As a starting point in making this question more precise, for a given a field K, we consider its absolute Galois group, a canonical object of symmetries that collects the finite Galois groups of K at once:

$$G_K \coloneqq \mathrm{Gal}(K^{\mathrm{sep}}/K) = \varprojlim_{L/K \text{ finite Galois}} \mathrm{Gal}(L/K).$$

This definition expresses G_K as the inverse limit of the finite Galois groups of K. G_K is the largest possible Galois group attached to K and is naturally a profinite group with the Krull topology: every finite Galois group of K occurs as a quotient of G_K by an open subgroup.

Viewing G_K this way suggests a natural question: to what extent does this profinite group determine the arithmetic of the base field?

In a first instance, one might wonder if G_K determines K up to isomorphism. Quickly, however, we see that this is not the case: For example, already the trivial group appears as the absolute Galois group of any algebraically closed field. However, examples like the algebraic numbers $\widetilde{\mathbb{Q}}$, the complex numbers $\mathbb{C}$, or the algebraic closure of a finite field $\widetilde{\mathbb{F}_p}$ show that G_K determines neither the cardinality nor the characteristic of such fields.

So perhaps expecting G_K to determine *all* of the structure of K is a bit overly optimistic. What if we restrict our attention only to certain fields? Here, we have the following striking result:

Theorem 1.1.1 (Neukirch-Uchida)**.** *Let K_1 and K_2 be algebraic number fields. Any topological isomorphism $G_{K_1} \cong G_{K_2}$ is given by conjugation by a field isomorphism*

$$\sigma : \widetilde{K_1} \xrightarrow{\cong} \widetilde{K_2}$$

restricting to $\sigma|_{K_1} : K_1 \xrightarrow{\cong} K_2$. *In particular, working within a fixed algebraic closure* $\widetilde{\mathbb{Q}}$ *of* $\mathbb{Q}$, *any two number fields* K_1 *and* K_2 *satisfy*

$$K_1 \cong K_2 \iff G_{K_1} \cong G_{K_2}. \tag{1.1.1}$$

By a result of Mochizuki [Moc97, Theorem 4.2], there is an analogous result for local number fields if we restrict ourselves even further to fields with a certain ramifaction filtration. Either way, the Neukirch-Uchida theorem and Mochizuki's result exemplify that, in general, we can only expect the absolute Galois group G_K of a field K to determine K up to isomorphism in very restricted classes of fields.

Looking back at our original question, our motivation was to determine how much of the *arithmetic* of a field K is determined in G_K. In the above results, G_K determined K up to isomorphism (within certain restricted classes), thus capturing the *entire* structure of K. However, one may wonder if it is possible to find a weaker and less restrictive notion that captures more precisely the algebraic properties (like the roots of polynomials and the characteristic) and might allow for more general results. This is where model theory and first-order logic enter the picture.

From the point of view of first-order logic, the arithmetic of K is precisely the first-order properties of K in the language of rings, i.e., the set of first-order sentences satisfied in K in a language with symbols for ring operations $\mathcal{L}_{\text{ring}} = \{0, 1, +, -, \cdot\}$. Viewed through this lens, maybe the question of how much of the *first-order properties* of K are encoded in G_K better captures our original motivation. For instance, in our above example where $G_K = 1$, once we fix the characteristic p (where we allow $p = 0$) of our field, the possible fields K are exactly the models of ACF_p, the theory of algebraically closed of characteristic p, which is complete [Mar02, Corollary 3.2.3].

While we were forced to fix the characteristic of our fields, the reader will agree that this is much less of a restriction than in the settings of Neukirch-Uchida's or Mochizuki's theorems. However, algebraically closed fields are far from the only examples. There are other fields for which the absolute Galois group G_K encodes (almost) all of the first-order properties of K. In fact, historically, the first non-trivial class of fields for which such a result was obtained is the class of *real closed fields*, i.e., fields that admit an ordering which does not extend to any proper algebraic extension of K.

By the classical theorem of Artin and Schreier [AS27a, AS27b], real closed fields are characterised by having absolute Galois group C_2, the cyclic group of order 2:

Theorem 1.1.2 (Artin-Schreier)**.** *Let K be a field. The absolute Galois group G_K is finite if and only if*

(i) $|G_K| = 1$*, in which case K is separably closed, or*

(ii) $|G_K| = 2$*, in which case K is real closed.*

At the advent of *model theory*, Tarski identified the real closed fields as precisely those structures that are elementarily equivalent to $\mathbb{R}$.

Theorem 1.1.3. *A field K is real closed if and only if $K \equiv \mathbb{R}$, i.e., K is elementarily equivalent to $\mathbb{R}$.*

See [Mar02, 3.3] for a modern presentation of Tarski's Theorem. Crucially, for a real closed field K the formula $\exists z\,(y - x = z^2)$ defines the unique ordering $x \leq y$ that makes K an ordered field. This is an instance of the phenomenon that G_K encodes *extra structure* on K.

Combining the results of Tarski and Artin-Schreier, we see that any field with absolute Galois group C_2 is elementarily equivalent to K, i.e., the absolute Galois group encodes all of the arithmetic properties of K. Let us give a name to this concept and call such fields *elementarily determined* by their absolute Galois group. In fact, Tarski and Artin-Schreier's results show even more: any field elementarily equivalent to K has an isomorphic absolute Galois group. In such cases, we say that a field is *elementarily characterised* by its absolute Galois group.

Definition 1.1.4. A field K is *elementarily determined* by its absolute Galois group G_K if for all fields L,

$$G_K \cong G_L \implies K \equiv L$$

in the language of rings.

K is *elementarily characterised* by G_K if for all fields L,

$$G_K \cong G_L \iff K \equiv L.$$

Throughout, we will tacitly assume that isomorphisms between profinite groups are topological group isomorphisms.

Drawing inspiration from Artin and Schreier's result, Pop formulated an analogous conjecture for the p-adic numbers $\mathbb{Q}_p$, the completions of $\mathbb{Q}$ with respect to the non-Archimedean valuations v_p [Pop88, Vermutung E.7]. Let us explore Pop's conjecture a bit further.

In analogy to real closed fields, fields elementarily equivalent to $\mathbb{Q}_p$ are known as *p-adically closed fields*. The arithmetic of such fields is well-understood by the following celebrated result of Ax, Kochen [AK65], and Ershov [Ers65].

Theorem 1.1.5 (Ax-Kochen/Ershov 1965)**.** *A field K is elementarily equivalent to $\mathbb{Q}_p$ if and only if it admits a (Krull) valuation v such that:*

(i) *(K, v) is henselian of mixed characteristic $(0, p)$;*

(ii) *$v(p)$ is minimal positive;*

(iii) *the value group vK is a $\mathbb{Z}$-group, i.e., $vK \equiv \mathbb{Z}$;*

(iv) *the residue field is equal to $\mathbb{F}_p$.*

In an early advance towards a Galois characterisation of p-adically closed fields, Pop [Pop88, Theorem E.11] established such a characterisation in a restricted setting.

Theorem 1.1.6 (Pop 1988)**.** *Let K be a field with $\widetilde{K} = K\widetilde{\mathbb{Q}}$. Then*

$$G_K \cong G_{\mathbb{Q}_p} \iff K \equiv \mathbb{Q}_p.$$

Pop conjectured [Pop88, E.7] that his theorem holds without any extra restrictions on K. The conjecture was independently solved by Efrat [Efr95c] (for $p \neq 2$) and Koenigsmann [Koe95] (for all primes p).

Theorem 1.1.7. *For any field K,*

$$G_K \cong G_{\mathbb{Q}_p} \iff K \equiv \mathbb{Q}_p$$

Perhaps the most notable feature of this result is the reappearance of the same phenomenon we have encountered in the case of real closed fields: the absolute Galois group of $\mathbb{Q}_p$ *encodes extra structure on* K, namely a valuation (of any potential rank), satisfying the axioms (i)–(iv) in Theorem 1.1.5. This provides a striking piece of evidence for the point of view that higher rank valuations appear "in nature"— even outside of model theory.

At this point, the reader may naturally ask whether there exist further fields that are elementarily characterised by their absolute Galois group, beyond those elementarily equivalent to $\mathbb{Q}_p$ or $\mathbb{R}$. Indeed, this is the case: The following classification theorem by Koenigsmann [Koe04, Main Theorem] provides a complete description of all fields elementarily characterised by their absolute Galois group:

Theorem 1.1.8. *K is elementarily characterised by G_K if and only if K is elementarily equivalent to one of the following:*

1. $\mathbb{R}$*;*
2. *a finite extension L of $\mathbb{Q}_p$ with $([L : L^{ab}], \frac{p}{p-1}\#\mu_L) = 1$, where L^{ab} denotes the maximal abelian subextension of $L/\mathbb{Q}_p$;*
3. *$L((t^{\mathbb{Z}_{(q)}}))$, where L is as in Case 2 and q an arbitrary prime;*
4. *$L((t^{\mathbb{Z}_{(p)}}))$, where L is such that*
   - $\operatorname{char} L = 0$,
   - *$L/\mathbb{Q}$ is of finite transcendence degree,*
   - *L admits no proper abelian extension,*
   - *L has a henselian valuation with residue characteristic p,*
   - *L is elementarily determined by G_L only among fields of characteristic not equal to p,*
   - $\operatorname{cd}_p G_L = 1$*, where $\operatorname{cd}_p G_L$ is the p-th cohomological dimension of G_L;*
5. *a field L elementarily characterised by G_L such that*
   - *G_L is not pro-solvable,*
   - *for all F, if $G_F \cong G_L$, then $\operatorname{char} F = 0$ and $\operatorname{td}(F/\mathbb{Q})$ is infinite.*

Koenigsmann further observes that Cases 4 and 5 are currently poorly understood, and he conjectures that no such fields actually exist, leaving a clear direction for further investigation.

In light of these developments, this thesis seeks to advance our understanding of how arithmetic and model–theoretic properties of fields are encoded in their absolute Galois group, through three complementary projects described below.

1.2 Goals and results

This thesis can be broadly structured into three projects, each exploring the above theme of understanding how arithmetic information is encoded in absolute Galois groups.

The first project is concerned with the absolute Galois group of $\mathbb{Q}_p$ and comprises a new, elementary, and explicit proof of the local Kronecker–Weber theorem. The motivation for this project is that the known proofs of the local Kronecker–Weber theorem often rely on the fundamental theorem of local class field theory, a result that itself is usually either proved via a cohomological approach or Lubin–Tate theory. The proof presented here is self-contained and does not involve Lubin–Tate constructions or Galois cohomology. Instead, our argument relies only on discrete valuation theory combined with basic results from (infinite) Galois theory and Kummer theory, which moreover provides an explicit description of the corresponding cyclotomic extensions.

The second project is also concerned with $G_{\mathbb{Q}_p}$ and gives a new and elementary proof of Efrat and Koenigsmann's Theorem 1.1.7. We present a revised proof of Theorem 1.1.7 for three main reasons. First, the original arguments rely heavily on advanced machinery. The proof involves an analysis of Galois groups using Galois cohomology, class field theory, and computational analyses of henselian extensions, together with the use of rigid elements originating in quadratic form theory. At present, no self-contained exposition exists in the literature. Secondly, some of the underlying techniques have only recently been fully understood, and modern developments shed new light on several key steps. Finally, we offer a modern perspective that highlights interactions with recent developments.

We replace many of the earlier arguments with more elementary and explicit considerations, avoiding cohomological tools entirely. Instead, we introduce all of the necessary results from first principles. Some arguments refine results from the first project, while others provide explicit, elementary counterparts to previously cohomological constructions. Other arguments rely on methods that were only discovered after the original publication or more systematically explored and understood in recent years.

The third project shifts the focus from fields with the absolute Galois group of $\mathbb{Q}_p$ to more general fields that are elementarily characterised by their absolute Galois group. In light of Theorem 1.1.8, this project investigates approaches to showing that Case 4 in Theorem 1.1.8 is indeed empty—a process to which we shall refer as *eliminating Case 4*. The main emphasis will be on a cohomological approach based on local–global principles in Galois cohomology.

We connect the problem of eliminating Case 4 to Galois cohomology by reducing it to a statement about the cohomological dimension of certain fields. To prove

this statement, we outline a local–global approach and examine both classical and modern local–global principles regarding their applicability to this problem. This approach allows us to deduce the following conditional result, which links the elimination of Case 4 to a currently open problem in field arithmetic:

Proposition 1.2.1. *Case 4 is eliminated if* $\mathbb{F}_p(t)^{\mathrm{solv}}$ *is a PAC field.*

Finally, we sketch a potential alternative, non-cohomological approach to the elimination of Case 4 and contrast it with the local–global approach and other related work.

Hence, the main contributions of the three projects can be summarised as follows:

1. A new elementary, self-contained, and explicit proof of the local Kronecker–Weber theorem, avoiding cohomological methods and relying instead on valuation-theoretic and Kummer-theoretic arguments.
2. A modern, simplified, and self-contained proof of the Galois characterisation of p-adically closed fields (Theorem 1.1.7), developed without appeal to class field theory or Galois cohomology.
3. A cohomological local–global analysis of fields elementarily characterised by their absolute Galois group, leading to a conditional elimination of *Case 4* in Koenigsmann's classification theorem (Theorem 1.1.8).

The first project is based on a joint preprint [KS22] with my supervisor, Jochen Koenigsmann, while the second is based on a collaboration with Leo Gitin and Jochen Koenigsmann [GKS]. With the exception of the initial sections, which consist of standard background material, Leo Gitin and I worked on distinct components of the proof presented here. Whenever the exposition draws on material from our joint preliminary sections, this is explicitly indicated. Likewise, when the presentation relies on results due to Gitin, these are cited explicitly, with references to the relevant sections of the preprint for further details.

1.3 Structure of this thesis

The three projects that constitute this thesis increase progressively in difficulty and level of abstraction, both in the arguments developed and in the mathematical machinery employed. The first project adopts a concrete, hands-on approach, working exclusively with classical (discrete rank-1) valuations. The second generalises

these ideas to general valuations and introduces concepts originating from other areas, while largely retaining an elementary and self-contained treatment. The third project, finally, introduces cohomological methods into the discussion, drawing upon several of the valuation-theoretic results discussed in the second one.

The Projects 1, 2, and 3 are presented in Chapters 2, 3, and 4, respectively.

- **Chapter 2** naturally divides into two parts. The first part recalls essential facts for local number fields, while the second part contains the proof of the local Kronecker–Weber theorem.
- **Chapter 3** contains a dedicated section for each of the principal methods used, including general valuation theory and methods to decode and transfer absolute Galois groups. The final section presents the new proof of the Galois characterisation of p-adically closed fields.
- **Chapter 4** begins with an introduction to Galois cohomology and an overview of current research on cohomological local–global principles. The remainder of the chapter connects these results to the elimination of Case 4, culminating in the conditional elimination described above.

Chapter 2

An elementary proof of the local Kronecker–Weber theorem

The Kronecker–Weber theorem states that every finite abelian extension of the rational numbers is contained in a cyclotomic extension.

A number of proofs of this result are known. Culler [Cul07] presents two proofs; an elementary approach based on David Hilbert's original proof and one that makes use of class field theory. Another classical approach proceeds via the local Kronecker–Weber theorem—the subject of this chapter—in which $\mathbb{Q}$ is replaced by $\mathbb{Q}_p$. Once the local version is established, it is not hard to deduce the global version via completions, Minkowski's bound, and basic properties of discriminants (cf. [Gui18, Chapter 14] for an excellent presentation of a complete proof).

As in the global case, several proofs of the local Kronecker–Weber theorem are known. Perhaps the most classical one goes via the fundamental theorem of local class field theory, a result that itself is usually either proved via the cohomological approach (cf. [Gui18]) or Lubin–Tate theory (cf. [Chi08, Haz75]). Our proof is distinct from those as it makes no mention of local class field theory at all. Papers by Rosen [Ros81] and Kozuka [Koz90] have a similar goal in mind. However, the new approach presented here differs from these in that it is self-contained and does not even mention Lubin–Tate constructions or Galois cohomology. Instead, our considerations are merely based on discrete valuation theory combined with basic results from Galois theory and Kummer theory. Moreover, it is explicit in that it provides a formula for a cyclotomic extension containing the given abelian extension, described in terms of the degree of the abelian extension. A proof with a similar structure to ours can be found in Washington's classical book [Was97, Chapter 14];

we will discuss the key similarities and differences in more detail at the end of this chapter in Remark 2.2.10.

In the next Section 2.1 we will remind the reader of some facts about local fields before presenting the proof of the local Kronecker–Weber theorem in Section 2.2.

2.1 Some facts about local number fields

Let us first fix some notation. We call finite extensions of $\mathbb{Q}_p$ *local number fields* or *p-adic fields*. For a p-adic field F, we denote by v_F (or simply v when the field is clear from context) the unique extension of the p-adic valuation v_p to F. We write $\mathcal{O}_F$ for the ring of integers of F, $\mathcal{M}_F$ for its unique maximal ideal, and Fv (or $\overline{F}$ when the valuation is clear from context) for its residue field $\mathcal{O}_F/\mathcal{M}_F$.

For an extension L/F of local number fields of degree n, we denote by $e = e(L/F)$ and $f = f(L/F)$ the *ramification index* and *inertia degree* of the extension L/F, respectively. We recall the fundamental equality $n = ef$ (cf. [Gui18, Theorem 2.38], [Neu99, II. 6.8]). More precisely, there exists an intermediate field L_0, called the *inertia subfield* of L, with the property that for any intermediate field $F \subseteq K \subseteq L$, the extension K/F is unramified if and only if $K \subseteq L_0$ (cf. [Gui18, Corollary 2.43]). For a more detailed treatment of these notions in the context of general valued fields, we refer the reader to Section 3.1.2 in the next chapter.

2.1.1 Cyclotomic extensions of local fields

We introduce some additional notation. For a field F, let μ_F denote the set of all roots of unity contained in F. Whenever F contains all n-th roots of unity for some $n \in \mathbb{N}_{>0}$, we write this set as μ_n. A fixed primitive n-th root of unity is denoted by ζ_n, and we write ζ_{q^∞} for the set of all q-power roots of unity. Finally, when several roots of unity are involved, we tacitly assume that they form a compatible system (for example, $\zeta_{q^2}^q = \zeta_q$).

Recall that the cyclotomic extensions of $\mathbb{Q}_p$ admit explicit descriptions (see [Gui18, Propositions 2.46 and 2.48]), which are summarised in the following lemma.

Lemma 2.1.1. *Let $F = \mathbb{Q}_p(\mu_m)$ be a cyclotomic extension of $\mathbb{Q}_p$.*

(i) If $(m, p) = 1$, then $F/\mathbb{Q}_p$ is unramified of degree $k = \mathrm{ord}_m(p)$, the order of $p + m\mathbb{Z}$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. Moreover,

$$\mathrm{Gal}(F/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{F}_{p^k}/\mathbb{F}_p) \cong C_k.$$

(ii) If $m = p^l$, then $F/\mathbb{Q}_p$ is totally ramified of degree $(p-1)p^{l-1}$ and $1-\zeta_{p^l}$ is a uniformiser. Moreover,

$$\mathrm{Gal}(F/\mathbb{Q}_p) \cong \left(\mathbb{Z}/p^l\mathbb{Z}\right)^\times.$$

Proof (Sketch). (i). We first observe that $\zeta_m \in \mathcal{O}_F$ since $\zeta_m^m = 1$ implies $v_F(\zeta_m) = 0$. In particular, the minimal polynomial $f(X)$ of ζ_m over $\mathbb{Q}_p$ lies in $\mathbb{Z}_p[X]$, so $\overline{f}(X) \in \mathbb{F}_p[X]$, where $\overline{f}(X)$ divides $X^m - 1$. Since $(m,p) = 1$, this means $\overline{f}(X)$ is separable over $\mathbb{F}_p$, and hence irreducible by Hensel's Lemma. In particular, $n = f$ and $\overline{F} = \mathbb{F}_p(\overline{\zeta_m})$. By the fundamental equality $n = ef$, we obtain $e = 1$, so $F/\mathbb{Q}_p$ is unramified.

By the Galois theory of finite fields, $\mathrm{Gal}(\overline{F}/\mathbb{F}_p)$ is cyclic of order k, generated by the Frobenius automorphism $x \mapsto x^p$, which is determined entirely by its action on $\overline{\zeta_m}$. The order of the Frobenius automorphism is therefore the smallest positive number k for which $\overline{\zeta_m}^{p^k} = \overline{\zeta_m}$, i.e., $p^k \equiv 1 \pmod{m}$, so $k = \mathrm{ord}_m(p)$. Finally, using again that any element in $\mathrm{Gal}(\overline{F}/\mathbb{F}_p)$ is determined by the image of $\overline{\zeta_m}$, every such element lifts to an element of $\mathrm{Gal}(F/\mathbb{Q}_p)$, which means the natural restriction map

$$\mathrm{Gal}(F/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{F}/\mathbb{F}_p)$$

is surjective. Since $f = n$, this restriction is in fact an isomorphism of Galois groups, from which the remaining claims follow.

(ii). Define

$$\Phi(X) \coloneqq 1 + X^{p^{l-1}} + \cdots + X^{(p-1)p^{l-1}}.$$

It is easy to see that $\Phi(\zeta_{p^l}) = 0$. Moreover, applying the Eisenstein criterion to $\Phi(X+1)$, we see that $\Phi(X)$ is irreducible, which means Φ is the minimal polynomial of ζ_{p^l} over $\mathbb{Q}_p$. The other roots of Φ are exactly the $\phi(p^l) = (p-1)p^{l-1}$ primitive p^l-th roots of unity of the form $\zeta_{p^l}^i$ for $(i,p) = 1$. Hence, the elements of $\mathrm{Gal}(F/\mathbb{Q}_p)$ are precisely determined by $\zeta_{p^l} \mapsto \zeta_{p^l}^i$, from which we recover the usual isomorphism $\mathrm{Gal}(F/\mathbb{Q}_p) \cong (\mathbb{Z}/p^l\mathbb{Z})^\times$.

Next, we observe that for every $\sigma \in \mathrm{Gal}(F/\mathbb{Q}_p)$, $v(\sigma(x)) = v(x)$ for all $x \in F$ by the uniqueness of v. Hence, using

$$p = \Phi(1) = \prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q}_p)} \sigma(1 - \zeta_{p^l}),$$

we see that $v(1-\zeta_{p^l}) = \frac{v(p)}{[F:\mathbb{Q}_p]}$. Thus, $1-\zeta_{p^l}$ is the required uniformiser, and it also witnesses that $F/\mathbb{Q}_p$ is totally ramified. □

From the fact that $\mathbb{F}_p^\times = \mu_{p-1}$, we obtain the following description of the roots of unity in $\mathbb{Q}_p$.

Corollary 2.1.2. *In $\mathbb{Q}_p$, the roots of unity are*

$$\mu_{\mathbb{Q}_p} = \begin{cases} \mu_{p-1} & \text{if } p \neq 2; \\ \mu_2 & \text{if } p = 2. \end{cases}$$

2.1.2 Residues and generators in $\mathbb{Q}_p$

The goal of this section is to study the multiplicative structure of p-adic fields by explicit means. Our starting point is the filtration

$$F^\times \supseteq U_F^{(0)} \supseteq U_F^{(1)} \supseteq \cdots \supseteq U_F^{(k)} \supseteq \cdots$$

of the multiplicative group $F^\times$ of a p-adic field F by *higher unit groups*.

Definition 2.1.3. Let F be a p-adic field with uniformiser π. The *k-th higher unit group* ($k \in \mathbb{N}$) is defined as

$$\begin{aligned} U_F^{(0)} &\coloneqq \mathcal{O}_F^\times; \\ U_F^{(k)} &\coloneqq \left\{ x \in \mathcal{O}_F^\times : x \equiv 1 \pmod{\pi^k} \right\} \quad \text{for } k \geq 1. \end{aligned}$$

For the remainder of this section, we display some calculations involving higher unit groups, some of which are standard and others which may be less well-known.

Fact 2.1.4. *Let F be a p-adic field with uniformiser π. Denote its prime-to-p roots of unity by μ'_F. The multiplicative group $F^\times$ can be decomposed as the direct product*

$$F^\times = \pi^{\mathbb{Z}} \times \mu'_F \times U_F^{(1)}.$$

Proof. Any $x \in F^\times$ can be uniquely written as $x = \pi^{v(x)}(\pi^{-v(x)}x)$, where $\pi^{-v(x)}x \in \mathcal{O}_F^\times$. Therefore, $F^\times = \pi^{\mathbb{Z}} \times \mathcal{O}_F^\times$. Now,

$$1 \to U_F^{(1)} \to \mathcal{O}_F^\times \to \overline{F}^\times \to 1 \tag{2.1.1}$$

is split via the section $\overline{\omega} \mapsto \omega$ for each $\omega \in \mu'_F$, so $\mathcal{O}_F^\times = \mu'_F \times U_F^{(1)}$ as required. □

Fact 2.1.5. *Let F be a p-adic field. For any $k \geq 1$, there exist isomorphisms*

$$\begin{aligned} U_F^{(0)}/U_F^{(1)} &\cong (\overline{F}^\times, \cdot) \\ U_F^{(k)}/U_F^{(k+1)} &\cong (\overline{F}, +). \end{aligned}$$

Proof. The first isomorphism is an immediate consequence of the short exact sequence (2.1.1). For $k \geq 1$, the map

$$\begin{aligned} U_F^{(k)}/U_F^{(k+1)} &\longrightarrow \overline{F}, \\ (1+\pi^k a)U_F^{(k+1)} &\longmapsto a + \mathcal{M}_F \end{aligned}$$

is a well-defined group isomorphism; see [Neu99, Chapter II, (3.10)], [Gui18, Lemma 2.56], and Remark 2.1.6 below. □

Remark 2.1.6. The fact that the above maps are indeed isomorphisms relies on the following rule linking additive and multiplicative congruences: for any $a, a' \in U_F^{(0)}$,

$$a \equiv a' \pmod{\pi^k} \quad \text{if and only if} \quad a \equiv a' \pmod{U_F^{(k)}}.$$

The equivalence is easily verified:

$$\exists b \in \mathcal{O}_F : a' = a + b\pi^k \iff \exists b \in \mathcal{O}_F : \frac{a'}{a} = 1 + a^{-1}b\pi^k \iff \frac{a'}{a} \in U_F^{(k)}.$$

Corollary 2.1.7. *Let F be a p-adic field and $\mathcal{A} \subseteq \mathcal{O}_F$ be a set of representatives for $\overline{F} = \mathcal{O}_F/\mathcal{M}_F$. Then any $x \in U_F^{(1)}/U_F^{(k+1)}$ has a unique representation of the form $x = aU_F^{(k+1)}$, where*

$$a = 1 + a_1\pi + \cdots + a_k\pi^k,$$

and all coefficients a_i lie in $\mathcal{A}$.

Proof. Assume that $a = 1 + \sum_{i=1}^{k} a_i\pi^i$ and $a' = 1 + \sum_{i=1}^{k} a_i'\pi^i$ represent the same element modulo $U_F^{(k+1)}$. In other words, there exists $1 + \pi^{k+1}b \in U_F^{(k+1)}$ with $a = a'(1+\pi^{k+1}b)$. Assume $a_i \neq a_i'$ for some i, in which case we choose the minimal such i. Then

$$v(a - a') = v((a_i - a_i')\pi^i) = v(\pi^i),$$

which contradicts $a - a' = a'\pi^{k+1}b$. Therefore, $a_i = a_i'$ for all $i = 1, \ldots, k$.

The fact that any element in $U_F^{(1)}/U_F^{(k+1)}$ can be written as claimed follows from a counting argument. Observe that

$$\left|U_F^{(1)}/U_F^{(k+1)}\right| = \left|U_F^{(1)}/U_F^{(2)}\right| \cdots \left|U_F^{(k)}/U_F^{(k+1)}\right| = |\overline{F}|^k$$

by Fact 2.1.5, which is exactly the number of distinct representatives we consider. □

The following residue calculation is crucial for many of the results that follow.

Lemma 2.1.8. *Let F be a p-adic field containing ζ_p and let $\pi = \zeta_p - 1$. Then*

$$\frac{p}{\pi^{p-1}} \equiv -1 \pmod{\pi}.$$

In particular, p/π^{p-1} reduces to -1 in the residue field.

Proof. Consider

$$f(X) = X^{p-1} + \cdots + X + 1 = \prod_{i=1}^{p-1}(X - \zeta_p^i).$$

Observe that

$$\frac{p}{\pi^{p-1}} = \frac{f(1)}{(-1)^{p-1}(1-\zeta_p)^{p-1}} = (-1)^{p-1}\prod_{i=1}^{p-1}\left(\frac{1-\zeta_p^i}{1-\zeta_p}\right) = (-1)^{p-1}\prod_{i=1}^{p-1}\sum_{j=0}^{i-1}\zeta_p^j.$$

For each factor, we compute

$$\sum_{j=0}^{i-1}\zeta_p^j = \sum_{j=0}^{i-1}(1+\pi)^j \equiv \sum_{j=0}^{i-1} 1 = i \pmod{\pi}.$$

The claim then follows using that $p \in (\pi)$, $(-1)^{p-1} \equiv 1 \pmod{p}$, and Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$. □

The three following results and their proofs are slight adaptations of an idea first observed by Koenigsmann [Koe03, Lemma 3.2].

Lemma 2.1.9. *Let $F/\mathbb{Q}_p(\zeta_p)$ be a finite extension with ramification index $e := e(F/\mathbb{Q}_p(\zeta_p))$. Then*

$$U_F^{(ep+1)} \subseteq \left(U_F^{(e)}\right)^p.$$

Proof. Recall that $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is totally ramified of degree $p-1$ by Lemma 2.1.1. Let $\pi = \zeta_p - 1$ be a uniformiser for $\mathbb{Q}_p(\zeta_p)$ and Π any uniformiser for F. If the valuation v on F is normalised such that $v(p) = 1$, then $v(\pi) = \frac{1}{p-1}$ and $v(\Pi) = \frac{1}{e(p-1)}$. In particular,

$$U_F^{(e)} = 1 + (\pi) \quad \text{and} \quad U_F^{(ep+1)} = 1 + (\pi^p\Pi).$$

Let $x = 1 + \pi^p a$ with $a \in (\Pi)$ be given. Then it suffices to show that

$$(1+\pi X)^p - (1+\pi^p a) = 0$$

has a solution in $\mathcal{O}_F$. Consider

$$f(X) := \frac{1}{\pi^p}\Big[(1+\pi X)^p - (1+\pi^p a)\Big] = X^p - a + \sum_{i=1}^{p-1}\binom{p}{i}\pi^{i-p}X^i.$$

Noting that

$$p\pi^{1-p} \equiv -1 \pmod{\pi}$$

for $i = 1$ by Lemma 2.1.8, and

$$v\left[\binom{p}{i}\pi^{i-p}\right] = v(p) + (i-p)v(\pi) = (i-1)v(\pi) > 0$$

for $i = 2, \dots, p-1$, we conclude that $f(X)$ reduces to $\overline{f}(X) = X^p - X \in \overline{F}[X]$. Thus, the claim follows by Hensel's Lemma. □

In the above proof, we could also start with an element $x = 1 + \pi^p a$ with $a \in \mathcal{O}_F$ instead of $a \in (\Pi)$. In that case, $x \in F^p$ is equivalent to the existence of a solution to the equation

$$X^p - (1 + \pi^p a) = 0.$$

Applying a change of variables $X \mapsto 1 + \pi X$, and using the same arguments as before, this becomes equivalent to $X^p - X - \overline{a}$ having a solution in $\overline{F}$ (in fact, a posteriori, this even shows equivalence with $x \in \left(U_F^{(e)}\right)^p$). We record this fact, which is essentially Koenigsmann's original statement, in the following lemma.

Lemma 2.1.10. *Let $F/\mathbb{Q}_p(\zeta_p)$ be a finite extension and $a \in \mathcal{O}_F$. Then*

$$1 + \pi^p a \in F^p \iff \exists z \in \overline{F} : z^p - z - \overline{a} = 0.$$

Next, we observe that the inclusion stated in Lemma 2.1.9 becomes an equality in the special case $F = \mathbb{Q}_p(\zeta_p)$.

Lemma 2.1.11. *For $F = \mathbb{Q}_p(\zeta_p)$, we have*

$$U_F^{(p+1)} = \left(U_F^{(1)}\right)^p.$$

Proof. The inclusion $U_F^{(p+1)} \subseteq \left(U_F^{(1)}\right)^p$ was shown in Lemma 2.1.9. For the reverse, let $(1 + \pi b)^p \in \left(U_F^{(1)}\right)^p$ for $b \in \mathcal{O}_F$. Then the considerations in the proof of Lemma 2.1.9 yield

$$(1 + \pi b)^p \equiv 1 - \pi^p b + \pi^p b^p = 1 + \pi^p(b^p - b) \pmod{\pi^{p+1}}.$$

Since $\overline{F} = \mathbb{F}_p$, we have $b^p \equiv b \pmod{\pi}$, and therefore

$$\left(U_F^{(1)}\right)^p \subseteq U_F^{(p+1)}.$$

□

The following result synthesises many of the considerations above, and it will play a central role in our proof of the local Kronecker–Weber theorem.

Lemma 2.1.12. *Let $F = \mathbb{Q}_p(\zeta_p)$ and let π be a uniformiser for F. Then the elements of $F^\times/F^{\times p}$ can be uniquely represented by*

$$a = p^{a_0}(1 + a_1\pi + \cdots + a_p\pi^p),$$

for some integers $0 \leq a_i \leq p-1$; in particular, $\dim_{\mathbb{F}_p} F^\times/F^{\times p} = p+1$.

Moreover, for any $b \coloneqq c\omega u$ with $c \in \pi^{\mathbb{Z}}$, $\omega \in \mu'_F$ and $u \in U_F^{(1)}$,

$$b \equiv a \pmod{F^{\times p}} \iff c \equiv p^{a_0} \pmod{\pi^{p\mathbb{Z}}} \wedge u \equiv 1 + a_1\pi + \cdots + a_p\pi^p \pmod{\pi^{p+1}}.$$

Proof. From Fact 2.1.4 and Lemma 2.1.11, we see that

$$F^\times/F^{\times p} \cong \pi^{\mathbb{Z}}/\pi^{p\mathbb{Z}} \times U_F^{(1)}/\left(U_F^{(1)}\right)^p = \pi^{\mathbb{Z}}/\pi^{p\mathbb{Z}} \times U_F^{(1)}/U_F^{(p+1)}. \tag{2.1.2}$$

Now, $\{p\}$ induces a basis of $\pi^{\mathbb{Z}}/\pi^{p\mathbb{Z}}$, since

$$p \equiv -\pi^{p-1} \pmod{\pi^p}$$

by Lemma 2.1.8, and $\{-\pi^{p-1} \cdot \pi^{p\mathbb{Z}}\}$ clearly forms a basis of $\pi^{\mathbb{Z}}/\pi^{p\mathbb{Z}}$. On the other hand, the elements of $U_F^{(1)}/U_F^{(p+1)}$ can be uniquely represented by elements

$$1 + a_1\pi + \cdots + a_k\pi^k$$

by Corollary 2.1.7, where we can choose each a_i as an integer with $0 \leq a_i \leq p-1$ because $F/\mathbb{Q}_p$ is totally ramified by Lemma 2.1.1. In particular, this means that $F^\times/F^{\times p}$ has cardinality p^{p+1}, which implies the claim about the dimension.

Next, (2.1.2) shows that

$$\begin{aligned} b \equiv a \pmod{F^{\times p}} \iff\ & c \equiv p^{a_0} \pmod{\pi^{p\mathbb{Z}}} \\ & \wedge\ u \equiv 1 + a_1\pi + \cdots + a_p\pi^p \pmod{U_F^{(p+1)}}. \end{aligned}$$

By Lemma 2.1.11, $U_F^{(p+1)} = \left(U_F^{(1)}\right)^p$ so the second congruence is equivalent to

$$u \equiv 1 + a_1\pi + \cdots + a_p\pi^p \pmod{\pi^{p+1}}$$

by Remark 2.1.6. □

Remark 2.1.13. In the next Chapter 3, we will generalise the dimension formula $\dim_{\mathbb{F}_p} F^\times/F^{\times p} = p+1$ in Lemma 2.1.12 from $F = \mathbb{Q}_p(\zeta_p)$ to general p-adic fields containing ζ_p (see Lemma 3.2.4). However, with the notable exception of the calculation in Lemma 2.2.8, we only require the formula for $F = \mathbb{Q}_p(\zeta_p)$. To keep the proof as comprehensible as possible, we decided to not prove the stronger and more complicated claim here, and instead perform a direct computation for the exceptional case in Lemma 2.2.8 below.

2.2 Proof of the local Kronecker–Weber theorem

We shall prove the following explicit version of the local Kronecker–Weber theorem.

Theorem 2.2.1 (Local Kronecker–Weber theorem)**.** *Let $F/\mathbb{Q}_p$ be an abelian extension of degree $n = p^l \cdot m$ with integers l and m such that $(p, m) = 1$. Then $F \subseteq \mathbb{Q}_p(\zeta_{p^{l+2}}, \zeta_{p^n-1})$.*

Since $F/\mathbb{Q}_p$ is abelian, its Galois group $G = \mathrm{Gal}(F/\mathbb{Q}_p)$ is finite abelian and hence (by the structure theorem for finite abelian groups) decomposes as

$$G = G_p \times G_{p'},$$

where G_p is the Sylow p-subgroup of G and $G_{p'}$ is the product of the Sylow l-subgroups for all primes $l \neq p$. Let L_p and $L_{p'}$ denote the fixed fields of G_p and $G_{p'}$, respectively. By the Galois correspondence,

$$[L_p : \mathbb{Q}_p] = |G_{p'}| = m \qquad \text{and} \qquad [L_{p'} : \mathbb{Q}_p] = |G_p| = p^l,$$

since $L_p/\mathbb{Q}_p$ has degree prime to p, while $L_{p'}/\mathbb{Q}_p$ has p-power degree. Moreover, because G is generated by G_p and $G_{p'}$, we have

$$L_p L_{p'} = F.$$

Consequently, it suffices to prove the theorem in the prime-to-p and p-power cases separately: if both L_p and $L_{p'}$ are contained in the cyclotomic extension appearing in Theorem 2.2.1, then so is F. We shall refer to the prime-to-p case as the *tame* case and to the p-power case as the *wild* case, following standard terminology that we will introduce in detail in Chapter 3.

2.2.1 The tame case

We first observe that in the notation of Theorem 2.2.1, $\mathbb{Q}_p(\zeta_{p^m-1}) \subseteq \mathbb{Q}_p(\zeta_{p^n-1})$ by Lemma 2.1.1 and the uniqueness of inertia fields. In particular,

$$\mathbb{Q}_p(\zeta_p, \zeta_{p^m-1}) \subseteq \mathbb{Q}_p(\zeta_{p^{l+2}}, \zeta_{p^n-1}).$$

In order to establish Theorem 2.2.1 in the tame case, it therefore suffices to show $L_p \subseteq \mathbb{Q}_p(\zeta_p, \zeta_{p^m-1})$, which is the statement of the following lemma.

Lemma 2.2.2. *Let $F/\mathbb{Q}_p$ be an abelian extension of degree n such that $(n, p) = 1$. Then $F \subseteq \mathbb{Q}_p(\zeta_p, \zeta_{p^n-1})$.*

Proof. We briefly outline the strategy of the proof. The unramified part of $F/\mathbb{Q}_p$ is cyclotomic by Lemma 2.1.1 and the uniqueness of inertia fields, so the analysis will focus on the ramified part. We show that the ramification is entirely controlled by adjoining $\sqrt[e]{-p}$. In particular, $\mathbb{Q}_p(\sqrt[e]{-p})/\mathbb{Q}_p$ is an intermediate abelian extension, which forces $\zeta_e \in \mathbb{Q}_p$. By Lemma 2.1.1, this implies $e \mid (p-1)$, giving an upper bound on the ramification index. Finally, we show that $\mathbb{Q}_p(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_p)$, which implies that the ramified part is cyclotomic as well.

Let F_0 denote the inertia subfield of $F/\mathbb{Q}_p$. By the uniqueness of inertia fields and Lemma 2.1.1, $F_0 = \mathbb{Q}_p(\zeta_{p^f-1})$. Let us also consider $E \coloneqq \mathbb{Q}_p(\zeta_{p^n-1})$, which is an unramified extension of $\mathbb{Q}_p$ satisfying $[E:\mathbb{Q}_p] = n$ and $[E:F_0] = e$ by the tower law and Lemma 2.1.1.

Let π be a uniformiser of F. As F is ramified of degree e, we have $v_F\left(\frac{\pi^e}{-p}\right) = 0$ so $\frac{\pi^e}{-p} \in \mathcal{O}_F^\times$. Then, since $\overline{F_0} = \overline{F}$, we may find $u \in \mathcal{O}_{F_0}^\times$ such that $\overline{u} = \overline{\frac{\pi^e}{-p}}$. In particular, $\frac{\pi^e}{-pu} \in U_F^{(1)}$. Now, applying Hensel's Lemma to the polynomials $X^e - u'$ for any $u' \in U_F^{(1)}$ (note that $(e,p)=1$), we see that $U_F^{(1)} \leq F^{\times e}$. Hence, $\sqrt[e]{\frac{\pi^e}{-pu}} \in F$ and thus $\sqrt[e]{-pu} \in F$. In particular,

$$v_F\big(\sqrt[e]{-pu}\big) = \frac{1}{e}(v_F(p) + v_F(u)) = \frac{1}{e},$$

so we get $F = F_0(\sqrt[e]{-pu})$.

We now shift our focus to E. By the properties of finite fields, every element in $\overline{F_0}$ is an e-th power[1] in $\overline{E}$, so u is an e-th power in E by Hensel's Lemma. In particular, this implies that

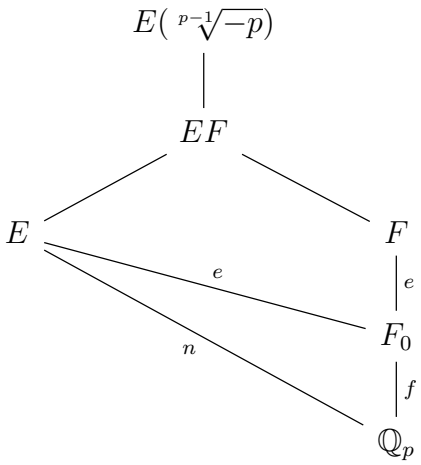
$$EF = E(\sqrt[e]{-pu}) = E(\sqrt[e]{-p}).$$

$EF/\mathbb{Q}_p$ is abelian as the compositum of two abelian extensions, which means that the intermediate extension $\mathbb{Q}_p(\sqrt[e]{-p})$ must be Galois. For this to be the case, we need $\zeta_e \in \mathbb{Q}_p$. However, by Corollary 2.1.2, this implies that $e \mid (p-1)$, and hence, $E(\sqrt[e]{-p}) \subseteq E(\sqrt[p-1]{-p})$. The following diagram gives an overview of the different extensions discussed so far:

[1]Indeed, let $E/\mathbb{F}_q$ be an extension of finite fields of degree e. Then $\mathbb{F}_q^\times \cong C_{q-1}$, $E^\times \cong C_{q^e-1}$, and taking e-th powers in $E^\times$ induces a subgroup isomorphic to $C_{(q^e-1)/(q^e-1,e)}$. We need to show that the latter group contains C_{q-1}, which is equivalent to

$$(q-1)\Big|\frac{(q^e-1)}{(q^e-1,e)} \iff (q^e-1,e)\Big|\frac{q^e-1}{q-1} = \sum_{i=0}^{e-1} q^i.$$

If we let $d = (q-1,e)$, one sees that it suffices to show that d divides the right-hand side, which is clearly the case since $q^i \equiv 1 \pmod{d}$ for all $0 \leq i \leq e-1$.



We claim $\mathbb{Q}_p(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_p)$ from which the result will follow since then

$$F \subseteq EF = E(\sqrt[e]{-p}) \subseteq E(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_{p^n-1})(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_{p^n-1}, \zeta_p).$$

To show that $\mathbb{Q}_p(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_p)$, we first observe that if w denotes the unique extension of v_p to $\mathbb{Q}_p(\sqrt[p-1]{-p})$, then $w\big(\sqrt[p-1]{-p}\big) = \frac{1}{p-1}$. It follows that

$$[\mathbb{Q}_p(\sqrt[p-1]{-p}) : \mathbb{Q}_p] = p - 1 = [\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p],$$

where the second equality follows from Lemma 2.1.1. Consequently, it suffices to show that $\mathbb{Q}_p(\sqrt[p-1]{-p}) \subseteq \mathbb{Q}_p(\zeta_p)$, or $\sqrt[p-1]{-p} \in \mathbb{Q}_p(\zeta_p)$. We note that the polynomial

$$X^{p-1} - \frac{-p}{(\zeta_p - 1)^{p-1}}$$

reduces to $X^{p-1} - 1$ in the residue field $\mathbb{F}_p$ of $\mathbb{Q}_p(\zeta_p)$ by Lemma 2.1.8. Therefore,

$$\sqrt[p-1]{\frac{-p}{(\zeta_p - 1)^{p-1}}} \in \mathbb{Q}_p(\zeta_p)$$

by Hensel's Lemma, which implies $\sqrt[p-1]{-p} \in \mathbb{Q}_p(\zeta_p)$ as required. □

2.2.2 The wild case

The wild case is more involved. Our goal is to show that the (infinite) maximal abelian pro-p extension of $\mathbb{Q}_p$ is a cyclotomic extension; the precise calculation will then allow us to read off a relevant cyclotomic extension containing the given finite abelian extension of $\mathbb{Q}_p$. In a first step, we determine an "upper bound" for the Galois group of this maximal abelian pro-p extension of $\mathbb{Q}_p$. As a base case, we compute the compositum of all C_p-extensions of $\mathbb{Q}_p(\zeta_p)$ that are abelian over

$\mathbb{Q}_p$[2], and then extend the argument to the infinite case. We proceed to show that the calculated Galois group actually appears as the Galois group of a cyclotomic extension. The concrete calculations will then allow us to explicitly describe for each finite abelian extension a cyclotomic extension containing it.

For ease of notation, we set $K := \mathbb{Q}_p(\zeta_p)$ and denote by v the extension of v_p to K. Observe that K is just the trivial extension for $p = 2$. For $p > 2$, on the other hand, $K/\mathbb{Q}_p$ is totally ramified of degree $p-1$ with uniformiser $\pi := \zeta_p - 1$ and $\mathrm{Gal}(K/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ by Lemma 2.1.1. The latter group is cyclic as the multiplicative group of the field $\mathbb{F}_p$. We let k be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, so $\mathrm{Gal}(K/\mathbb{Q}_p) = \langle\sigma\rangle$, where $\sigma(\zeta_p) = \zeta_p^k$. Crucially, note that k is a primitive root modulo p.

Following the structure described above, the first step is the base case, i.e., classifying (the compositum of) the C_p-extensions of K that are abelian over $\mathbb{Q}_p$. The crucial ingredient is Kummer theory, which can be summarised as the following fundamental result.

Theorem 2.2.3 (Kummer theory)**.** *Let F be a field with $\mathrm{char}\, F \neq p$ and $\zeta_p \in F$. Then there exists a bijection*

$$\begin{aligned}\{\textit{one-dim. subspaces } \langle c\rangle F^{\times p} \leq F^\times/F^{\times p}\} &\longleftrightarrow \{L/F \textit{ Galois extensions of deg. } p\}\\ \langle c\rangle F^{\times p} &\longmapsto F(\sqrt[p]{c})\\ (F^\times \cap L^{\times p})/F^{\times p} &\longmapsfrom L.\end{aligned}$$

Kummer theory thus tells us that the C_p-extensions of K are in a one-to-one correspondence with the 1-dimensional $\mathbb{F}_p$-subspaces of $K^\times/K^{\times p}$. When $p > 2$, however, not all such extensions are necessarily abelian over $\mathbb{Q}_p$. Determining which of these C_p-extensions remain abelian over $\mathbb{Q}_p$ requires an analysis of the action of σ on elements of the higher unit groups of K, as summarised in the next lemma.

Lemma 2.2.4. *Let $a \in \mathcal{O}_K$ be such that*

$$a \equiv 1 + a_j\pi^j \pmod{\pi^{j+1}}$$

with $a_j \in \mathcal{O}_K^\times$ (so $a \in U_K^{(j)}$ but $a \notin U_K^{(j+1)}$). Then

$$\sigma(a) \equiv 1 + k^j a_j \pi^j \pmod{\pi^{j+1}}.$$

[2]We work over $\mathbb{Q}_p(\zeta_p)$ to apply Kummer theory; this merely potentially enlarges the cyclotomic extensions.

Proof. First observe that

$$\frac{\sigma(\pi)}{\pi} = \frac{\sigma(\zeta_p - 1)}{\zeta_p - 1} = \frac{\zeta_p^k - 1}{\zeta_p - 1} = \sum_{i=0}^{k-1} \zeta_p^i = \sum_{i=0}^{k-1} (\pi + 1)^i \equiv k \pmod{\pi},$$

which implies

$$\frac{\sigma(\pi^j)}{\pi^j} = \left(\frac{\sigma(\pi)}{\pi}\right)^j \equiv k^j \pmod{\pi},$$

so

$$\sigma\left(\pi^j\right) \equiv \pi^j k^j \pmod{\pi^{j+1}}. \tag{2.2.1}$$

Similarly,

$$\sigma(\pi^{j+1}) \equiv \pi^{j+1} k^{j+1} \pmod{\pi^{j+2}},$$

which implies

$$\sigma(\pi^{j+1}) \equiv 0 \pmod{\pi^{j+1}}. \tag{2.2.2}$$

The claim then follows by combining equations (2.2.1) and (2.2.2). □

We can now prove the following characterisation of the C_p-extensions of K which are abelian over $\mathbb{Q}_p$.

Lemma 2.2.5. *The compositum F of all C_p-extensions of K which are abelian over $\mathbb{Q}_p$ is*

(i) $\mathbb{Q}_2(\sqrt{-1}, \sqrt{2}, \sqrt{5})$ *with* $\mathrm{Gal}\left(\mathbb{Q}_2(\sqrt{-1}, \sqrt{2}, \sqrt{5})/\mathbb{Q}_2\right) \cong C_2 \times C_2 \times C_2$ *for* $p = 2$*;*

(ii) $\mathbb{Q}_p(\zeta_{p^2}, \zeta_{p^p-1})$ *with* $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^2}, \zeta_{p^p-1})/K) \cong C_p \times C_p$ *for* $p > 2$.

Proof. (i). By Kummer theory (Theorem 2.2.3), it is enough to show that $\{-1, 2, 5\}$ represents a basis of $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ as an $\mathbb{F}_2$-vector space. As $\pi = 2$ is a uniformiser for $\mathbb{Q}_2$, Lemma 2.1.12 implies that it suffices to show that $\{-1, 5\}$ generates all elements of the shape

$$y = 1 + 2a_1 + 4a_2$$

for $a_1, a_2 \in \{0, 1\}$ modulo $\mathbb{Q}_2^{\times 2}$. So let us consider the four different cases for (a_1, a_2).

- $(a_1, a_2) = (0, 0)$. Then $y = 1 = (-1)^0 \cdot 5^0$.
- $(a_1, a_2) = (0, 1)$. Then $y = 5 = (-1)^0 \cdot 5^1$.
- $(a_1, a_2) = (1, 0)$. Then $y = 3 \equiv -5 = (-1)^1 \cdot 5^1 \pmod{\mathbb{Q}_2^{\times 2}}$.
- $(a_1, a_2) = (1, 1)$. Then $y = 7 \equiv -1 = (-1)^1 \cdot 5^0 \pmod{\mathbb{Q}_2^{\times 2}}$.

In the last two cases, we used Lemma 2.1.12 to reduce modulo $\pi^3 = 8$.

(ii) We first observe that $\mathbb{Q}_p(\zeta_{p^2})$ and $\mathbb{Q}_p(\zeta_{p^p-1})$ are C_p-extensions of K that are abelian over $\mathbb{Q}_p$ by Lemma 2.1.1, which implies that F contains $\mathbb{Q}_p(\zeta_{p^2}, \zeta_{p^p-1})$. Lemma 2.1.1 further tells us that $K(\zeta_{p^2})/K$ is totally ramified while $K(\zeta_{p^p-1})/K$ is unramified. This means that both subextensions are linearly disjoint over K, which implies $\mathrm{Gal}(K(\zeta_{p^2}, \zeta_{p^p-1})/K) \cong C_p \times C_p$.

It remains to see that any C_p-extensions L/K with $L/\mathbb{Q}_p$ abelian is contained in $\mathbb{Q}_p(\zeta_{p^2}, \zeta_{p^p-1})$. By Kummer theory, $L = K\left(\sqrt[p]{u}\right)$ for some $u \in K^\times$, where we may represent u as

$$u = p^{a_0}\left(1 + a_1\pi + \cdots + a_p\pi^p\right)$$

with $a_i \in \{0, \ldots, p-1\}$ by Lemma 2.1.12.

Claim. $a_0 = 0$.

Proof of Claim. Let us assume $a_0 \neq 0$. On the one hand,

$$\sigma(u) = p^{a_0}\sigma\left(1 + a_1\pi + \cdots + a_p\pi^p\right).$$

On the other hand, as $K\left(\sqrt[p]{u}\right) = K\left(\sqrt[p]{\sigma(u)}\right)$, we have $\sigma(u) \in \langle u\rangle K^{\times p}$ by Kummer theory, say $\sigma(u) \in u^r K^{\times p}$ with $r \in \{1, ..., p-1\}$. Hence,

$$\sigma(u) \equiv u^r = p^{ra_0}\left(1 + a_1\pi + \cdots + a_p\pi^p\right)^r \pmod{K^{\times p}}.$$

Comparing the last two equations and using Lemma 2.1.12, we see $ra_0 \equiv a_0 \pmod{p}$, which implies $r = 1$ since $a_0 \neq 0$. In particular, Lemma 2.1.12 then further implies

$$\sigma(1 + a_1\pi + \cdots + a_p\pi^p) \equiv 1 + a_1\pi + \cdots + a_p\pi^p \pmod{\pi^{p+1}}.$$

Now let $j \in \{1, \ldots, p\}$ be minimal such that $a_j \neq 0$. Combining the previous equation with Lemma 2.2.4 then implies that

$$a_j k^j \pi^j \equiv a_j \pi^j \pmod{\pi^{j+1}},$$

which is equivalent to $\overline{a_j} = \overline{a_j k^j}$. However, as k is a primitive root modulo p, this is impossible for $j < p-1$, so we may write

$$u = p^{a_0}(1 + a_{p-1}\pi^{p-1} + a_p\pi^p).$$

Next, we observe that we can factorise

$$u = p^{a_0}(1 + a_{p-1}\pi^{p-1} + a_p\pi^p) \equiv p^{a_0}(1 + lp)(1 + a'_p\pi^p) \pmod{K^{\times p}}$$

for suitable $l, a'_p \in \{0, \dots, p-1\}$. Indeed, using Lemma 2.1.8 to write $p = -\pi^{p-1} + x\pi^p$ for some $x \in \mathcal{O}_K$, we get

$$(1+lp)(1+a'_p\pi^p) \equiv 1 - l\pi^{p-1} + (lx + a'_p)\pi^p \pmod{\pi^{p+1}},$$

so choosing $l, a'_p \in \{0, \dots, p-1\}$ such that $\overline{l} = \overline{-a_{p-1}}$ and $\overline{a'_p} = \overline{a_p - lx}$, the claim follows from Lemma 2.1.12.

Let us assume we could show that $K\big(\sqrt[p]{1+a'_p\pi^p}\big) \subseteq K(\zeta_{p^p-1})$. Then the last equation shows that the extension $K\big(\zeta_{p^p-1}, \sqrt[p]{p^{a_0}(1+lp)}\big)/\mathbb{Q}_p$ is the compositum of the two abelian extensions $\mathbb{Q}_p(\zeta_{p^p-1})/\mathbb{Q}_p$ and $L/\mathbb{Q}_p$, and is therefore itself abelian. In particular, this means that the intermediate extension $\mathbb{Q}_p\big(\sqrt[p]{p^{a_0}(1+lp)}\big)/\mathbb{Q}_p$ is Galois. However, as $\mathbb{Q}_p$ does not contain the p-th roots of unity by Corollary 2.1.2, this is impossible when $a_0 \neq 0$, contradicting our assumption.

The last paragraph shows that in order to complete the proof of $a_0 = 0$, it suffices to show that $K\big(\sqrt[p]{1+a'_p\pi^p}\big) \subseteq K(\zeta_{p^p-1})$. This is clearly the case for $a'_p = 0$, so let us assume $a'_p \neq 0$ and denote $u' = 1 + a'_p\pi^p \in U_K^{(p)}$. Then $u' \notin K^{\times p}$ by Lemma 2.1.12, so $K\big(\sqrt[p]{u'}\big)/K$ is a C_p-extension by Kummer theory. In particular, u' is a p-th power in $K\big(\sqrt[p]{u'}\big)$, so Lemma 2.1.10 tells us that we may find $\overline{x} \in \overline{K\big(\sqrt[p]{u'}\big)}$ such that $\overline{x}^p - \overline{x} - \overline{a'_p} = 0$. However, this would be impossible for $\overline{a'_p} \neq 0$ if we had $\overline{K} = \mathbb{F}_p$, so we conclude that the extension $K(\sqrt[p]{u'})/K$ must give rise to a (degree-p) extension of residue fields. In particular, $K\big(\sqrt[p]{u'}\big)/K$ is unramified, so $K\big(\sqrt[p]{u'}\big) = K(\zeta_{p^p-1})$ by Lemma 2.1.1, as required. This concludes the proof that $a_0 = 0$. ◇

To complete the proof of Lemma 2.2.5, we calculate all possible values for the remaining a_i and show that in each case, $L \subseteq F$. Let $j \in \{1, \dots, p\}$ be minimal such that $a_j \neq 0$.

We first consider the case $j = p$, in which case $u = 1 + a_p\pi^p$, so the argument in the last paragraph shows that

$$L = \mathbb{Q}_p(\zeta_p, \sqrt[p]{u}) = \mathbb{Q}_p(\zeta_p, \zeta_{p^p-1}) \subseteq F$$

for any $a_p \in \{1, \dots, p-1\}$. In particular, this shows that $\mathbb{Q}_p(\zeta_p, \zeta_{p^p-1})/K$ corresponds to $\{(1+a_p\pi^p)K^{\times p} : a_p \in \{0, \dots, p-1\}\}$ under the Kummer correspondence.

If $j < p$, the previous paragraph and Lemma 2.1.12 show that $u \notin \langle u' \rangle K^{\times p}$ for any $u' = 1 + a'_p\pi^p$ with $a'_p \in \{1, \dots, p-1\}$. Using again that $\mathbb{Q}_p(\zeta_p, \sqrt[p]{u'}) = \mathbb{Q}_p(\zeta_p, \zeta_{p^p-1})$, we observe that $K\big(\sqrt[p]{uu'}\big)/\mathbb{Q}_p$ is a subextension of the compositum of the two

abelian extensions $L/\mathbb{Q}_p$ and $\mathbb{Q}_p(\zeta_{p^p-1})/\mathbb{Q}_p$, and hence is itself abelian. In particular, $K\left(\sqrt[p]{uu'}\right) = K\left(\sqrt[p]{\sigma(uu')}\right)$ and hence $\sigma(uu') \in \langle uu' \rangle K^{\times p}$ by Kummer theory, so there exists an $l \in \{0, \dots, p-1\}$ such that $\sigma(uu') \in (uu')^l K^{\times p}$.

Using the identity $\sigma(uu') = \sigma(u)\sigma(u')$, we now find a different expression for the domain of $\sigma(uu')$. As we have already observed in the argument for $a_0 = 0$, there is an $r \in \{0, \dots, p-1\}$ such that $\sigma(u) \in u^r K^{\times p}$. For the domain of $\sigma(u')$, we use Lemma 2.2.4 to observe that

$$\sigma(u') = \sigma(1 + a'_p \pi^p) \equiv 1 + k^p a'_p \pi^p \equiv 1 + k a'_p \pi^p \equiv (1 + a'_p \pi^p)^k = (u')^k \pmod{\pi^{p+1}},$$

so

$$\sigma(u') \equiv (u')^k \pmod{K^{\times p}}$$

by Lemma 2.1.12. Hence,

$$\sigma(uu') \in (uu')^l K^{\times p} \cap u^r \, (u')^k \, K^{\times p},$$

which forces $l = r = k$, so $\sigma(u) \in u^k K^{\times p}$. By Lemma 2.1.12 and expanding out, we see that

$$\sigma(u) \equiv u^k = (1 + a_j \pi^j + \cdots + a_p \pi^p)^k \equiv 1 + k a_j \pi^j \pmod{\pi^{j+1}}.$$

On the other hand,

$$\sigma(u) \equiv k^j a_j \pi^j \pmod{\pi^{j+1}}.$$

by Lemma 2.2.4. Since $j < p$ and k is a primitive root modulo p, this implies $j = 1$, so $a_1 \neq 0$.

We claim that the value of a_1 determines the value of the other a_i for $i < p$. Indeed, on the one hand, expanding out u^k once more, we see that

$$\sigma(u) \equiv (1 + a_1 \pi + \cdots + a_p \pi^p)^k \equiv 1 + k a_1 \pi + \sum_{i=2}^{p} (k a_i + f_i(a_1, \dots, a_{i-1})) \pi^i \pmod{\pi^{p+1}},$$

where $f_i \in \mathbb{Z}[X_1, \dots, X_{i-1}]$ for each i. On the other hand, writing $\sigma(\pi) = k\pi + b\pi^2$ for some $b \in \mathcal{O}_K^\times$, we get

$$\sigma(u) = 1 + \sum_{i=1}^{p} a_i (k\pi + b\pi^2)^i \equiv 1 + k a_1 \pi + \sum_{i=2}^{p} (a_i k^i + g_i(a_1, \dots, a_{i-1}; b)) \pi^i \pmod{\pi^{p+1}},$$

where $g_i \in \mathbb{Z}[X_1, \dots, X_{i-1}; Y]$. Recursively reducing modulo π^{i+1} for $i \in \{2, \dots, p-1\}$, this implies

$$\overline{a_i k^i + g_i(a_1, \dots, a_{i-1}; b)} = \overline{k a_i + f_i(a_1, \dots, a_{i-1})},$$

giving rise to unique values $a_i \in \{0, \dots, p-1\}$ for each i as k is a primitive root modulo p.

For a_p, there are p possible different values, which correspond to multiplying u with $u' = 1 + a'_p \pi^p$ for different values of a'_p. In particular, modulo these u', there are at most p distinct values of u, corresponding to the p different values of a_1. As $\sigma(\zeta_p^i) = (\zeta_p^i)^k$ and $\zeta_p = \pi + 1$, we see that these p values correspond precisely to the values ζ_p^i modulo $K^{\times p}$ for $i \in \{1, \dots p-1\}$. Thus, we get that

$$F \subseteq K\big(\sqrt[p]{\zeta_p u'}\big) \subseteq K\big(\sqrt[p]{\zeta_p}, \sqrt[p]{u'}\big) \subseteq \mathbb{Q}_p(\zeta_{p^2}, \zeta_{p^p-1})$$

as claimed. □

From this base case, we can now conclude the infinite case. While this is straightforward for $p > 2$, the case $p = 2$ requires the following slightly technical lemma:

Lemma 2.2.6. *$\mathbb{Q}_2(i)$ is not contained in a C_4-extension of $\mathbb{Q}_2$.*

This lemma at hand, we may then deduce:

Corollary 2.2.7. *Let $\tilde{F}$ be the unique maximal pro-p extension of K that is abelian over $\mathbb{Q}_p$. Then* $\mathrm{Gal}(\tilde{F}/K)$

(i) is a quotient of $C_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ for $p = 2$, and

(ii) is a quotient of $\mathbb{Z}_p \times \mathbb{Z}_p$ for $p > 2$.

Proof. (ii). By Lemma 2.2.5, the compositum of all C_p-extensions of K contained in $\tilde{F}$ is exactly $L := K(\zeta_{p^2}, \zeta_{p^p-1})$. As these C_p-extensions are the minimal subextensions of $\tilde{F}/K$, the Galois group $\mathrm{Gal}(\tilde{F}/L)$ is exactly the intersection of all maximal subgroups of $\mathrm{Gal}(\tilde{F}/K)$ by the infinite Galois correspondence (cf. [Sza09], Theorem 1.3.11). In other words, $\mathrm{Gal}(\tilde{F}/L)$ is the Frattini subgroup of $\mathrm{Gal}(\tilde{F}/K)$ and

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\tilde{F}/K)/\,\mathrm{Gal}(\tilde{F}/L)$$

is its Frattini quotient. As $\mathrm{Gal}(L/K) \cong C_p \times C_p$, we see that, as pro-$p$ groups,

$$\mathrm{rank}(\mathrm{Gal}(\tilde{F}/K)) = \mathrm{rank}(\mathrm{Gal}(L/K)) = \mathrm{rank}(C_p \times C_p) = 2,$$

so $\mathrm{Gal}(\tilde{F}/K)$ must be a quotient of the free abelian pro-p group of rank 2, which is $\mathbb{Z}_p \times \mathbb{Z}_p$.

(i). By the same argument as in (ii), we could now conclude that the Galois group of the maximal abelian pro-2 extension of $\mathbb{Q}_2$ is a quotient of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. However,

by Lemma 2.2.6, $\mathbb{Q}_2(i)$ is not contained in a C_4-extension of $\mathbb{Q}_2$, so $\mathrm{Gal}(\tilde{F}/K)$ must actually be a quotient of $C_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. □

To show Lemma 2.2.6, we must examine the quadratic extensions of $\mathbb{Q}_2(i)$. By Kummer theory, these extensions correspond exactly to the 1-dimensional $\mathbb{F}_2$-subspaces of $\mathbb{Q}_2(i)^\times/\mathbb{Q}_2(i)^{\times 2}$. The next lemma calculates a basis of $\mathbb{Q}_2(i)^\times/\mathbb{Q}_2(i)^{\times 2}$ as an $\mathbb{F}_2$-vector space explicitly.

Lemma 2.2.8. *$(1+i, 1+2i, 2, 5)$ is a basis of $\mathbb{Q}_2(i)^\times/\mathbb{Q}_2(i)^{\times 2}$ as an $\mathbb{F}_2$-vector space.*

Proof. Let us write $F = \mathbb{Q}_2(i)$ and denote $v = v_F$. We note that $F/\mathbb{Q}_2$ is ramified of degree 2 with uniformiser $\pi = i - 1$ since

$$v(\pi) = \frac{1}{2}v(\pi^2) = \frac{1}{2}v(-2i) = \frac{v(2)}{2} + \frac{v(i^2)}{4} = \frac{1}{2}.$$

As a first step, we show that $F^\times/F^{\times 2}$ has $\mathbb{F}_2$-dimension 4, for which we generalise the argument in Lemma 2.1.12 (as already mentioned in Remark 2.1.13, we present a more general dimension formula in Lemma 3.2.4). We recall that

$$F^\times/F^{\times 2} \cong \pi^{\mathbb{Z}}/\pi^{2\mathbb{Z}} \times U_F^{(1)}/\left(U_F^{(1)}\right)^2$$

by Fact 2.1.4, so it suffices to show that $U_F^{(1)}/\left(U_F^{(1)}\right)^2$ has $\mathbb{F}_2$-dimension 3, or equivalently, cardinality 8. Writing

$$U_F^{(1)}/\left(U_F^{(1)}\right)^2 \cong \frac{U_F^{(1)}/U_F^{(5)}}{\left(U_F^{(1)}\right)^2/U_F^{(5)}}$$

by Lemma 2.1.9 and noting that

$$\left|U_F^{(1)}/U_F^{(5)}\right| = 16$$

by Corollary 2.1.7, we observe that it suffices to show

$$\left|\left(U_F^{(1)}\right)^2/U_F^{(5)}\right| = 2.$$

Letting $\Phi : U_F^{(1)}/U_F^{(5)} \to \left(U_F^{(1)}\right)^2/U_F^{(5)}$ denote the map $x \mapsto x^2$, this is equivalent to showing $|\ker \Phi| = 16/2 = 8$.

We note immediately that $\ker \Phi < 16$: For example $\Phi\left((1+\pi)U_F^{(5)}\right)$ is non-trivial as otherwise

$$(1+\pi)^2 \equiv 1 \pmod{\pi^5}$$

by Remark 2.1.6, meaning $v((1+\pi^2)^2-1) \geq 5v(\pi)$, which contradicts

$$v\left((1+\pi)^2-1\right) = v(\pi^2+2\pi) = \min\{v(\pi^2), v(2\pi)\} = v(\pi^2) = 2v(\pi).$$

It remains to show $|\ker\Phi| \geq 8$. To do so, we use Corollary 2.1.7 to represent any of $U_F^{(1)}/U_F^{(5)}$ as

$$(1+a_1\pi+a_2\pi^2+a_3\pi^3+a_4\pi^4)U_F^{(5)},$$

with $a_i \in \{0,1\}$ for each i; we will show that all elements with $a_1 = 0$ are contained in $\ker\Phi$. Indeed, writing $b = a_3\pi^3 + a_4\pi^4 \in (\pi^3)$ to slightly simplify the notation and expanding out, we see (using $a_2^2 = a_2$)

$$(1+a_2\pi^2+b)^2 = 1+a_2^2\pi^4+b^2+2a_2\pi^2+2b+2a_2\pi^2 b \equiv 1+a_2\pi^4+2a_2\pi^2 \pmod{\pi^5},$$

where

$$a_2\pi^4+2a_2\pi^2 = a_2\pi^2(\pi^2+2) = a_2\pi^2(-2\pi) \equiv 0 \pmod{\pi^5},$$

so the claim follows from Remark 2.1.6.

To show that $\{1+i, 1+2i, 2, 5\}$ forms a basis of $F^\times/F^{\times 2}$, it hence suffices to show that the four elements are linearly independent over $F^{\times 2}$. So assume

$$x = (1+i)^\alpha \cdot (1+2i)^\beta \cdot 2^\gamma \cdot 5^\delta = y^2$$

for some $y \in F^\times$ and $\alpha, \beta, \gamma, \delta \in \{0,1\}$. Then, denoting by N the field-theoretic norm map of the extension $F/\mathbb{Q}_2$,

$$2^\alpha \cdot 5^\beta \cdot 4^\gamma \cdot 25^\delta = N(x) = N(y^2) = N(y)^2 \in \mathbb{Q}_2^{\times 2},$$

so $\alpha = \beta = 0$ by the proof of Lemma 2.2.5(i). It remains to exclude the three cases $(\gamma, \delta) = (1,0), (0,1), (1,1)$.

- $(\gamma, \delta) = (1,0)$ would mean that $2 \in F^{\times 2}$, so $F = \mathbb{Q}_2(i, \sqrt{2})$. But then also $\zeta_8 = \frac{1+i}{\sqrt{2}} \in F$, contradicting the fact that $\mathbb{Q}_2(\zeta_8)$ is totally ramified of degree $4 \neq 2$ over $\mathbb{Q}_2$ by Lemma 2.1.1.
- $(\gamma, \delta) = (0,1)$ would mean that $F = \mathbb{Q}_2(i, \sqrt{5})$. As $5 \equiv -3 \pmod{2^3}$, Lemma 2.1.12 further implies that $F = \mathbb{Q}_2(i, \sqrt{-3})$. In particular, $\zeta_3 = \frac{-1+\sqrt{-3}}{2} \in F$, contradicting the fact that $\mathbb{Q}_2(\zeta_3)$ is the unique unramified extension of $\mathbb{Q}_2$ of degree 2 by Lemma 2.1.1.
- $(\gamma, \delta) = (1,1)$ would mean that $\mathbb{Q}_2(i) = \mathbb{Q}_2(i, \sqrt{2 \cdot 5})$. However, this would imply that $\mathbb{Q}_2(i, \sqrt{5}) = \mathbb{Q}_2(i, \sqrt{2})$, which contradicts what we have shown in the previous two items. □

We can now deduce Lemma 2.2.6.

Proof (Lemma 2.2.6). We continue to write $F = \mathbb{Q}_2(i)$ and let $L/\mathbb{Q}_2$ be a Galois extension of degree 4 containing F. Then $[L : F] = 2$, so $L = F(\sqrt{x})$ by Kummer theory. By the previous lemma, we may assume $x = (1+i)^\alpha \cdot (1+2i)^\beta \cdot 2^\gamma \cdot 5^\delta$ for $\alpha, \beta, \gamma, \delta \in \{0, 1\}$. Let us assume we could show $\alpha = \beta = 0$. Then x would be one of 2, 5, 10, and either way $\mathbb{Q}_2(\sqrt{x})$ is an intermediate extension of degree 2, meaning $L/\mathbb{Q}_2$ has two distinct proper non-trivial intermediate fields, so it cannot be a C_4-extension.

It hence remains to prove $\alpha = \beta = 0$. If σ denotes the generator of $\mathrm{Gal}(F/\mathbb{Q}_2)$ (i.e., σ is complex conjugation), then, $F(\sqrt{x}) = F\big(\sqrt{\sigma(x)}\big)$, so $\sigma(x) \in \langle x \rangle F^{\times 2}$ by Kummer theory. In particular, $\sigma(x) \equiv x \pmod{F^{\times 2}}$.

We now consider the different cases for α and β, starting with $\alpha = \beta = 1$. Then

$$x \equiv (1+i) \cdot (1+2i) \cdot 2^\gamma \cdot 5^\delta \pmod{F^{\times 2}},$$

and

$$\begin{aligned} \sigma(x) &\equiv (1-i) \cdot (1-2i) \cdot 2^\gamma \cdot 5^\delta \\ &\equiv (1-i) \cdot (1-2i) \cdot 2^\gamma \cdot 5^\delta (1+i)^2 (1+2i)^2 \\ &\equiv (1+i) \cdot (1+2i) \cdot 2^{\gamma+1} \cdot 5^{\delta+1} \pmod{F^{\times 2}}. \end{aligned}$$

Together the last two equations imply $0 \equiv 2 \cdot 5 \pmod{F^{\times 2}}$, contradicting the linear independence proved in Lemma 2.2.8. Similarly, we get contradictions $2, 5 \equiv 0 \pmod{F^{\times 2}}$ for $(\alpha, \beta) = (1, 0), (0, 1)$, respectively. □

For the next step of our argument, we want to show that $\tilde{F}$ from Corollary 2.2.7 is cyclotomic. To do so, we prove that the groups calculated in Corollary 2.2.7 actually appear as the Galois groups of cyclotomic extensions of K.

Lemma 2.2.9. *Let $F = \mathbb{Q}_p(\zeta_{p^{p^\infty}-1}, \zeta_{p^\infty})$. Then*

(i) $\mathrm{Gal}(F/K) = \mathrm{Gal}(F/\mathbb{Q}_2) \cong C_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ *for $p = 2$, and*

(ii) $\mathrm{Gal}(F/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p$ *for $p > 2$.*

Proof. (ii). From infinite Galois theory, we have $\mathrm{Gal}(F/K) \cong \varprojlim \mathrm{Gal}(E/K)$, where E runs over the directed partially ordered set I of finite Galois subextensions of F/K (cf. [Sza09], Proposition 1.3.5). By definition of F, these finite subextensions are of the form $E = \mathbb{Q}_p(\zeta_{p^{p^n}-1}, \zeta_{p^m})$ for some non-negative integers m, n.

Now $K(\zeta_{p^{p^n}-1})/K$ is unramified of degree p^n with $\mathrm{Gal}(K(\zeta_{p^{p^n}-1})/K) \cong C_{p^n}$ by Lemma 2.1.1. $K(\zeta_{p^m})/K$, on the other hand, is totally ramified by Lemma 2.1.1, and

$$\mathrm{Gal}(K(\zeta_{p^m})/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times \cong C_{p^{m-1}(p-1)} \cong C_{p^{m-1}} \times C_{p-1}.$$

Hence, as $(p^{m-1}, p-1) = 1$,

$$\mathrm{Gal}(K(\zeta_{p^m})/K) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)/\mathrm{Gal}(K/\mathbb{Q}_p) \cong C_{p^{m-1}}.$$

Finally, $K(\zeta_{p^{p^n}-1})$ and $K(\zeta_{p^m})$ are linearly disjoint as one extension is unramified and the other one totally ramified. Thus, $\mathrm{Gal}(E/K) = C_{p^n} \times C_{p^{m-1}}$, and the claim follows since $\mathbb{Z}_p = \varprojlim_k C_{p^k}$.

(i). As $\mathbb{Q}_2(\zeta_{2^\infty})/\mathbb{Q}_2$ is totally ramified and $\mathbb{Q}_2(\zeta_{2^{2^\infty}-1})/\mathbb{Q}_2$ is unramified, we see that both extensions are linearly disjoint over $\mathbb{Q}_2$, so

$$\mathrm{Gal}(F/\mathbb{Q}_2) \cong \mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^\infty})/\mathbb{Q}_2) \times \mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{2^\infty}-1})/\mathbb{Q}_2).$$

By Lemma 2.1.1,

$$\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{2^\infty}-1})/\mathbb{Q}_2) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{2^n}-1})/\mathbb{Q}_2) \cong \varprojlim_n C_{2^n} = \mathbb{Z}_2.$$

It remains to show that $\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^\infty})/\mathbb{Q}_2) \cong C_2 \times \mathbb{Z}_2$. Again, we have

$$\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^\infty})/\mathbb{Q}_2) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^n})/\mathbb{Q}_2) \cong \varprojlim_n C_{2^n}^\times \cong \varprojlim_n (C_2 \times C_{2^{n-2}})$$

by Lemma 2.1.1, so the claim follows if we can show that the projective limit splits as the product of the inverse limits of the two factors C_2 and $C_{2^{n-2}}$. To do so, we analyse the projection maps in the projective system.

Observe that the elements of $\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^n})/\mathbb{Q}_2)$ are precisely the automorphisms $\sigma_{n,k}$, defined by

$$\sigma_{n,k}(\zeta_{2^n}) \coloneqq \zeta_{2^n}^k,$$

where $k \in (\mathbb{Z}/2^n\mathbb{Z})^\times$. Then the natural projection

$$\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^n})/\mathbb{Q}_2) \longrightarrow \mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^{n-1}})/\mathbb{Q}_2)$$

sends $\sigma_{n,k}$ to $\sigma_{n-1,k}$ since

$$\sigma_{n-1,k}(\zeta_{2^{n-1}}) = \sigma_{n,k}(\zeta_{2^{n-1}}) = \sigma_{n,k}\big(\zeta_{2^n}^2\big) = \zeta_{2^n}^{2k} = \zeta_{2^{n-1}}^k,$$

which, under the isomorphism

$$\mathrm{Gal}(\mathbb{Q}_2(\zeta_{2^n})/\mathbb{Q}_2) \cong (\mathbb{Z}/2^n\mathbb{Z})^\times,$$

corresponds to the reduction map $k \mapsto k \pmod{2^{n-1}}$ Hence, if we use the standard decomposition $(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \{\pm 1\} \times \langle 5\rangle \cong C_2 \times C_{2^{n-2}}$, the projection maps in the projective system carry the C_2–factor to the C_2–factor and the $C_{2^{n-2}}$–factor to the $C_{2^{n-3}}$–factor compatibly, yielding the required decomposition. □

By Lemma 2.1.1, F from the previous lemma is a pro-p extension of K that is abelian over $\mathbb{Q}_p$. In particular, $F \subseteq \tilde{F}$. Hence, together with Corollary 2.2.7 and the previous lemma, this gives rise to maps

$$C_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \twoheadrightarrow \mathrm{Gal}(\tilde{F}/K) \overset{|_F}{\twoheadrightarrow} \mathrm{Gal}(F/K) \cong C_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

for $p = 2$, and

$$\mathbb{Z}_p \times \mathbb{Z}_p \twoheadrightarrow \mathrm{Gal}(\tilde{F}/K) \overset{|_F}{\twoheadrightarrow} \mathrm{Gal}(F/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

for $p > 2$. In either case, all epimorphisms are necessarily isomorphisms. Therefore, $F = \tilde{F}$ by the infinite Galois correspondence.

We can now readily conclude the wild case and thus, our proof of Theorem 2.2.1. Indeed, given an extension $L/\mathbb{Q}_p$ of degree p^l, we can see that the maximal abelian p-extension of K of exponent p^l that is also abelian over $\mathbb{Q}_p$ is contained in

$$\mathbb{Q}_2(\zeta_4, \zeta_{2^{l+2}}, \zeta_{2^{2^l}-1}) = \mathbb{Q}_2(\zeta_{2^{l+2}}, \zeta_{2^{2^l}-1}) \text{ for } p = 2, \text{ and}$$
$$\mathbb{Q}_p(\zeta_p)(\zeta_{p^{l+1}}, \zeta_{p^{p^l}-1}) = \mathbb{Q}_p(\zeta_{p^{l+1}}, \zeta_{p^{p^l}-1}) \text{ for } p > 2.$$

Either way, $L \subseteq \mathbb{Q}_p(\zeta_{p^{l+2}}, \zeta_{p^{p^l}-1})$.

Remark 2.2.10. As noted in the introduction, Washington's book [Was97, Chapter 14] contains a proof of the local Kronecker–Weber theorem that is structurally close to the one presented in this chapter. The present proof was developed independently; Washington's argument came to our attention only during the review process of the paper on which this chapter is based. We therefore take this opportunity to compare the two approaches and to clarify both their common strategy and their conceptual differences.

At a high level, both proofs proceed by decomposing a finite abelian extension $L/\mathbb{Q}_p$ into its tamely ramified and wildly ramified parts. In the tame case, both arguments essentially follow the strategy outlined in the first paragraph of the proof of

Lemma 2.2.2. The treatment above is slightly more streamlined than Washington's, as it develops the necessary constructions within a unified framework. Washington instead first uses Krasner's lemma to show that L can be written as $L = L_0(\sqrt[q^r]{a})$ for some a [Was97, Lemma 14.5], and only later proves that one may take $a = -up$ [Was97, p. 324]. Moreover, his argument does not make explicit the cyclotomic extensions required at each step; for example, in passing from $\sqrt[e]{-pu}$ to $\sqrt[e]{-p}$, it is not specified which roots of unity must be adjoined. As a result, Washington's proof does not yield an explicit description of the relevant cyclotomic extensions, unlike ours.

Moreover, another methodological difference that already becomes apparent in the tame case is that Washington frequently employs analytic arguments. For instance, Washington shows that $\mathbb{Q}_p(\sqrt[p-1]{-p}) = \mathbb{Q}_p(\zeta_p)$ using analytic arguments that rely on the completeness of $\mathbb{Q}_p$ (cf. [Was97, Lemma 14.6]), whereas our proof relies exclusively on algebraic and valuation-theoretic methods.

Even more substantial differences arise in the treatment of the wildly ramified case. Washington distinguishes between the cases $p \neq 2$ and $p = 2$, analysing them separately in [Was97, Case II, p. 325] and [Was97, Case III, p. 328]. When $p \neq 2$, his argument shows that any abelian extension not contained in a field of the form $\mathbb{Q}_p(\zeta_{p^{m+1}}, \zeta_n)$ gives rise to an extension $N/\mathbb{Q}_p$ with $\mathrm{Gal}(N/\mathbb{Q}_p) \cong C_p^3$. To exclude this possibility, Washington employs a strategy closely related to the one used in Lemma 2.2.5: after adjoining ζ_p, Kummer theory over $K = \mathbb{Q}_p(\zeta_p)$ is applied, and the action of $\mathrm{Gal}(K/\mathbb{Q}_p)$ on $K^\times/K^{\times p}$ is analysed in order to determine all possible generators explicitly. A key technical input in this argument is the statement proved here in Lemma 2.1.11, which Washington establishes using the logarithm on local fields.

The case $p = 2$ is treated in a similar spirit. Here, Washington identifies extensions $N/\mathbb{Q}_2$ with $\mathrm{Gal}(N/\mathbb{Q}_2) \cong C_2^4$ and $\mathrm{Gal}(N/\mathbb{Q}_2) \cong C_4^3$ as the two problematic cases that must be excluded. The former is ruled out using his analogue of Lemma 2.1.11, while the latter is excluded by observing that the equation $X^2 + Y^2 = -1$ has no solution in $\mathbb{Q}_2$.

In contrast, the approach taken in this chapter treats the wild case for all primes p within a single algebraic framework. By computing explicit representatives for the relevant quotients of unit groups and analysing their behaviour under the Galois action, we are able to determine explicitly the compositum of all C_p-extensions of K that are abelian over $\mathbb{Q}_p$ (Lemma 2.2.5), a point that is only implicit in Washington's

treatment for $p \neq 2$ and is not carried out for $p = 2$. The additional subtleties arising when $p = 2$ therefore emerge naturally from these computations, rather than necessitating a separate structural argument. An additional advantage of this method is that it allows us to determine the relevant absolute Galois group explicitly, which aligns with the overall theme of this thesis.

In summary, the proof presented here relies exclusively on algebraic and valuation-theoretic arguments, together with explicit calculations in unit groups, and avoids analytic tools such as logarithmic or exponential series on local fields. This emphasis on explicit algebraic structures and valuation-theoretic methods not only leads to a streamlined and uniform proof of the local Kronecker–Weber theorem, but also prepares the ground for later chapters. In particular, several of the unit group computations introduced in Section 2.1 are revisited and generalised in Chapter 3, illustrating how the techniques developed here can be extended to the more general setting of p-adically closed fields.

Chapter 3

Galois characterisation of p-adically closed fields

The goal of this chapter is to give a new and self-contained proof of Theorem 1.1.7, which we restate here again for the convenience of the reader.

Theorem 3.0.1. *For any field K,*

$$G_K \cong G_{\mathbb{Q}_p} \quad \textit{if and only if} \quad K \textit{ is } p\textit{-adically closed.}$$

Before embarking on the proof of this theorem, let us give some examples of p-adically closed fields. Abstractly speaking, there are of course p-adically closed fields of any infinite cardinality by the Löwenheim-Skolem Theorem. However, there are also natural algebraic examples.

Example 3.0.2.

1. The field of algebraic p-adic numbers $k = \mathbb{Q}_p \cap \mathbb{Q}^{\mathrm{alg}}$ is p-adically closed.
2. The field of Puiseux series over $\mathbb{Q}_p$,

$$K = \bigcup_{n>0} \mathbb{Q}_p((t^{1/n})),$$

is p-adically closed. This is perhaps the simplest example of rank two.

Proof strategy The main ingredients in our proof are:

(I) A systematic use of coarsenings and the Standard Decomposition.

(II) The Galois characterisation of henselianity; in particular,

- the creation of valuations, and

- going-down statements for henselianity.

(III) Transfer of Galois groups between different characteristics.

(IV) Explicit constructions replacing abstract cohomological considerations.

(V) Pop's Lemma on mixed characteristic henselian valued fields with absolute Galois group of finite p-rank.

It follows readily from the smallness of $G_{\mathbb{Q}_p}$ that every p-adically closed field has absolute Galois group isomorphic to $G_{\mathbb{Q}_p}$. The main task, therefore, is to establish the converse: that any field K whose absolute Galois group is isomorphic to $G_{\mathbb{Q}_p}$ is p-adically closed. The proof proceeds as follows. We begin by constructing a henselian valuation v_K on K using the Galois characterisation of henselianity. Combining explicit criteria inspired by Galois cohomology with a careful analysis of the roots of unity in K, we then show that (K, v_K) has mixed characteristic $(0, p)$. This enables us to apply the Standard Decomposition, expressing v_K as a composition of three valuations, with the middle component $\overline{v_p}$ having rank one and mixed characteristic. Utilising Pop's Lemma together with transfer principles for Galois groups, we demonstrate that $\overline{v_p}$ has value group $\mathbb{Z}$ and residue field $\mathbb{F}_p$. Finally, we translate these structural properties back to the original valuation v_K and verify that it satisfies all four axioms of the Ax-Kochen/Ershov Theorem 1.1.5.

Structure of this chapter Section 3.1 is a survey of valuation theory, aimed at the reader familiar with rank 1 (i.e. real-valued) valuations—those that correspond to absolute values on fields—but not familiar with higher rank (i.e. Krull) valuations that take values in an ordered abelian group.

Section 3.2 connects valued fields to their absolute Galois groups. Section 3.2.1 deals with most of the computational aspects around $\mathbb{Q}_p$. In Section 3.2.2, we prove Pop's Lemma. In Section 3.2.3, we present both explicit and elementary criteria for distinguishing fields of characteristic 0 from those of positive characteristic p. Although motivated by ideas from Galois cohomology, the results are self-contained and rely only on Hilbert's Theorem 90. Section 3.2.4 contains the Transfer Lemma (Lemma 3.2.18), for which we outline two proofs: Koenigsmann's original proof and a new proof by Gitin based on the tilting construction. In Section 3.2.5, we prove the Galois characterisation of henselianity, providing a method to recover henselian valuations from absolute Galois groups.

Section 3.3 finally contains the proof of Theorem 3.0.1.

Joint Work. This chapter reproduces large parts of the paper [GKS], which itself builds on an initial sketch of an elementary proof of Theorem 3.0.1 presented by Koenigsmann in a lecture at the University of Oxford in Trinity Term 2022 [Koe22]. Section 3.1—which contains the preliminary Sections 3.1.1, 3.1.2, 3.1.3, and 3.1.5, as well as Section 3.1.4 that follows the presentation in Efrat's book [Efr06]—were written in collaboration with Leo Gitin. They correspond to Sections 2.1, 2.2, 2.3, 2.5, and 2.4 in [GKS], respectively. All remaining parts of this chapter, except where the paper is explicitly cited, are my work.

3.1 Methods in valuation theory

This section will provide us with our basic toolbox. It is not meant to replace textbook treatments such as Engler-Prestel [EP05] and Efrat [Efr06]. Rather, we aim for a transparent synopsis. Our main goals in this section are:

(a) Introduce the three equivalent ways of thinking about valuations on a field K, as indicated by the following bijections:

$$\begin{array}{ccc} \{v \text{ valuation on } K\}/\sim & \longleftrightarrow & \{\mathcal{O} \text{ valuation ring on } K\} \\ & \searrow \quad \swarrow & \\ & \{\varphi \text{ place on } K\}/\sim & \end{array}$$

Our treatment emphasises the places point-of-view (Section 3.1.1).

(b) Explain how valuations behave under algebraic extensions of fields and the associated ramification (Hilbert-Dedekind) theory (Section 3.1.2).

(c) Examine how valuations interact with one another when several valuations are present on a given field (Section 3.1.3):

- Explain coarsenings, and how this gives rise to the concept of decompositions (Section 3.1.3.1);
- define the Standard Decomposition (Section 3.1.3.2);
- introduce a natural choice of valuation in a general abstract setting, giving rise to the canonical henselian valuation (Section 3.1.3.3).

(d) Explain the creation of abstract valuations from rigid and p-rigid elements (Section 3.1.4).

3.1.1 Valuations, valuation rings, and places

3.1.1.1 Ordered abelian groups

Abstract valuations on fields take values in ordered abelian groups, generalising real-valued valuations.

Definition 3.1.1. A *convex* subgroup Δ of an ordered abelian group $(\Gamma, \leq)$ is a subgroup such that for any positive $\delta \in \Delta$ and $\gamma \in \Gamma$, $0 \leq |\gamma| \leq \delta$ implies $\gamma \in \Delta$. We write $\Gamma_{>\gamma}$ for the interval (γ, ∞) in Γ and

$$\mathrm{Conv}(X) \coloneqq \{\gamma \in \Gamma : |\gamma| \leq \delta \text{ for some } \delta \in \langle X \rangle\}$$

for the *convex hull* of a set $X \subseteq \Gamma$ (here, $\langle X \rangle$ denotes the group generated by X in Γ). We further write $\mathrm{Conv}(\gamma) \coloneqq \mathrm{Conv}(\{\gamma\})$ for $\gamma \in \Gamma$.

Any convex subgroup Δ naturally gives rise to an ordering on the quotient group Γ/Δ. Crucially, the set of convex subgroups of Γ is linearly ordered by inclusion. The *(Archimedean) rank* of Γ is the cardinality of the set of proper convex subgroups. The following is classical:

Fact 3.1.2 (Hölder)**.** *Any ordered abelian group that is Archimedean, i.e., of rank 1, embeds into the ordered group of reals.*

For ordered abelian groups, we have an intrinsic notion of infinitesimals:

Definition 3.1.3. Let $\varepsilon \in \Gamma$ and $\gamma \in \Gamma_{>0}$. We say ε is *infinitesimal with respect to* γ (in symbols: $\varepsilon \ll \gamma$), if $n|\varepsilon| < \gamma$ for all $n \in \mathbb{N}$.

To any $\gamma \in \Gamma_{>0}$, we associate two canonical convex subgroups: the minimal convex subgroup containing γ and the maximal convex subgroup not containing γ. These are, respectively,

$$\Gamma_\gamma^+ \coloneqq \mathrm{Conv}(\gamma)$$
$$\Gamma_\gamma^- \coloneqq \{\varepsilon \in \Gamma : |\varepsilon| \ll \gamma\}.$$

Fact 3.1.4. *For any $\gamma \in \Gamma_{>0}$, the ordered quotient group $\Gamma_\gamma^+/\Gamma_\gamma^-$ is of rank 1.*

3.1.1.2 Valuations and valuation rings

Basic examples of discrete valuations are the p-adic valuation on $\mathbb{Q}$ and the order of vanishing at X in a field of rational functions $k(X)$. Abstract (Krull) valuations generalise this notion.

Definition 3.1.5. A *valuation* on a field K with values in an ordered abelian group $(\Gamma, \leq)$ is a surjective map

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

that satisfies the three properties

(i) $v(x) = \infty$ if and only if $x = 0$;

(ii) $v(x \cdot y) = v(x) + v(y)$ (additivity);

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ (ultrametric triangle inequality);

where the relations $\gamma < \infty$ and $\gamma + \infty = \infty + \gamma = \infty + \infty = \infty$ are assumed for all $\gamma \in \Gamma$. The pair (K, v) is called a *valued field*.

Associated to any (K, v) are the following basic objects:

(a) Γ is called the *value group* of v and is alternatively denoted by vK or Γ_v.

(b) $\mathcal{O}_v \coloneqq \{x \in K : v(x) \geq 0\}$ is the *valuation ring* of v.

(c) $\mathcal{M}_v \coloneqq \{x \in K : v(x) > 0\}$ is the unique maximal ideal of $\mathcal{O}_v$.

(d) $\mathcal{O}_v/\mathcal{M}_v$ is the *residue field* of v and denoted by Kv. We sometimes write xv or $\overline{x}$ for the residue class $x\mathcal{M}_v$ of $x \in \mathcal{O}_v$.

(e) The *rank* of (K, v) is the Archimedean rank of its value group Γ.

(f) The pair $(\operatorname{char} K, \operatorname{char} Kv)$ is the *characteristic* of (K, v).

(g) The *valuation topology* is induced by basic open sets of balls

$$B_\gamma(x) \coloneqq \{y \in K : v(y - x) > \gamma\}, \quad \text{where } \gamma > 0,\ x \in K,$$

making K into a topological field. Whenever we refer to topological properties of a valued field, it is with respect to this topology.

Fact 3.1.6. *The invariants above form canonical short exact sequences*

$$\begin{aligned} 1 \longrightarrow \mathcal{O}_v^\times \longrightarrow K^\times \longrightarrow vK \longrightarrow 1 \\ 1 \longrightarrow 1 + \mathcal{M}_v \longrightarrow \mathcal{O}_v^\times \longrightarrow Kv^\times \longrightarrow 1. \end{aligned} \tag{3.1.1}$$

The valuation v can be recovered solely from the ring $\mathcal{O}_v$, and, moreover, axioms (i)–(iii) correspond to abstract properties of the ring $\mathcal{O}_v$.

Definition 3.1.7. An (abstract) *valuation ring* is an integral domain A such that for any non-zero element $a \in \operatorname{Frac}(A)$, $a \in A$ or $a^{-1} \in A$.

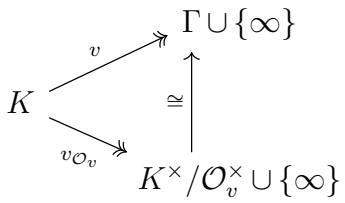
Let $K = \mathrm{Frac}(A)$. If A is an abstract valuation ring, then K can be endowed with a canonical valuation with valuation ring A. This is the quotient map

$$v_A : K^\times \longrightarrow\!\!\!\!\!\rightarrow K^\times/A^\times,$$

where the latter becomes an ordered abelian group by declaring

$$xA^\times \leq yA^\times :\Longleftrightarrow \tfrac{y}{x} \in A$$

and switching from multiplicative to additive notation (in particular, $1A^\times$ is identified with the neutral element 0). Clearly, $\mathcal{O}_{v_A} = A$. Conversely, given a valued field (K, v), the valuations v and $v_{\mathcal{O}_v}$ are *equivalent* in the sense of the following commutative diagram:



3.1.1.3 Places

We give a third and final description of the concept.

Definition 3.1.8. A *place* on K is given by a field k together with a surjective map

$$\varphi : K \longrightarrow\!\!\!\!\!\rightarrow k \cup \{\infty\}$$

that satisfies the three "ring homomorphism" properties

$$\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y), \\ \varphi(x \cdot y) &= \varphi(x) \cdot \varphi(y), \\ \varphi(1) &= 1, \end{aligned}$$

where addition and multiplication on k are extended to $k \cup \{\infty\}$ subject to the relations

$$a + \infty = \infty + a = \infty \quad \text{and} \quad a \cdot \infty = \infty \cdot a = \infty \cdot \infty = \infty$$

for any $a \in k$. We leave $\infty + \infty$, $0 \cdot \infty$, and $\infty \cdot 0$ undefined and the conditions on φ vacuous in these three cases.

The relationship between valuations and places can be described as follows. Given a valuation v on K with residue field $Kv = \mathcal{O}_v/\mathcal{M}_v$, taking residues induces a place φ_v:

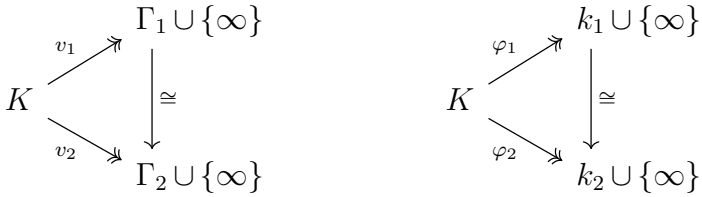
$$\begin{aligned} \varphi_v : K &\longrightarrow Kv \cup \{\infty\} \\ x &\longmapsto xv := \begin{cases} x\mathcal{M}_v & \text{if } x \in \mathcal{O}_v \\ \infty & \text{if } x \notin \mathcal{O}_v. \end{cases} \end{aligned}$$

Conversely, given a place $\varphi : K \longrightarrow\!\!\!\!\!\rightarrow k \cup \{\infty\}$, it induces a valuation

$$v_\varphi : K \longrightarrow\!\!\!\!\!\rightarrow K^\times/\mathcal{O}_\varphi^\times \cup \{\infty\}$$

via the valuation ring $\mathcal{O}_\varphi := \varphi^{-1}(k)$.

These two constructions are mutually inverse—except that we need to identify two valuations v_1, v_2 and places φ_1, φ_2 according to the following commutative diagrams:



Under this identification, v and v_{φ_v}, respectively, φ and φ_{v_φ}, become equivalent.

It will be crucial to translate between these three equivalent ways of viewing valuations.

3.1.1.4 Extensions of valuations

Let L/K be a field extension, and assume that L and K come equipped with valuations w and v, respectively. We say that $(L, w)/(K, v)$ is an *extension of valued fields*, and that w is a *prolongation* of v, if $w|_K$ is equivalent to v, or, correspondingly, $\mathcal{O}_v = \mathcal{O}_w \cap K$. Conversely, any valuation on (K, v) can be restricted to any subfield F of K such that $(K, v)/(F, v|_F)$ is an extension of valued fields.

The following facts are fundamental (for proofs, see e.g. [EP05, Chapter 3]):

Theorem 3.1.9 (Chevalley)**.** *Let L/K be an arbitrary extension of fields. Then any valuation v on K extends to some valuation w on L.*

Fact 3.1.10. *Let K be a field of characteristic $p > 0$ and L/K a purely inseparable extension. Then any valuation v on K extends uniquely to L via $v(x^{1/p^n}) = \frac{1}{p^n} v(x)$ for any $x^{1/p^n} \in L$.*

Fact 3.1.11. *Let $(L, w)/(K, v)$ be an algebraic extension of valued fields. Then any element in wL/vK has finite order, i.e., wL is contained in the divisible hull of vK, and Lw/Kv is an algebraic extension of residue fields.*

For transcendental extensions of valued fields, we have the following:

Fact 3.1.12 (Abhyankar (Dimension) Inequality)**.** *Let $(L, w)/(K, v)$ be an extension of valued fields with L/K finitely generated. Then*

$$\mathrm{td}(Lw/Kv) + \mathrm{rr}(wL/vK) \leq \mathrm{td}(L/K),$$

where $\mathrm{rr}(G) \coloneqq \dim_{\mathbb{Q}} G \otimes_{\mathbb{Z}} \mathbb{Q}$ denotes the rational rank *of an abelian group G.*

Fact 3.1.13. *Let (K, v) be a valued field and L/K an algebraic extension. If w_1 and w_2 denote valuations on L extending v, then $\mathcal{O}_{w_1} \subseteq \mathcal{O}_{w_2}$ implies $\mathcal{O}_{w_1} = \mathcal{O}_{w_2}$.*

In particular, it follows from the above that if w_1 and w_2 are not equivalent, then $\mathcal{O}_{w_1} \not\subseteq \mathcal{O}_{w_2}$ and $\mathcal{O}_{w_2} \not\subseteq \mathcal{O}_{w_1}$, i.e., the valuation rings of w_1 and w_2 are *incomparable*. Incomparable valuation rings satisfy the following form of the Chinese remainder theorem:

Fact 3.1.14 (Weak approximation theorem)**.** *Let $\mathcal{O}_{v_1}, \ldots, \mathcal{O}_{v_n}$ be pairwise incomparable valuation rings on K. Then, for any tuple $(x_i)_{i=1}^n \in \prod_{i=1}^n \mathcal{O}_{v_i}$, there exists $x \in K$ such that $x - x_i \in \mathcal{M}_{v_i}$ for $i = 1, \ldots, n$.*

The following describes the most basic connection to Galois theory:

Theorem 3.1.15 (Conjugacy Theorem)**.** *Let (K, v) be a valued field and L/K a normal algebraic extension. Then $\mathrm{Aut}(L/K)$ acts transitively on the set of extensions w of v, i.e., for any two extensions w and w' on L, there exists an automorphism $\sigma \in \mathrm{Aut}(L/K)$ such that $\mathcal{O}_{w'} = \sigma\mathcal{O}_w$.*

Beyond that, one can show that the conjugate roots of a polynomial $f(X)$ vary continuously in the coefficients of $f(X)$.

Fact 3.1.16 (Continuity of roots)**.** *Let (K, v) be a valued field and $\tilde{v}$ an extension of v to K^{sep}. Assume $f(X) = a_n X^n + \cdots + a_1 X + a_0$ is a polynomial over K with pairwise distinct roots $x_1, \ldots, x_n$. Then for any $\gamma \in vK$, there exists $\delta \in vK$ and a permutation $\sigma \in \mathfrak{S}_n$, such that for any polynomial $g(X) = b_n X^n + \cdots + b_1 X + b_0 \in K[X]$ with roots $y_1, \ldots, y_n$ satisfying*

$$\min_{1 \leq i \leq n} v(a_i - b_i) \geq \delta,$$

we have

$$\min_{1\le i\le n} \tilde{v}(x_i - y_{\sigma(i)}) \ge \gamma.$$

Remark 3.1.17. Note that if $\gamma > \max_{i\neq j} \tilde{v}(x_i - x_j)$, then additionally,

$$\tilde{v}(y_{\sigma(i)} - y_{\sigma(j)}) = \tilde{v}(x_i - x_j).$$

The following refines Fact 3.1.11 into a quantitative form:

Fact 3.1.18 (Fundamental inequality, simple form)**.** *Let $(L, w)/(K, v)$ be a finite extension of valued fields. Assume that*

$$A = \{a_i\}_{1\le i\le e} \subseteq L^\times \quad \text{and} \quad B = \{b_j\}_{1\le j\le f} \subseteq \mathcal{O}_w^\times$$

are given such that wA is a set of representatives for wL/vK and $Bw \subseteq Lw$ is Kv-linearly independent. Then

$$A \cdot B = \{a_i b_j\}_{\substack{1\le i\le e\\ 1\le j\le f}}$$

is K-linearly independent. In particular,

$$[L : K] \ge (wL : vK)[Lw : Kv]. \tag{3.1.2}$$

3.1.2 Structure theory

Ramification theory (sometimes also called Dedekind-Hilbert theory) relates the structure of Galois groups of extensions of valued fields to the structure of their basic invariants, the value group and residue field. For proofs, we point the reader to [Efr06, Chapters 15–17]. For valuations of higher rank, the theory is due to Krull and Deuring.

We have the following nomenclature for extensions of valued fields.

Definition 3.1.19. Let $(L, w)/(K, v)$ be a finite extension of valued fields. The basic ramification invariants of the extension are:

(a) the *ramification index* $e(w/v) \coloneqq (wL : vK) < \infty$, and

(b) the *inertia degree* $f(w/v) \coloneqq [Lw : Kv] < \infty$.

We say that the extension $(L, w)/(K, v)$ is

(c) *immediate* if $e(w/v) = f(w/v) = 1$;

(d) *inert* if $f(w/v) = [L : K]$;

(e) *unramified* if it is inert and Lw/Kv is separable;

(f) *totally ramified* if $e(w/v) = [L : K]$;

(g) *tamely ramified* if $e(w/v) = [L : K]$ and $p \nmid e(w/v)$ whenever $\operatorname{char} Kv = p > 0$;

(h) *tame* if $e(w/v)f(w/v) = [L : K]$, $p \nmid e(w/v)$, and Lw/Kv is separable ($\operatorname{char} Kv = p > 0$);

(i) *purely wild* if $e(w/v)$ is a power of p and Lw/Kv is purely inseparable (where $\operatorname{char} Kv = p > 0$).

For any of the above properties P, we say that an algebraic extension $(L, w)/(K, v)$ *is* P if all finite subextensions are P. In residue characteristic 0, by definition, all algebraic extensions are tame, and there are no non-trivial purely wild extensions.

3.1.2.1 General ramification theory

We associate to any Galois extension $(L, w)/(K, v)$ of valued fields a filtration

$$\operatorname{Gal}(L/K) \supseteq D_w(L/K) \supseteq I_w(L/K) \supseteq R_w(L/K) \qquad \text{(shortened: } G \supseteq D \supseteq I \supseteq R\text{)}$$

of the Galois group $G = \operatorname{Gal}(L/K)$.

Definition 3.1.20. We define

(a) the *decomposition group*

$$D \coloneqq \{\sigma \in G : \sigma\mathcal{O}_w = \mathcal{O}_w\} = \{\sigma \in G : \sigma(x) - x \in \mathcal{O}_w \text{ for all } x \in \mathcal{O}_w\};$$

(b) the *inertia group* $I \coloneqq \{\sigma \in G : \sigma(x) - x \in \mathcal{M}_w \text{ for all } x \in \mathcal{O}_w\}$;

(c) the *ramification group* $R \coloneqq \{\sigma \in G : \sigma(x) - x \in x\mathcal{M}_w \text{ for all } x \in \mathcal{O}_w\}$.

We denote the corresponding fixed fields by L^D, L^I, and L^R, respectively.

The groups D, I, and R encode structural information about $(L, w)/(K, v)$.

Fact 3.1.21 (Decomposition group D)**.** *Let $(L, w)/(K, v)$ be a Galois extension of valued fields. Then*

(i) $(L^D, w|_{L^D})/(K, v)$ is immediate.

(ii) w is the unique *prolongation of $w|_{L^D}$ to L.*

(iii) v *has exactly* $r = [L^D : K] = (G : D)$ *prolongations of* v *to* L.

Fact 3.1.22 (Inertia group I)**.** *The homomorphism*

$$\begin{aligned} \Phi : D &\longrightarrow \mathrm{Aut}(Lw/Kv) \\ \sigma &\longmapsto \left(\overline{x} \longmapsto \overline{\sigma(x)}\right) \end{aligned}$$

is well-defined. It induces a short exact sequence

$$1 \longrightarrow I \longrightarrow D \xrightarrow{\Phi} \mathrm{Aut}(Lw/Kv) \longrightarrow 1, \tag{3.1.3}$$

which we call the First Exact Sequence*. In particular,* I *is normal and closed in* D*. Moreover,*

(i) $L^I w|_{L^I}/Kv$ *is relatively separably closed in* Lw/Kv*.*

(ii) L^I/L^D *is inert. In particular,* $w|_{L^I} L^I = vK$*.*

Fact 3.1.23 (Ramification group R)**.** *Let* μ_{Lw} *denote the set of roots of unity in* Lw*. Then the homomorphism*

$$\begin{aligned} \Psi : I &\longrightarrow \mathrm{Hom}(wL/vK, \mu_{Lw}) \\ \sigma &\longmapsto \left(wx + vK \longmapsto \overline{\sigma(x)/x}\right) \end{aligned}$$

is well-defined and induces a short exact sequence

$$1 \longrightarrow R \longrightarrow I \xrightarrow{\Psi} \mathrm{Hom}(wL/vK, \mu_{Lw}) \longrightarrow 1, \tag{3.1.4}$$

which we call the Second Exact Sequence*. Moreover,*

(i) R *is a normal closed subgroup of* I*.*

(ii) R *is the unique normal Sylow* p*-subgroup of* I *whenever* $\mathrm{char}\, Kv = p > 0$*. It is trivial if* $\mathrm{char}\, Kv = 0$*.*

(iii) L^R/L^I *is tamely ramified and maximal with this property.*

These findings are summarised in the diagram on the next page.

Ramification theory gives rise to yet another multiplicative invariant called the *defect*, which measures the failure of the fundamental inequality $[L : K] = ef$. The fundamental inequality does not prominently appear in local class field theory because separable extensions of discretely valued fields always satisfy it, cf. [Neu68, Chapter II, (6.8)].

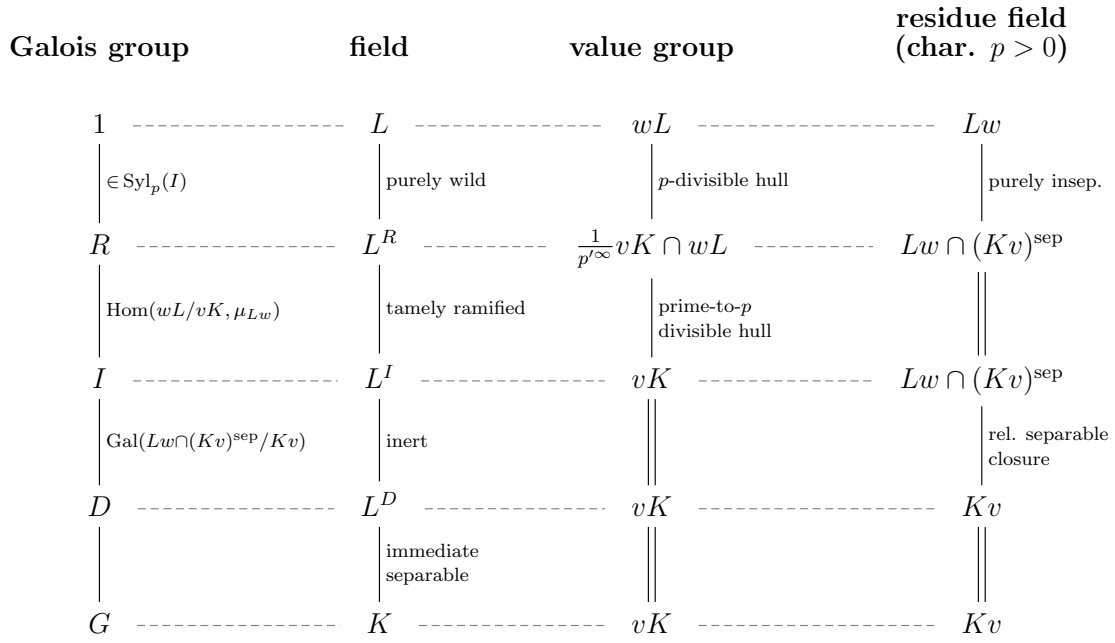


Diagram summarising the properties of the decomposition subgroup D, the inertia group I, and the ramification group R, as well as their respective fixed fields and corresponding value groups and residue fields (Facts 3.1.21, 3.1.22, 3.1.23). For $\operatorname{char} Kv = 0$, the first two rows collapse. See also [End72, p. 171].

Corollary/Definition 3.1.24 (Lemma of Ostrowski)**.** *Let (K, v) be a valued field and L/K a finite extension such that v has a unique prolongation w to L. Then*

$$d(w/v) := \frac{[L : K]}{e(w/v)f(w/v)}$$

is a power of p whenever $\operatorname{char} Kv = p > 0$, and equal to 1 if $\operatorname{char} Kv = 0$. The invariant $d(w/v)$ is called the defect *of L/K. The extension is called* defectless *if $d(w/v) = 1$.*

One proves the Lemma of Ostrowski by passing to a splitting field and applying the following consequence of the Conjugacy Theorem 3.1.15 and ramification theory:

Corollary 3.1.25 (Fundamental equality)**.** *Let $(L, w)/(K, v)$ be a finite Galois extension of valued fields. Let r be the number of prolongations of v to L (all of which are conjugate). Then*

$$[L : K] = refd,$$

where e, f, d are the ramification invariants of $(L, w)/(L^D, w|_{L^D})$.

As our main concern is with absolute Galois groups, we now consider the case $L = K^{\mathrm{sep}}$.

Definition 3.1.26. For a fixed prolongation $\tilde{v}$ of v to K^{sep}, write

$$\begin{aligned} D_K &\coloneqq D_{\tilde{v}}(K^{\mathrm{sep}}/K) \\ I_K &\coloneqq I_{\tilde{v}}\,(K^{\mathrm{sep}}/K) \\ R_K &\coloneqq R_{\tilde{v}}(K^{\mathrm{sep}}/K) \end{aligned}$$

to denote the *absolute* decomposition, inertia, and ramification groups, respectively. Furthermore, we say that (K, v) is

(a) *henselian* if $D_K = G_K$ (equivalently, $K = L^D$);

(b) *algebraically maximal* if every finite immediate extension is trivial;

(c) *tame* if K is perfect, henselian, and $R_K = 1$ (equivalently, any finite extension is tame).

In the absolute case, we have the following splitting result (cf. [Efr06, Corollary 22.1.2, Proposition 22.1.3]):

Theorem 3.1.27. *Let $L = K^{\mathrm{sep}}$. There is a semi-direct product decomposition*

$$D_K/R_K \cong \mathrm{Hom}(wL/vK, \mu_{Lw}) \rtimes G_{Kv},$$

where G_{Kv} acts naturally on the left. Moreover,

$$\mathrm{Hom}(wL/vK, \mu_{Lw}) \cong \prod_{q \neq p} \mathbb{Z}_q^{r_q},$$

where q runs over primes away from $p = \mathrm{char}\, Kv$, and

$$r_q \coloneqq \dim_{\mathbb{F}_q}(vK/qvK)$$

*denotes the q-*rank *of vK.*

Observe that, in view of the First (3.1.3) and Second Exact Sequence (3.1.4), Theorem 3.1.27 precisely expresses the existence of a section of

$$1 \to I_K/R_K \to D_K/R_K \to D_K/I_K \to 1. \tag{3.1.5}$$

In this light, the next theorem due to Kuhlmann, Pank, and Roquette [KPR86, Theorem 2.2] (see also [Efr06, Theorem 22.2.1]) provides a natural complement to Theorem 3.1.27. A reader familiar with this result may correctly object that its proof relies on Galois cohomology and therefore does not align with the elementary approach taken in this chapter. However, neither their theorem nor the ensuing corollary will be used in what follows; we include them here solely for completeness and for later reference in Chapter 4.

Theorem 3.1.28. *There exists a section for the following exact sequence.*

$$1 \to R_K \to D_K \to D_K/R_K \to 1$$

Composing the section in (3.1.5) with the section from Theorem 3.1.28, we get the following result (cf. [Efr06, Corollary 22.2.2]):

Corollary 3.1.29. *The (absolute) First Exact Sequence*

$$1 \to I_K \to D_K \to G_{Kv} \to 1$$

splits. In particular,

$$D_K \cong I_K \rtimes G_{Kv}.$$

We can use the First and Second Exact Sequence together with Theorem 3.1.27 to calculate concrete absolute Galois groups.

Example 3.1.30.

1. Consider $K = \mathbb{C}(\!(t)\!)$ with the t-adic valuation. It has value group $\mathbb{Z}$ and residue field $\mathbb{C}$. As a complete field of rank 1, $\mathbb{C}(\!(t)\!)$ is henselian (see next Section 3.1.2.2 for more context). By Fact 3.1.23(ii), $R_{\mathbb{C}(\!(t)\!)} = 1$. Moreover, $\mathrm{Aut}(\mathbb{C}^{\mathrm{sep}}/\mathbb{C}) = 1$. Therefore, combining the First (3.1.3) and Second Exact Sequences (3.1.4) with Theorem 3.1.27, we obtain

$$G_{\mathbb{C}(\!(t)\!)} = D_K \cong I_K \cong \prod_q \mathbb{Z}_q \cong \widehat{\mathbb{Z}}.$$

   Note that any finite field has absolute Galois group isomorphic to $\widehat{\mathbb{Z}} \cong G_{\mathbb{C}(\!(t)\!)}$!

2. Let k be an arbitrary field of characteristic 0. Consider the field of Puiseux series

$$K = \bigcup_{n>0} k(\!(t^{1/n})\!)$$

   with the t-adic valuation. The value group is $\mathbb{Q}$ and the residue field is k. The valuation on K is again henselian. Here, the First and Second Exact Sequences yield $I_K = 1$ and therefore

$$G_K = D_K \cong \mathrm{Aut}(k^{\mathrm{sep}}/k) = G_k.$$

Proposition 3.1.31. *Fix rational primes $p \neq q$. Then any Sylow q-subgroup of $G_{\mathbb{Q}_p}$ is isomorphic to $\mathbb{Z}_q \rtimes \mathbb{Z}_q$.*

Proof. Let G_q be a Sylow q-subgroup of $G_{\mathbb{Q}_p}$, and denote by (F_q, w_q) the fixed field of G_q with prolongation w_q of v_p. As G_q is a pro-q group, we must have $R_{F_q} = 1$ by Fact 3.1.23(ii). Moreover, $w_q F_q = \mathbb{Z}_{(q)}$ and $G_{F_q w_q} \cong \mathbb{Z}_q$ by infinite Galois theory. Therefore, Theorem 3.1.27 yields

$$G_q \cong G_q / R_{F_q} \cong \mathbb{Z}_q \rtimes \mathbb{Z}_q. \qquad \square$$

Remark 3.1.32. The group action in $\mathbb{Z}_q \rtimes \mathbb{Z}_q$ is the natural action arising from Theorem 3.1.27. Let τ denote the Frobenius element topologically generating the right copy of $\mathbb{Z}_q$; its action on elements σ in the left copy is given by $\phi_\tau(\sigma) = \sigma^p$ (cf. also [Efr06, Example 22.1.4]). In additive notation for $\mathbb{Z}_q$, this corresponds to multiplication by p. Hence, for general $(a, b), (c, d) \in \mathbb{Z}_q \rtimes \mathbb{Z}_q$, the group law is given by

$$(a, b) \cdot (c, d) = (a + p^b c,\ b + d).$$

In particular, $\mathbb{Z}_q \rtimes \mathbb{Z}_q$ is non-abelian.

The structure of Sylow p-subgroups of $G_{\mathbb{Q}_p}$ is also known, though somewhat more complicated. It was determined by Labute [Lab66], building on earlier work of Shafarevich [Sha47], Demuškin [Dem61], and Serre [Ser64].

3.1.2.2 Henselianity

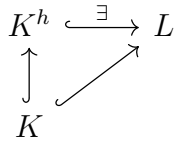
We have already introduced the single most important notion in valuation theory in passing: a valued field (K, v) is called *henselian* if $D_K = G_K$. Equivalently, (K, v) is henselian if and only if v extends uniquely to any fixed algebraic closure K^{alg} of K (recall that by Chevalley's Theorem 3.1.9, there exists at least one such extension, and valuations extend uniquely to inseparable extensions, see Fact 3.1.10). We point the reader to [EP05, Section 4.1].

It is possible to construct a henselian valued field from any given one in a universal fashion:

Definition 3.1.33. Let (K, v) be a valued field. Fix a separable closure K^{sep} of K and a prolongation $\tilde{v}$ of v to K^{sep}. We define $K^h := (K^{\mathrm{sep}})^D$ to be the fixed field of K^{sep} with respect to $D = D_{\tilde{v}}(K^{\mathrm{sep}}/K)$ and call it a *henselisation* of K.

By construction, K^h is henselian. A henselisation is only unique up to conjugation by an automorphism $\sigma \in G_K$ — nonetheless, one often speaks of "the" henselisation of K. The extension K^h/K is separable and immediate (Fact 3.1.21(i)), and further

satisfies the universal property that for any henselian valued field (L, w) extending (K, v), there exists a factorisation



of valued fields. The terminology arises from the fact that henselian valued fields are precisely those valued fields that satisfy *Hensel's Lemma*, which relates the roots of a polynomial $f(X) \in \mathcal{O}_v[X]$ with the roots of its coefficient-wise reduction $\overline{f}(X) \in (Kv)[X]$. Hensel originally proved his lemma for $\mathbb{Q}_p$.

Lemma 3.1.34 (Hensel's Lemma)**.** *A valued field (K, v) is henselian if and only if it satisfies the following property: given a monic polynomial $f(X) \in \mathcal{O}_v[X]$ and $a \in \mathcal{O}_v$ satisfying*

$$v(f(a)) > 2v(f'(a)),$$

then $f(X)$ has a unique root $\alpha \in \mathcal{O}_v$ with $v(\alpha - a) > v(f'(a))$. In particular, if $f(X)$ is such that the reduced polynomial $\overline{f}(X) \in (Kv)[X]$ has a simple root $\overline{a} \in Kv$, then $f(X)$ has a unique root $\alpha \in \mathcal{O}_v$ lifting $\overline{a}$.

Henselianity plays a role analogous to that of completeness in algebraic number theory: there, instead of the henselisation, one would consider the completion of a global field with respect to a non-Archimedean absolute value. Indeed, for all valued fields of rank 1, completeness implies henselianity. Another equivalent characterisation of henselianity is the following result, which is remarkably useful in practice.

Lemma 3.1.35 (Krasner's Lemma)**.** *A valued field (K, v) is henselian if and only if it satisfies the following property: given a separable element $x \in K^{\mathrm{sep}}$ with conjugates $x = x_1, \ldots, x_n$ and any algebraic element $y \in K^{\mathrm{alg}}$, the condition*

$$v(y - x) > \max_{2 \leq i \leq n} v(x_i - x),$$

implies $K(x) \subseteq K(y)$.

The following folklore result can be seen as a consequence of Krasner's Lemma. We refer the reader to [GKS, Proposition 2.34] for the proof.

Proposition 3.1.36. *Let (K, v) be a henselian valued field of rank 1. Then*

$$G_{\widehat{K}} \cong G_K.$$

Perhaps the most far-reaching reason for the importance of henselian valued fields is the fact that henselianity is a *first-order* property (it can be expressed as an axiom scheme via Hensel's Lemma 3.1.34). This allows the class of henselian valued fields (structures) to be studied via model theory. In contrast, completeness is not a first-order property (as it entails a cardinality bound). In model-theoretic practice, henselianity is used—among other things—to lift residue field embeddings to valued field embeddings, which has model-theoretic consequences through methods pioneered by A. Robinson. One key formative result in this direction is the *Ax-Kochen-Ershov Theorem.*

Theorem 3.1.37 (Ax-Kochen-Ershov)**.** *Let (K, v) and (K', v') be two henselian valued fields of equicharacteristic (0,0). Then:*

$$(K, v) \equiv (K', v') \iff vK \equiv v'K' \quad \textit{and} \quad Kv \equiv K'v'.$$

3.1.2.3 p-henselianity

An important weakening of henselianity in the context of pro-p groups is the notion of *p-henselianity.*

Definition 3.1.38. A valued field (K, v) is called *p-henselian* if v extends uniquely to any finite Galois extension of p-power degree, or equivalently, to the maximal pro-p Galois extension of K, which we denote by $K(p)$.

Hensel's Lemma still holds with the same statement as in Lemma 3.1.34 for polynomials $f(X) \in \mathcal{O}_v[X]$ that split in $K(p)$. The notion of p-henselianity admits the following useful characterisation:

Lemma 3.1.39 ([EP05, Theorem 4.2.2])**.** *Let (K, v) be a valued field. Then v is p-henselian if and only if v extends uniquely to any Galois extension of degree p.*

Proof. Without loss of generality, let F/K be a finite Galois extension of p-power degree, and assume that v extends uniquely to any degree p Galois extension of K. By the Conjugacy Theorem 3.1.15, $G = \mathrm{Gal}(F/K)$ acts transitively on the set of valuation rings $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$ of F extending $\mathcal{O}_v$. If $r > 1$, then $D = D_{\mathcal{O}_1}(F/K) \lneq G$, and we may choose a maximal proper subgroup $D \leq N < G$. For any finite p-group, the maximal proper subgroups are precisely the normal subgroups of index p (see, for example, [Rot95, Theorem 4.6(ii)]). So $N \lhd G$ is of index p. By the Galois correspondence, F^N/K is a Galois extension of degree p, so $\mathcal{O}_v$ extends uniquely to F^N by assumption. Thus, $N = \mathrm{Gal}(F/F^N)$ acts transitively on $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$ as

well. But now D is the stabiliser of $\mathcal{O}_1$ with respect to the action of either G or N, so

$$|G| = r \cdot |D| = |N|,$$

by the Orbit-Stabiliser Theorem, which is a contradiction. □

Corollary 3.1.40. *Let (K, v) be a valued field. If G_K is a pro-p group, then v is henselian if and only if v extends uniquely to any C_p-extension.*

Corollary 3.1.41 ([EP05, Corollary 4.2.4])**.** *Let (K, v) be a valued field such that $\mathrm{char}(Kv) \neq p$ and $\zeta_p \in K$. Then v is p-henselian if and only if $1 + \mathcal{M}_v \subseteq K^{\times p}$.*

Proof. $\Rightarrow$. Fix $a \in \mathcal{M}_v$ and consider the polynomial $f(X) = X^p - (1 + a) \in \mathcal{O}_v[X]$, which splits in $K(p)$. By the p-analogue of Hensel's Lemma, it has a root in $K^\times$.

$\Leftarrow$. By Lemma 3.1.39 and Kummer theory, it suffices to show that v extends uniquely to $K(x^{1/p})$ for any fixed $x \in K^\times \setminus K^{\times p}$. If $v(x) \notin pvK$, then

$$w\left(a_0 + a_1 x^{1/p} + \cdots + a_{p-1} x^{(p-1)/p}\right) = \min_{0 \leq i \leq p-1} w\left(a_i x^{i/p}\right) \quad \text{for all } a_0, \ldots, a_{p-1} \in K, \tag{3.1.6}$$

holds for any extension w of v and thus determines it uniquely. If $v(x) \in pvK$, we may assume without loss of generality that $v(x) = 0$. We must have $\overline{x} \notin Kv^{\times p}$, for otherwise, $1 + \mathcal{M}_v \subseteq K^{\times p}$ would imply $x \in K^{\times p}$. Hence, $[Kv(\overline{x}^{1/p}) : Kv] \geq p$, so v extends uniquely to $K(x^{1/p})$ by Corollary 3.1.25. □

3.1.3 Coarsenings and decomposition

Fix a field K. One may endow K with several different valuations (equivalently, valuation rings). The following relations are of particular significance.

Definition 3.1.42. Let v, w be valuations on a field K. Then w is a *coarsening* of v (and v is a *refinement* of w) if $\mathcal{O}_v \subseteq \mathcal{O}_w$. Moreover, we say v and w are *dependent* if $\mathcal{O}_v$ and $\mathcal{O}_w$ have a non-trivial common coarsening, i.e., the compositum $\mathcal{O}_v\mathcal{O}_w$ is not equal to K. Otherwise, we say v and w are *independent*.

The following two facts provide a first indication of the usefulness of these notions. Note that Fact 3.1.44 is a partial strengthening of the Weak Approximation Theorem (Fact 3.1.14).

Fact 3.1.43 ([EP05, Section 2.3])**.** *Let v, w be valuations on a field K. Then v and w induce the same topology on K if and only if $\mathcal{O}_v$ and $\mathcal{O}_w$ are dependent.*

Fact 3.1.44 (Approximation Theorem, [EP05, Theorem 2.4.1])**.** *Let $\mathcal{O}_{v_1}, \dots, \mathcal{O}_{v_n}$ be pairwise independent, non-trivial valuation rings on K. Given tuples $(x_i) \in K^n$ and $(\gamma_i) \in \prod_{i=1}^n v_i K$, there exists $x \in K$ such that*

$$v_i(x - x_i) > \gamma_i \quad \text{for } i = 1, \dots, n.$$

The full strength of coarsenings only becomes apparent when we shift our focus back to the valuation and place formalism.

Lemma 3.1.45. *Let v, w be valuations on a field K. The following are equivalent:*

(i) $\mathcal{O}_v \subseteq \mathcal{O}_w$*;*

(ii) $\mathcal{O}_v^\times \subseteq \mathcal{O}_w^\times$*;*

(iii) $\mathcal{M}_w \subseteq \mathcal{M}_v$ *[sic];*

(iv) there exists a convex subgroup $\Delta \leq \Gamma_v$ such that w is given by the composition

$$\begin{array}{ccccc} K^\times & \xrightarrow{\ v\ } & \Gamma_v & \longrightarrow & \Gamma_v/\Delta \cong \Gamma_w, \\ & \searrow^{w} & & & \nearrow \end{array}$$

and v induces a valuation $\overline{v}$ on Kw with $\overline{v}(Kw) = \Delta$ and $(Kw)\overline{v} = Kv$.

Proof (sketch). Note that

$$K = \mathcal{O}_v \sqcup \mathcal{M}_v^{-1} = \mathcal{O}_w \sqcup \mathcal{M}_w^{-1}$$

can be written as the disjoint union of elements of valuation ≥ 0 and < 0. Taking complements, this implies the—at first sight counterintuitive—inclusion $\mathcal{M}_w \subseteq \mathcal{M}_v$.

Given a convex subgroup $\Delta \leq \Gamma_v$, the composition of v with the natural quotient map

$$w : K^\times \xrightarrow{\ v\ } \Gamma_v \longrightarrow \Gamma_v/\Delta$$

is a valuation with valuation ring

$$\mathcal{O}_w = \{x \in K : w(x) \geq 0\} \supseteq \{x \in K : v(x) \geq 0\} = \mathcal{O}_v.$$

Conversely, given a coarsening $\mathcal{O}_v \subseteq \mathcal{O}_w$, we obtain a commutative diagram

$$\begin{array}{ccccc} K^\times & \longrightarrow & K^\times/\mathcal{O}_v^\times & \xrightarrow{\ q\ } & K^\times/\mathcal{O}_w^\times \\ & \searrow^{v} & \| & & \| \\ & & \Gamma_v & \xrightarrow{\ q'\ } & \Gamma_w \end{array}$$

where the dashed arrow q' is a weakly monotonic quotient map induced by q and the two isomorphisms. Unravelling definitions, one sees that $\Delta \coloneqq \ker q' = v(\mathcal{O}_w^\times)$ and $w = q' \circ v$. Furthermore, note that v restricts to a homomorphism $\mathcal{O}_w^\times \twoheadrightarrow \Delta$, which induces a well-defined valuation

$$\overline{v} : Kw^\times = \{x + \mathcal{M}_w : x \in \mathcal{O}_w^\times\} \twoheadrightarrow \Delta,$$

where

$$\mathcal{M}_w = \{x \in K : q'(v(x)) > 0\} = \{x \in K : v(x) > \Delta\}$$

is the coset of value ∞ with respect to $\overline{v}$. Moreover, we have

$$\mathcal{O}_{\overline{v}} = \overline{\mathcal{O}_v} = \mathcal{O}_v/\mathcal{M}_w \subseteq Kw = \mathcal{O}_w/\mathcal{M}_w$$
$$\mathcal{M}_{\overline{v}} = \overline{\mathcal{M}_v} = \mathcal{M}_v/\mathcal{M}_w,$$

and consequently, $(Kw)\overline{v} = Kv$. □

3.1.3.1 Composition of places

The second—and perhaps most practical—description of coarsenings is given by the formalism of places. Indeed, for a valued field (K, v) with a coarsening $\mathcal{O}_w \supseteq \mathcal{O}_v$, one can separate the structural information encoded in v into two parts using the coarsening $\mathcal{O}_w$. In the mixed characteristic case, there are two canonical choices of coarsenings, leading to the notion of *Standard Decomposition* that we will introduce in the next Section 3.1.3.2.

Let us now explain in more detail what is meant by "structural information" and how decompositions are obtained.

As seen above, the valuation w can be written as a composition

$$w : K^\times \xrightarrow{v} \Gamma_v \longrightarrow \Gamma_v/\Delta \cong \Gamma_w,$$

where $\Delta = v(\mathcal{O}_w^\times)$ is a convex subgroup of Γ_v, and v induces a valuation $\overline{v}$ on the residue field Kw. How can we express this setup in terms of places—namely, what is the relationship between φ_v, φ_w, and $\varphi_{\overline{v}}$, the places associated to v, w, and $\overline{v}$, respectively?

Let $a \in K$. By construction, these places act on a according to the following rules:

$$a \overset{\varphi_w}{\longmapsto} \begin{cases} \text{if } a \in \mathcal{O}_w : & a\mathcal{M}_w \overset{\varphi_{\overline{v}}}{\longmapsto} \begin{cases} a\mathcal{M}_v & \text{if } a \in \mathcal{O}_v \\ \infty & \text{if } a \notin \mathcal{O}_v \end{cases} \\ \text{if } a \notin \mathcal{O}_w : & \infty \end{cases}$$

Therefore, φ_v is—as a matter of fact—the composition of φ_w and $\varphi_{\overline{v}}$:

$$K \xrightarrow{\varphi_w} Kw \cup \{\infty\} \xrightarrow{\varphi_{\overline{v}}} Kv \cup \{\infty\}$$
$$\varphi_v$$

(Note that here we extend $\varphi_{\overline{v}}$ by the additional assignment $\infty \longmapsto \infty$.)

Conversely, the composition of two places $\varphi_w : K \longrightarrow Kw \cup \{\infty\}$ and $\psi : Kw \longrightarrow k \cup \{\infty\}$,

$$K \xrightarrow{\varphi_w} Kw \cup \{\infty\} \xrightarrow{\psi} k \cup \{\infty\},$$

gives rise to a coarsening $\mathcal{O}_w = \varphi_w^{-1}(Kw)$ of the valuation ring $\mathcal{O}_v \coloneqq \varphi_w^{-1}(\psi^{-1}(k))$. Again, these two constructions are mutually inverse (subject to the same proviso that equivalent places are identified; see the end of Section 3.1.1.3).

Slogan. *Any coarsening can be decomposed as a composition of places.*

Once and for all, we remark that, by abuse of notation, we will use valuation rings, valuations, and places interchangeably whenever there is no danger of confusion. As a final remark, we note that one of the key properties of decompositions is that they preserve and reflect henselianity.

Fact 3.1.46 ([EP05, Corollary 4.1.4])**.** *Let v be a valuation that decomposes as $v = \overline{v} \circ w$. Then v is henselian if and only if $\overline{v}$ and w are henselian.*

3.1.3.2 Standard Decomposition

Any valuation of mixed characteristic $(0, p)$ admits two canonical coarsenings, corresponding to the change in characteristic from 0 to p.

Theorem 3.1.47 (Standard Decomposition)**.** *Let (K, v) be a valued field of mixed characteristic $(0, p)$. Then v can be written as the composition of three places,*

$$v : K \xrightarrow{v_0} Kv_0 \cup \{\infty\} \xrightarrow{\overline{v_p}} Kv_p \cup \{\infty\} \xrightarrow{\overline{\overline{v}}} Kv \cup \{\infty\},$$

where

(a) v_0 is the finest coarsening with residue characteristic 0;

(b) v_p is the coarsest coarsening with residue characteristic p;

(c) $\overline{v}$ is the valuation induced by v on Kv_0;

(d) $\overline{v_p}$ is the valuation induced by v_p on Kv_0;

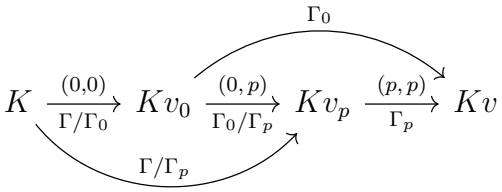
(e) $\overline{\overline{v}}$ *is the valuation induced by* v *on* Kv_p.

Furthermore, $\overline{v_p}$ *is of rank 1 and* $\overline{v}$ *has value group* $\mathrm{Conv}(v(p))$.

The proof relies on the correspondence between decompositions, coarsenings, and convex subgroups introduced already, with Fact 3.1.4 serving as the source of the rank-1 valuation $\overline{v_p}$. For the proof of a more general version of this theorem with explicit descriptions of the involved valuation rings and value groups, we refer the reader to [GKS, Theorem 2.46].

The valued field $(Kv_0, \overline{v})$ is often called the *core field* of (K, v). Fortunately, the above notation is consistent with writing v_p for the p-adic valuation on $\mathbb{Q}_p$.

To simplify notation even further, we will from now on omit the symbol "∞" when working with places. In this case, the decomposition can be written as follows:



Each arrow is labelled with the value group of the corresponding valuation. The three middle arrows are additionally labelled with the characteristic of the valuations.

Hence, $\overline{v_p}$ is the place at which a change in characteristic occurs for valuations of mixed characteristic $(0, p)$.

Slogan. *The* $(0, 0)$ *and* (p, p)*-equicharacteristic places in the Standard Decomposition are chosen maximally possible, thus creating a rank 1 place in the middle.*

3.1.3.3 Canonical henselian valuation

Fix a field K that is not separably closed. We will introduce the tree structure of the set of henselian valuations on K and determine a distinguished element v_K in it, which we call the *canonical henselian valuation*. We will show that the canonical henselian valuation admits a "going-down" statement (Theorem 3.1.54). More specifically, for the proof of the Theorem 3.0.1, v_K will be the source of a non-trivial valuation that gives K the structure of a p-adically closed field.

Everything that follows builds on F. K. Schmidt's Theorem, initially proven for complete rank 1 valued fields, but easily adapted to the henselian setting.

Theorem 3.1.48 (F. K. Schmidt)**.** *If K admits two independent and non-trivial henselian valuations, then K must be separably closed.*

Proof. Let v_1 and v_2 be independent non-trivial henselian valuations and assume $K \neq K^{\text{sep}}$. Furthermore, let $f(X) \in K[X]$ be a separable irreducible polynomial and $g(X) \in K[X]$ any polynomial of the same degree $n > 1$. If $g(X)$ is sufficiently close to $f(X)$ in each coefficient (with respect to a henselian valuation), then by continuity of roots (Fact 3.1.16), Remark 3.1.17, and Krasner's Lemma 3.1.35, $f(X)$ and $g(X)$ have the same splitting field. Now let $h(X)$ be any polynomial with precisely n distinct roots in K (i.e., a product of linear factors). By the Approximation Theorem (Fact 3.1.44), we may choose $g(X)$ sufficiently close to $f(X)$ with respect to v_1 and, at the same time, sufficiently close to $h(X)$ with respect to v_2, so that $f(X)$ and $h(X)$ have the same splitting field. This is a contradiction. □

Example 3.1.49. Let $\mathbb{C}_p$ be the completion of $\mathbb{Q}_p^{\text{alg}}$. By Proposition 3.1.36, $\mathbb{C}_p$ is algebraically closed. If $q \neq p$ is another prime, then there exists a non-canonical field isomorphism $\mathbb{C}_p \cong \mathbb{C}_q$ between algebraically closed fields of characteristic 0 and of size continuum (we forget the topology). In this way, $\mathbb{C}_p$ can be endowed with a natural p-adic topology and an abstract q-adic topology induced by the non-canonical isomorphism. The point of F. K. Schmidt's Theorem is that such an anomaly can only occur if K is separably closed.

Definition 3.1.50. Let $K \neq K^{\text{sep}}$ be a field. We partition the set of henselian valuation rings on K into two sets

$$H_1(K) \coloneqq \{\mathcal{O}_v : \mathcal{O}_v \text{ henselian with } Kv \underline{\text{not}} \text{ separably closed}\};$$
$$H_2(K) \coloneqq \{\mathcal{O}_v : \mathcal{O}_v \text{ henselian with } Kv \text{ separably closed}\}.$$

Lemma 3.1.51 (Tree structure)**.** *The coarsening relation induces the following structure:*

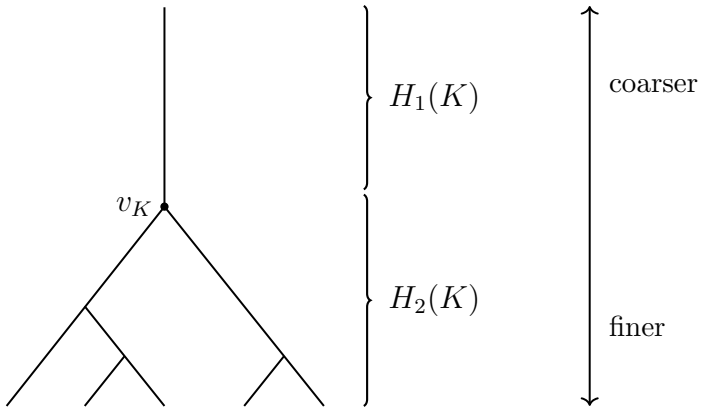
(i) *$H_1(K)$ is non-empty (it contains the trivial valuation) and linearly ordered by $\subseteq$.*

(ii) *Any valuation in $H_1(K)$ is coarser than any valuation in $H_2(K)$.*

(iii) *Any non-empty subset of $H_2(K)$ has a supremum (finest common coarsening) in $H_2(K)$.*

(iv) *If $H_2(K) = \emptyset$, then $H_1(K)$ has a minimum (a finest coarsening).*

In short, we get the following picture:



Proof (sketch). All valuations we consider will be henselian by virtue of Fact 3.1.46. Let $\mathcal{O}_w = \mathcal{O}_u\mathcal{O}_v$ be the finest common coarsening of two incomparable henselian valuation rings $\mathcal{O}_u$ and $\mathcal{O}_v$ on K. The proof boils down to the following observation: the induced valuations $\overline{u}$ and $\overline{v}$ on Kw are—by design—non-trivial independent henselian valuations. By F. K. Schmidt's Theorem 3.1.48, this implies that Kw is separably closed, which in turn implies that $Ku = (Kw)\overline{u}$ and $Kv = (Kw)\overline{v}$ are separably closed as well. This proves (i), (ii), and the fact that any finite subset in $H_2(K)$ has a supremum in $H_2(K)$. One can further show that for any non-empty subset $S \subseteq H_2(K)$, its supremum $\mathcal{O}_S$ (i.e., the ring generated by all $\mathcal{O} \in S$) is given by

$$\mathcal{O}_S = \left\{ x_1 \cdots x_n : x_1, \ldots, x_n \in \bigcup_{\mathcal{O} \in S} \mathcal{O},\ n \in \mathbb{N} \right\}, \tag{3.1.7}$$

and that it lies in $H_2(K)$ (cf. [EP05, Theorem 4.4.2]). Likewise, one can see that

$$\mathcal{O}_1 \coloneqq \bigcap_{\mathcal{O} \in H_1(K)} \mathcal{O}$$

is a valuation ring and the infimum of $H_1(K)$. □

Definition 3.1.52 (Canonical henselian valuation)**.** Let $K \neq K^{\text{sep}}$ be a field. The *canonical henselian valuation* v_K (with valuation ring $\mathcal{O}_{v_K}$) is defined to be

(i) the coarsest valuation in $H_2(K)$ if $H_2(K) \neq \emptyset$, and

(ii) the finest valuation in $H_1(K)$ otherwise.

If $H_2(K) \neq \emptyset$, then $\mathcal{O}_{v_K}$ does not lie in $H_1(K)$. We further define:

$$H(K) \coloneqq H_1(K) \cup \{\mathcal{O}_{v_K}\}$$

Note that any valuation in $H(K)$ is comparable to any other henselian valuation and that $\mathcal{O}_{v_K}$ is the minimum of $H(K)$.

Example 3.1.53. The canonical henselian valuation of $\mathbb{Q}_p$ is the p-adic valuation v_p. The only other henselian valuation on $\mathbb{Q}_p$ is the trivial one.

Proof. As $\mathbb{Q}_p v_p = \mathbb{F}_p$ is not separably closed, $\mathcal{O}_{v_p}$ is comparable to all other henselian valuation rings. It does not admit any proper refinement, since such a refinement would induce a non-trivial valuation on $\mathbb{F}_p$, which does not exist. Similarly, the value group of any coarsening is a quotient of $\mathbb{Z}$ by a convex subgroup. The only non-trivial convex subgroup is $\mathbb{Z}$ itself — the corresponding coarsening is the trivial valuation. □

3.1.3.4 "Henseling down"

By definition, henselianity "goes up" — any algebraic extension of a henselian valued field is henselian. The following partial converse was established only in 2003.

Theorem 3.1.54 (Henseling down, [Koe03, Proposition 3.1])**.** *Let L/K be an algebraic extension with L not separably closed. Consider a valuation w on L with $\mathcal{O}_w \in H(L)$. Then, the valuation ring of the restriction $v := w|_K$ lies in $H(K)$ in each of the following cases:*

(i) *L/K is normal.*

(ii) *L/K is finite.*

(iii) *G_L is a Sylow p-subgroup of G_K for some prime p. If $p = 2$, additionally assume that no proper coarsening of w has real closed residue field.*

Proof. (i) We need to establish two properties: first, that v is henselian, and second, that it is a coarsening of v_K. To prove that v is henselian, it suffices to show that w is the unique extension of v to L. So let w' be any prolongation of v to L. By the Conjugacy Theorem 3.1.15, w' is henselian. Since $\mathcal{O}_w \in H(L)$, it follows that $\mathcal{O}_w$ and $\mathcal{O}_{w'}$ are comparable. Hence, by Fact 3.1.13, $\mathcal{O}_w = \mathcal{O}_{w'}$.

For the second part, note that if $\mathcal{O}_w \in H_1(L)$, then $\mathcal{O}_v \in H_1(K)$ by the definition of $H_1(K)$. Thus, it remains to consider the case $w = v_L$. All proper coarsenings of v_L lie in $H_1(L)$, and hence their restrictions to K (and therefore, all proper coarsenings of v) lie in $H_1(K)$. This implies that $\mathcal{O}_v \in H(K)$ for $w = v_L$.

(ii) Essentially, the strategy is to pass to the splitting field of L/K and apply (i). Let N be the splitting field of L/K. Then w has a unique henselian prolongation w' to N. If $\mathcal{O}_{w'} \in H(N)$, the claim follows directly from (i). Otherwise, v_N is a proper coarsening of w', and both Nv_N and Nw' are separably closed. Hence, by Fact 3.1.13, $v_N|_L$ must be a proper coarsening of w as well. Since $\mathcal{O}_w \in H(L)$, it follows that $L(v_N|_L)$ is not separably closed. However, $Nv_N/L(v_N|_L)$ is finite, so $L(v_N|_L)$ must be real closed by the Artin-Schreier Theorem 1.1.2. Note that $L(v_N|_L)/K(v_N|_K)$ is finite, and therefore $L(v_N|_L) = K(v_N|_K)$ by the same theorem. In this setup, v_N restricts to a coarsening of w on L and to a coarsening of v on K, giving rise to induced valuations $\overline{w}$ and $\overline{v}$:

$$L \xrightarrow{v_N|_L} L(v_N|_L) \xrightarrow{\overline{w}} Lw \qquad K \xrightarrow{v_N|_K} K(v_N|_K) \xrightarrow{\overline{v}} Kv$$

By (i), $v_N|_K$ is henselian. Hence, by Fact 3.1.46, to show that v is henselian, it suffices to prove that $\overline{v}$ is henselian. Since w is henselian, so is $\overline{w}$ (Fact 3.1.46, again). Moreover, as $v = w|_K$, we have $\mathcal{O}_{\overline{v}} = \mathcal{O}_{\overline{w}}$, which implies that $\overline{v}$ is henselian. We conclude $\mathcal{O}_v \in H(K)$ as before.

(iii) To show that v is henselian, let F/K be a finite Galois extension. We must show that v has a unique prolongation to F. Clearly, one such prolongation is $v_1 := \widetilde{w}|_F$, where $\widetilde{w}$ denotes the unique prolongation of w to K^{sep}. Let v_2 be any other prolongation of v to F, and let $\widetilde{v_2}$ denote a prolongation of v_2 to K^{sep}. By the Conjugacy Theorem 3.1.15, there exists $\sigma \in G_K$ such that $\mathcal{O}_{\widetilde{v_2}} = \sigma\mathcal{O}_{\widetilde{w}}$.

Additionally, set $M := LF$. Recall that $G_L \in \mathrm{Syl}_p(G_K)$, where $\mathrm{Syl}_p(G_K)$ denotes the set of Sylow p-subgroups of G_K.

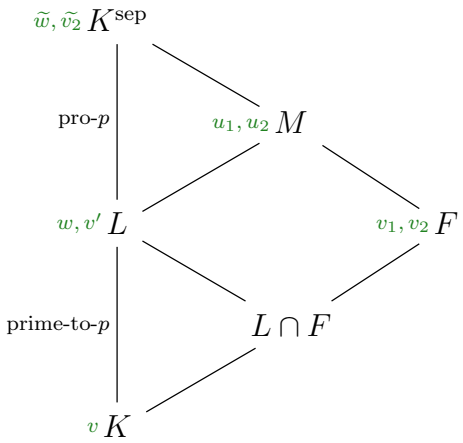


Diagram of fields in the proof; colours indicate the valuations considered for each field.

Since K^{sep}/L is a pro-p extension, so is K^{sep}/M. Similarly, $L/(L\cap F)$ is a prime-to-p extension, hence so is M/F. Therefore, $G_M \in \mathrm{Syl}_p G_F$.

As F/K is Galois, we have $\sigma F = F$, so $F \subseteq \sigma M$. Applying the preceding argument to σM in place of M (with σL replacing L), we find that $G_{\sigma M} \in \mathrm{Syl}_p G_F$ as well. By the second pro-finite Sylow Theorem (see [RZ10, Corollary 2.3.6 (c)]), G_M and $G_{\sigma M}$ are conjugate in G_F, so there exists $\tau \in G_F$ with $\tau(M) = \sigma M$. Hence, $u_2 \coloneqq \widetilde{v_2}|_{\sigma M} \circ \tau$ is a henselian prolongation of v to M, which restricts to v_2 on F.

To show that $v_1 = v_2$, it suffices to prove that $u_1 \coloneqq \widetilde{w}|_M$ and u_2 coincide. By Fact 3.1.13, it is enough to show that $\mathcal{O}_{u_1}$ and $\mathcal{O}_{u_2}$ are comparable. This holds if $u_1 \in H(M)$ or $u_2 \in H(M)$. Suppose, for contradiction, that v_M is a proper coarsening of both u_1 and u_2. Then, $v' \coloneqq v_M|_L$ is a proper coarsening of $w = u_1|_L$ (again by Fact 3.1.13), and hence its residue field Lv' is not separably closed. Consequently, the residue field extension Mv_M/Lv' is finite with Mv_M separably closed, which is only possible if Lv' is real closed. In this case, $[Mv_M : Lv'] = 2$ implies $2 \mid [M : L]$ by the fundamental equality (Corollary 3.1.25), so we must have $p = 2$. Our standing assumption for $p = 2$ excludes the existence of the valuation v', yielding a contradiction.

Finally, by the same argument as in part (i), we conclude $v \in H(K)$. □

Later, we will need an additional technical fact about real closed fields to handle the special case $p = 2$ in the Galois characterisation of henselianity in Section 3.2.5.

Fact 3.1.55 ([EP05, p. 109])**.** *Let K be a field and $\mathcal{O}_w \in H_1(K)$ a henselian valuation ring with real closed residue field. Then any henselian refinement $\mathcal{O}_v \in H_1(K)$ of w will also have real closed residue field. In particular, if K admits at least one henselian valuation with real closed residue field, then it has a coarsest one.*

The proof relies on the observation that henselian valuation rings on K are convex with respect to any ordering on K (see [EP05, Lemma 4.3.6]), and that any ordering on K induces an ordering on the residue field Kv of any convex valuation ring $\mathcal{O}_v \subseteq K$.

3.1.4 Creation of valuations

One of our main ingredients, the Galois characterisation of henselianity (Theorem 3.2.22), requires us to *create* a valuation on a field K based on abstract properties of K — out of thin air, as it would seem. The constructions originate in

quadratic form theory, developed in the works of Arason, Bröcker, Elman, Jacob, and Ware [Brö76, Jac81, War81, War92, AEJ87], and later adapted by Hwang, Jacob, and Koenigsmann [HJ95, Koe95].

Leitfaden. The purpose of this section is to explain the proof of Theorem 3.1.68, which provides a sufficient condition for the existence of a non-trivial valuation with non-p-divisible value group on K, based on the interplay between $K^{\times p}$ and the additive structure of the field K. Historically, the somewhat computational proof was hard to motivate. It turns out that the computations involved work in a much more general setup — this setup, however, is easier to motivate. We follow Efrat's abstract approach (§11 and §26.4 in his book [Efr06]) using S-compatible valuations (see Definition 3.1.56). Later, we will specialise to our case of interest.

3.1.4.1 Creating valuations from rigid elements

Certainly, any field K can be endowed with the trivial valuation. What we are looking for are abstract properties of K that guarantee the existence of a valuation v that is *as non-trivial as possible*. This is realised by the idea of *multiplicative stratification*, which is made precise as follows:

Definition 3.1.56. Let $S \leq H$ be multiplicative subgroups of $K^\times$. Define two sets of valuation rings on K,

$$\begin{aligned} \mathrm{Val}(S) &:= \{\mathcal{O}_v \subseteq K \text{ val. ring} : 1 + \mathcal{M}_v \leq S\}, \text{ and} \\ \mathrm{Val}(S, H) &:= \{\mathcal{O}_v \in \mathrm{Val}(S) : \mathcal{O}_v^\times \leq H\}. \end{aligned}$$

A valuation v is *S-compatible* if $\mathcal{O}_v \in \mathrm{Val}(S)$.

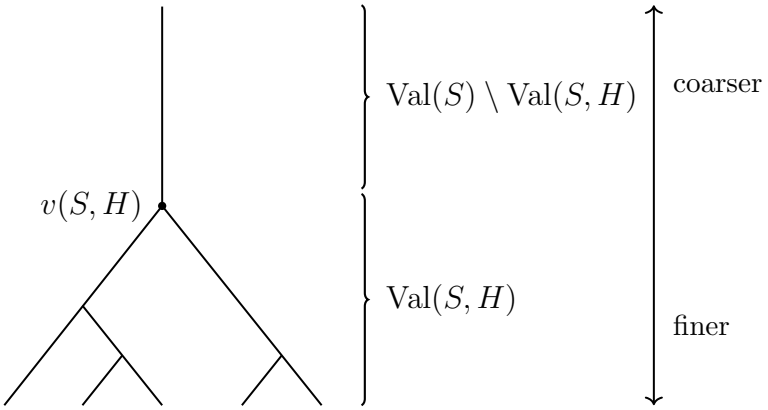
The parameters S and H *stratify* possible valuation rings into the sets $\mathrm{Val}(S)$ and $\mathrm{Val}(S, H)$. If v is trivial on K, then $1 + \mathcal{M}_v = \{1\}$ and $\mathcal{O}_v^\times = K^\times$. Hence, S and H control the non-triviality of v. Strikingly, $\mathrm{Val}(S)$ and $\mathrm{Val}(S, H)$ fit into a hierarchy analogous to the tree $H_1(K) \cup H_2(K)$ of henselian valuations (cf. Lemma 3.1.51). In this sense, the condition $1 + \mathcal{M}_v \leq S$ defining $\mathrm{Val}(S)$ can be seen as a weak analogue of henselianity.

Proposition 3.1.57 ([Efr06, Lemma 11.1.2])**.** *Let $S \leq H \leq K^\times$ be multiplicative subgroups. The set $\mathrm{Val}(S)$, ordered by the coarsening relation, has the following properties:*

(i) $\mathrm{Val}(S) \setminus \mathrm{Val}(S, H)$ *is linearly ordered and any* $\mathcal{O}_w \in \mathrm{Val}(S) \setminus \mathrm{Val}(S, H)$ *is coarser than any* $\mathcal{O}_v \in \mathrm{Val}(S, H)$.

(ii) $\mathrm{Val}(S, H)$ *is closed under refinements.*

(iii) Any non-empty subset of $\mathrm{Val}(S, H)$ *has a supremum (i.e., a finest common coarsening) in* $\mathrm{Val}(S, H)$*. If* $\mathrm{Val}(S, H) \neq \emptyset$*, we write* $v(S, H)$ *for the coarsest valuation in* $\mathrm{Val}(S, H)$*. In particular,* $v(S, H)$ *is comparable to any valuation in* $\mathrm{Val}(S)$*.*



In our reasoning, the question now is how to identify suitable candidates for subgroups $S \leq H \leq K^\times$ such that S is sufficiently large, H is sufficiently small, and, moreover, to establish a criterion for the non-emptiness of $\mathrm{Val}(S, H)$. The key to this is the following explicit description of $v(S, H)$.

Definition 3.1.58. Given $S \leq H \leq K^\times$, define

$$\begin{aligned} \mathcal{O}^-(S, H) &\coloneqq (1 - S) \setminus H \\ \mathcal{O}^+(S, H) &\coloneqq \{x \in H : x\mathcal{O}^-(S, H) \subseteq \mathcal{O}^-(S, H)\} \\ \mathcal{O}(S, H) &\coloneqq \mathcal{O}^-(S, H) \cup \mathcal{O}^+(S, H). \end{aligned}$$

Consider the case that $S = 1 + \mathcal{M}_v$ and $H = \mathcal{O}_v^\times$ for some valuation v on K. Then

$$\mathcal{O}^-(S, H) = \mathcal{M}_v, \ \mathcal{O}^+(S, H) = \mathcal{O}_v^\times, \text{ and } \ \mathcal{O}(S, H) = \mathcal{O}_v.$$

Therefore, $\mathcal{O}^-(S, H)$ is supposed to model the maximal ideal, $\mathcal{O}^+(S, H)$ the units, and $\mathcal{O}(S, H)$ the valuation ring of the valuation we aim to construct.

Proposition 3.1.59 ([Efr06, Theorem 11.3.6])**.** *The following statements are equivalent:*

(i) $\mathrm{Val}(S, H)$ *is non-empty;*

(ii) $\mathcal{O}(S, H)$ *lies in* $\mathrm{Val}(S, H)$*;*

(iii) $\mathcal{O}(S, H)$ *is equal to the valuation ring* $\mathcal{O}_{v(S,H)}$ *of* $v(S, H)$*.*

By doing computations with $\mathcal{O}(S,H)$, which gives an explicit description of $v(S,H)$, one can derive a criterion for the non-emptiness of $\mathrm{Val}(S,H)$. This, in turn, relies crucially on the notion of *rigidity* coming from the theory of quadratic forms.

Definition 3.1.60. Fix a subgroup $S \leq K^\times$. An element $x \in K^\times$ is *S-rigid* (or simply: *rigid*) if $S + xS \subseteq S \cup xS$, or equivalently, $1 + xS \subseteq S \cup xS$. Write

$$A(S) \coloneqq \{-x \in K^\times : 1 + x \notin S \cup xS\} = \{x \in K^\times : 1 - x, 1 - x^{-1} \notin S\}$$

for a distinguished set of additive inverses of non-rigid elements, which we use in the proposition below.

The notion of rigidity is in harmony with the ultrametric triangle inequality for valuations: if $S = 1 + \mathcal{M}_v$, and $H = \mathcal{O}_v^\times$, then any element in $K^\times \setminus H$ is rigid and $A(S) = \mathcal{O}_v^\times$. Note that our first goal is to formulate a full criterion determining for which H (depending on S) the set $\mathrm{Val}(S,H)$ is non-empty.

Proposition 3.1.61. *Let $S \leq H \leq K^\times$. The following conditions are equivalent:*

(i) $\mathrm{Val}(S,H)$ *is non-empty;*

(ii) -1 *and* $A(S)$ *are contained in* H*, and* $\mathcal{O}^-(S,H)$ *satisfies the closure property*

$$\mathcal{O}^-(S,H)\mathcal{O}^-(S,H) \subseteq 1 - S; \tag{$\dagger$}$$

(iii) every $x \in K^\times \setminus H$ is rigid and $\mathcal{O}^-(S,H)$ satisfies ($\dagger$).

Proof. (i) $\Leftrightarrow$ (ii). See [Efr06, Theorem 11.3.6] for the proof of this equivalence.

(ii) $\Leftrightarrow$ (iii). Assume $-1 \in H$ and $A(S) \subseteq H$. Let x be non-rigid, i.e., there exists $s \in S$ such that $1 + xs \notin S \cup xS$. Then $-xs \in A(S) \subseteq H$, and therefore, $x \in H$.

Conversely, assume that each $x \in K^\times \setminus H$ is rigid. Note that -1 is non-rigid, so $-1 \in H$. If $x \in A(S)$, then $-x$ is non-rigid, hence $x \in H$. □

This proposition shows that non-rigid elements and ($\dagger$) are the only obstructions to creating valuations in the aforementioned sense, motivating the following:

Definition 3.1.62. Fix $S \leq K^\times$. We define

$$H_S \coloneqq \langle -1, S, A(S)\rangle \leq K^\times.$$

Equivalently, H_S is the group generated by S and all non-rigid elements with respect to S. We call H_S the *non-rigid hull of S*.

The last ingredient we need is an additional fact about property (†): it allows us to tweak H slightly to ensure that (†) holds.

Lemma 3.1.63 ([Efr06, Proposition 11.4.2])**.** *Given $S \leq H_S \leq H$, assume that $a, b \in \mathcal{O}^-(S, H)$ violate (†), i.e., $ab \notin 1 - S$. Then $a^2 \in S$ and $\mathcal{O}^-(S, \langle H, a\rangle)$ satisfies (†).*

Theorem 3.1.64 (Creating valuations from rigid elements)**.** *The set $\mathrm{Val}(S, H)$ is non-empty if and only if*

(i) $H_S \leq H$ in case that $\mathrm{Val}(S, H_S) \neq \emptyset$, or

(ii) $H_S < H' \leq H$, where $(H' : H_S) = 2$, $H' = \langle H, a\rangle$, and $a \in \mathcal{O}^-(S, H_S)$ is an element as in the preceding lemma (in case that $\mathrm{Val}(S, H_S) = \emptyset$).

In particular, if no element in $K^\times/S$ has order two, (ii) cannot hold, and we must have $\mathrm{Val}(S, H_S) \neq \emptyset$. In that case, $H_S \neq K^\times$ implies that $\mathcal{O}(S, H_S)$ is a non-trivial valuation ring.

Proof. In essence, this is [Efr06, Theorem 11.4.4]. The theorem follows directly from the above: Proposition 3.1.61 shows that $H_S \leq H$ is a necessary condition and Lemma 3.1.63 describes how to choose H' in the case $\mathrm{Val}(S, H_S) = \emptyset$. □

We may now drop the S-compatibility requirement for valuation rings and replace it with a condition on the value group:

Corollary 3.1.65 ([Efr06, Theorem 11.4.5])**.** *Let $S \leq K^\times$ be a subgroup such that no element in $K^\times/S$ has order two. Then the following are equivalent:*

(i) there exists a (non-trivial) valuation v on $K^\times$ with $v(K^\times) \neq v(S)$;

(ii) the non-rigid hull H_S is a proper subgroup of $K^\times$.

Proof. (i) ⇒ (ii). Let $H = \mathcal{O}_v^\times S = v^{-1}(v(S))$, which is a proper subgroup of $K^\times$ since $v(K^\times) \neq v(S)$. The ultrametric triangle inequality for v implies that $A(S) \subseteq H$. Therefore, $H_S \leq H$ are proper subgroups of $K^\times$.

(ii) ⇒ (i). By Theorem 3.1.64, $\mathcal{O}_v \coloneqq \mathcal{O}(S, H_S)$ is a non-trivial valuation ring. We cannot have $v(K^\times) = v(S)$, for then $K^\times = \mathcal{O}_v^\times S \leq H_S$, but H_S is supposed to be a proper subgroup. Hence, v is non-trivial with $v(K^\times) \neq v(S)$. □

In [Jac81, War81, AEJ87, Koe95], $\mathcal{O}(S,H)$ is constructed directly as in Definition 3.1.58. Without the additional context of the tree of S-compatible valuations and its canonical member $v(S,H)$, the construction of the non-trivial valuation ring $\mathcal{O}(S,H_S)$, together with the associated choice of H_S via rigid elements, can appear somewhat mysterious (see the discussion in [Efr06, p. xi]).

3.1.4.2 Creating valuations from p-rigid elements

In the context of the Galois characterisation of henselianity, we do not construct H_S directly. Instead, we will see that considerations from Kummer theory more naturally lead to the study of subgroups $T \leq K^\times$ that satisfy a weaker form of rigidity.

Definition 3.1.66. Fix a prime p, and let $-1 \in S \leq K^\times$. We say an element $x \in K^\times$ is *p-rigid* if

$$S + xS \subseteq \bigcup_{i=0}^{p-1} x^i S.$$

Let $T_S \leq K^\times$ be the *non-p-rigid hull of S*, i.e., the subgroup generated by S and all non-p-rigid elements $x \in K^\times$. Equivalently, T_S is generated by S and all $x \in K^\times$ that satisfy

$$1 - x \notin \bigcup_{i=0}^{p-1} x^i S.$$

Note that any $x \in K^\times \setminus S$ is p-rigid, whenever we consider a valuation v on K and we choose $S = \mathcal{O}_v^\times K^{\times p}$. This example trivialises if vK is p-divisible, because then $\mathcal{O}_v^\times K^{\times p} = K^\times$.

Since there are more non-rigid elements than non-p-rigid elements, it is clear that $T_S \leq H_S$. The goal is to bound the index $(H_S : T_S)$, so that the non-triviality of $(K^\times : H_S)$ can be expressed as a condition on $(K^\times : T_S)$. This final step was nicknamed the "wonderful creation of rigid elements" in [Koe03, Chapter 2.5].

Lemma 3.1.67 (From p-rigid to rigid elements)**.** *Let $S \leq K^\times$ be a subgroup that contains -1 and $K^{\times p}$. If $a, b \in A(S)$, then a and b have $\mathbb{F}_p$-linearly dependent cosets[1] in $K^\times/T_S$. In particular, $(H_S : T_S) \leq p$.*

Proof. Our proof is an adaptation of [Efr06, Lemma 26.4.2, Proposition 26.4.3], which itself is based on [HJ95, Proposition 2.5].

[1] Note that since $K^{\times p} \leq T_S$, the abelian group $K^\times/T_S$ has exponent p.

Let $x, y \in K^\times \setminus T_S$ represent $\mathbb{F}_p$-linearly independent cosets in $K^\times/T_S$. By assumption, x, y, and $xy \in K^\times \setminus T_S$ are p-rigid, so we there are unique $i, j, k \in \{0, \dots, p-1\}$ such that

$$1 - x \in x^i S, \quad 1 - y \in y^j S, \quad 1 - xy \in (xy)^k S.$$

We expect some kind of relationship between i, j, and k, which we now determine as a first step. We may write

$$1 - xy = (1 - x) + x(1 - y) \in x^i S + xy^j S = x^i(S + x^{1-i}y^j S).$$

If $(i, j) \neq (1, 0)$, then $x^{1-i}y^j \notin T_S$ is p-rigid and hence

$$1 - xy \in x^i(S + x^{1-i}y^j S) \subseteq \bigcup_{l=0}^{p-1} x^i(x^{1-i}y^j)^l S.$$

Moreover, recall that $1 - xy \in (xy)^k S$. Viewing the exponents of x and y as $\mathbb{F}_p$-coordinates in $\langle x, y, S\rangle/S$, we deduce that there exists a unique $l \in \{0, \dots, p-1\}$ such that

$$k \equiv i + (1 - i)l \equiv jl \pmod{p}.$$

This implies

$$i \equiv (i + j - 1)l \pmod{p} \Longrightarrow ij \equiv (i + j - 1)jl \equiv (i + j - 1)k \pmod{p}.$$

If $(i, j) \neq (0, 1), (1, 0)$, then $k \neq 0$ implies $i, j \neq 0$. In that case, we can rearrange as

$$(1 - i^{-1})(1 - j^{-1}) \equiv (1 - k^{-1}) \pmod{p}. \tag{3.1.8}$$

This analysis therefore yields the desired relationship between i, j, k, and allows us to define a sign function $\chi : K^\times \setminus T_S \longrightarrow \mathbb{F}_p$ via

$$\chi(x) \coloneqq \begin{cases} 1 - i^{-1} & \text{if } i \neq 0 \text{ and } 1 - x \in x^i S \\ 0 & \text{if } 1 - x \in S. \end{cases}$$

From this definition and (3.1.8), we conclude that χ satisfies the properties:

(i) $1 \notin \mathrm{im}(\chi)$;

(ii) $\chi(x) = 0$ if and only if $1 - x \in S \cup xS$;

(iii) if $x, y \in K^\times \setminus T_S$ have linearly independent cosets in $K^\times/T_S$, and $\chi(x) \neq 0$ or $\chi(y) \neq 0$, then $\chi(xy) = \chi(x)\chi(y)$.

Finally, assume there exist $a, b \in A(S)$ that represent linearly independent cosets in $K^\times/T_S$. We will show that this is impossible by the properties of χ.

Note that (ii) implies $\chi(a), \chi(b) \neq 0$. Using (iii) inductively, we obtain

$$\chi(a^{p-1}b) = \chi(a)^{p-1}\chi(b) \quad \text{and} \quad \chi(a^{p-1}b) = \chi(a^{p-1})\chi(b).$$

But since $\chi(a)^{p-1} = 1$, it follows that $\chi(a^{p-1}) = 1$, contradicting (i). □

Putting everything together, we conclude:

Theorem 3.1.68 (Creating valuations from p-rigid elements)**.** *Let p be any prime, and let $S \leq K^\times$ be a subgroup containing -1 and $K^{\times p}$. If $(K^\times : T_S) > p$, then there exists a non-trivial valuation v on K with non-p-divisible value group, i.e., $vK \neq pvK$.*

Proof. For $p = 2$, we have $T_S = H_S$. By Theorem 3.1.64, there exists $H_S \leq H' \lneq K^\times$ for which $\mathcal{O}_v = \mathcal{O}(S, H')$ is a non-trivial valuation ring. We cannot have $vK = 2vK$, for otherwise, $K^\times = \mathcal{O}_v^\times K^{\times 2} \subseteq H'$.

For $p > 2$, Lemma 3.1.67 implies that $(K^\times : H_S) > 1$. Note that any element in $K^\times/S$ has odd order dividing p. Finally, by Corollary 3.1.65, there exists a valuation v on K with

$$pvK = v(K^{\times p}) \subseteq v(S) \neq v(K^\times) = vK.$$ □

As a final remark, let us note that all known proofs of Theorem 3.0.1 rely on the creation of valuations: in each case, the above construction serves as the original source of an abstract valuation for fields with absolute Galois group isomorphic to $G_{\mathbb{Q}_p}$.

3.1.5 First-order languages for valued fields

In the below, we view ordered groups, valued fields, etc., as model-theoretic structures. For the avoidance of doubt, we specify here the precise first-order languages that we use.

We regard fields as structures in the language of rings

$$\mathcal{L}_{\text{ring}} := \{0, 1, +, -, \cdot\},$$

and ordered abelian groups as structures in the language

$$\mathcal{L}_{\text{oag}} := \{0, +, -, \leq\}.$$

Here, $+, -, \cdot$ are binary function symbols, and $\leq$ is a binary relation symbol. Our language for valued fields is

$$\mathcal{L}_{\mathrm{VF}} \coloneqq (\mathsf{VF}, \mathsf{VG}, \mathsf{RF};\, v, \mathrm{res}),$$

a three-sorted language consisting of sorts for the underlying valued field, the value group, and the residue field. For VF and RF we have the same symbols as in $\mathcal{L}_{\mathrm{ring}}$, and VG is given the symbols in $\mathcal{L}_{\mathrm{oag}}$; additionally, $\mathcal{L}_{\mathrm{VF}}$ contains two unary function symbols $v : \mathsf{VF} \longrightarrow \mathsf{VG}$ and $\mathrm{res} : \mathsf{VF} \longrightarrow \mathsf{RF}$, interpreted as the valuation and residue maps, respectively.

A more economical, one-sorted language for valued fields is

$$\mathcal{L}_{\mathrm{val}} \coloneqq \mathcal{L}_{\mathrm{ring}} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is a unary predicate interpreted as a valuation ring. The languages $\mathcal{L}_{\mathrm{VF}}$ and $\mathcal{L}_{\mathrm{val}}$ have the same expressive power; formulas may differ in complexity.

Fact 3.1.69. *The $\mathcal{L}_{\mathrm{VF}}$- and $\mathcal{L}_{\mathrm{val}}$-structure of a valued field (K, v) are uniformly bi-interpretable. In particular, for any two valued fields (K, v) and (K, v'), we have*

$$(K, vK, Kv;\, v, \mathrm{res}) \equiv_{\mathcal{L}_{\mathrm{VF}}} (K', v'K', K'v';\, v', \mathrm{res}') \iff (K, \mathcal{O}_v) \equiv_{\mathcal{L}_{\mathrm{val}}} (K', \mathcal{O}_{v'}).$$

For brevity, we will simply write (K, v) for the entire $\mathcal{L}_{\mathrm{VF}}$-structure.

3.2 Valuations and absolute Galois groups

3.2.1 The explicit structure of $\mathbb{Q}_p$

This section deals with the structure of $\mathbb{Q}_p$, which we have already explored in Chapter 2. Here, we revisit and generalise some of the results discovered there to the more general setting of p-adically closed fields.

3.2.1.1 Cyclotomic extensions

In the context of Theorem 3.0.1, we consider the situation where a field K satisfies $G_K \cong G_{\mathbb{Q}_p}$. To draw conclusions about the roots of unity contained in K, we seek a purely Galois-theoretic criterion that identifies the roots of unity in K. This motivates the following lemma.

Lemma 3.2.1. *Let (K, v) be a henselian valued field, and let q be any prime. Assume that*

(i) $\operatorname{char} Kv \neq q$;

(ii) vK *is not* q*-divisible;*

(iii) $\mathrm{Gal}(Kv(q)/Kv) \cong \mathbb{Z}_q$, *where* $Kv(q)$ *is the maximal pro-*q *Galois extension.*

Then, for any $r \geq 1$,

$$\zeta_{q^r} \in K \quad \textit{if and only if} \quad K \textit{ admits a } C_{q^r} \times C_{q^r}\textit{-extension.}$$

In particular, the lemma applies to $(K, v) = (\mathbb{Q}_p, v_p)$ *for* $p \neq q$.

Proof. Note that the assumptions hold for $K = \mathbb{Q}_p$ by the Galois theory of finite fields.

Assume $\zeta_{q^r} \in K$. By assumption (iii), K admits an unramified C_{q^r}-extension. Moreover, by (ii), we may choose $x \in K$ with $v(x)$ not q-divisible and consider the totally ramified Kummer extension $K(\sqrt[q^r]{x})/K$, which is well-defined by (i) and the existence of a primitive q^r-th root of unity. Any unramified and totally ramified extensions of K are linearly disjoint, so taking the compositum of these two C_{q^r}-extensions yields the desired $C_{q^r} \times C_{q^r}$-extension.

Conversely, assume that K has a $C_{q^r} \times C_{q^r}$-extension L/K. Consider the maximal unramified extension K^{ur}/K inside L. By assumption (iii), $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ must be cyclic and a quotient of $C_{q^r} \times C_{q^r}$. Therefore, K admits a C_{q^r}-extension E/K linearly disjoint from K^{ur}/K. Then, the extension E/K is totally ramified, and tamely so by assumption (i).

Let w be the unique prolongation of v to E. By Hensel's Lemma and (i), it suffices to show that $\zeta_{q^r} \in Ew = Kv$. We can see that this follows from the Second Exact Sequence (3.1.4):

$$C_{q^r} \cong \mathrm{Gal}(E/K) = I_w(E/K) \cong \mathrm{Hom}(wE/vK, \mu_{Ew}).$$

Indeed, $\mathrm{Hom}(wE/vK, \mu_{Ew}) \cong C_{q^r}$ if and only if $wE/vK \cong C_{q^r}$ and $\zeta_{q^r} \in \mu_{Ew} = \mu_{Kv}$. □

Remark 3.2.2. Observe that if a valued field (K, v) satisfies (i)–(iii) in the above lemma, and L/K is a finite abelian extension with unique prolongation w of v, then the valued field (L, w) also satisfies (i)–(iii).

We will further consider infinite cyclotomic extensions of K, to which the following subtle observation applies.

Lemma 3.2.3. *Let F be a field with* $\operatorname{char} F \neq q$. *Then $F(\zeta_{q^\infty}) = F(\zeta_q)$, $F(\zeta_{2^\infty}) = F(\zeta_4)$ (if $q = 2$)[2], or $\operatorname{Gal}(F(\zeta_{q^\infty})/F) \cong \mathbb{Z}_q \times C$, where C is cyclic of order dividing $q-1$ for $q \neq 2$ and cyclic of order dividing 2 for $q = 2$.*

Proof. Consider $F_n \coloneqq F(\zeta_{q^n})$ for $n \in \mathbb{N}$, which form a tower of field extensions. Assume $F(\zeta_q) \neq F(\zeta_{q^\infty})$, which means that there exists an $n \geq 2$ such that $\zeta_{q^n} \notin F_{n-1}$. If $\zeta_{q^{n+1}} \in F_n$, then

$$(N_{F_n/F_{n-1}}(\zeta_{q^{n+1}}))^q = N_{F_n/F_{n-1}}(\zeta_{q^n}) = (-1)^{q-1}\zeta_{q^{n-1}} \in F_{n-1}.$$

For $q \neq 2$, $(-1)^{q-1} = 1$, so this shows that $\zeta_{q^{n-1}}$ has a q-th root in F_{n-1}, hence $\zeta_{q^n} \in F_{n-1}$, a contradiction. Therefore, $\zeta_{q^{n+1}}$ cannot lie in F_n, and by induction, the F_n form an infinite degree tower. The claim now follows by taking the inverse limit of $\operatorname{Gal}(F_n/F)$, given that $F(\zeta_q)/F$ is cyclic of order dividing $q-1$.

If $q = 2$, either $F(\zeta_4) = F(\zeta_{2^\infty})$ or $n > 2$. In the latter case, $\zeta_4 = \sqrt{-1} \in F_2$, so we get

$$(\zeta_4 N_{F_n/F_{n-1}}(\zeta_{2^{n+1}}))^2 = (-1) \cdot N_{F_n/F_{n-1}}(\zeta_{2^n}) = \zeta_{2^{n-1}} \in F_{n-1}.$$

We now finish the proof analogously to the case where $q \neq 2$, noting that $F(\zeta_4)/F$ is either trivial or a C_2-extension. □

3.2.1.2 Counting in $\mathbb{Q}_p$

The following lemma counts the q-rank of a p-adic field F (the $\mathbb{F}_q$-dimension of $F^\times/F^{\times q}$). As such, it generalises Lemma 2.1.12 and our calculation in Lemma 2.2.8 to more general p-adic fields.

Lemma 3.2.4 (Degree Lemma)**.** *Let $F/\mathbb{Q}_p$ be a finite extension of degree n. Let q be a prime such that $\zeta_q \in F$. Then*

$$\dim_{\mathbb{F}_q}(F^\times/F^{\times q}) = \begin{cases} 2 & \text{if } q \neq p \\ n+2 & \text{if } q = p. \end{cases}$$

The result is most commonly proved via a direct sum decomposition based on the p-adic logarithm, which turns $F^\times$ into an additive structure, see [Neu99, Chapter II, (5.8)]. Here, we present an alternative proof, which has the added benefit of working in a much larger class of valued fields that includes p-adically closed fields.

[2] These exceptional cases do occur in general (even if not for the field K that we considered so far): $\mathbb{Q}(\{\Re(e^{2i\pi/q^n}), \Im(e^{2i\pi/q^n})\}_{n\geq 1}) \subseteq \mathbb{R}$ contains only ζ_2 — after adjoining ζ_q, it will have all q^n-th roots of unity.

Proof. We first consider the case $q \neq p$. Let $f \coloneqq f(F/\mathbb{Q}_p)$ be the inertia degree. Note that any element in $U^{(1)} \coloneqq U_F^{(1)}$ has a q-th root by Hensel's Lemma. Using the direct sum decomposition for $F^\times$ (Fact 2.1.4), we obtain

$$F^\times/F^{\times q} \cong \mathbb{Z}/q\mathbb{Z} \times \mu'_F/(\mu'_F)^q.$$

From $\zeta_q \in \mu'_F = \mu_{p^f-1}$ (Lemma 2.1.1), we conclude that $q \mid (p^f - 1)$, so the second factor is isomorphic to $\mathbb{Z}/q\mathbb{Z}$ and the claim follows.

Now consider the case $q = p$. Then $\mathbb{Q}_p(\zeta_p) \subseteq F$, and let $e \coloneqq e(F/\mathbb{Q}_p(\zeta_p))$ be the ramification index relative to $\mathbb{Q}_p(\zeta_p)$. Hence,

$$n = e(F/\mathbb{Q}_p)f(F/\mathbb{Q}_p) = e(p-1)f. \tag{3.2.1}$$

Reasoning as in the first case, we obtain

$$F^\times/F^{\times p} \cong \mathbb{Z}/p\mathbb{Z} \times U^{(1)}/\big(U^{(1)}\big)^p,$$

so it suffices to show that $U^{(1)}/\big(U^{(1)}\big)^p$ has $\mathbb{F}_p$-dimension $n+1$. To calculate the dimension, we work modulo $U^{(ep+1)}$ using that $U^{(ep+1)} \subseteq \big(U^{(1)}\big)^p$ by Lemma 2.1.9. First of all, write

$$U^{(1)}/\big(U^{(1)}\big)^p \cong \frac{U^{(1)}/U^{(ep+1)}}{(U^{(1)})^p/U^{(ep+1)}}$$

using Lemma 2.1.9. By Corollary 2.1.7 and (3.2.1), we have

$$\big|U^{(1)}/U^{(ep+1)}\big| = |Fv|^{ep} = p^{fep} = p^{n+\frac{n}{p-1}}.$$

Hence, it remains to prove

$$\big|(U^{(1)})^p/U^{(ep+1)}\big| = p^{\frac{n}{p-1}-1}. \tag{3.2.2}$$

Claim. The p-th power map $x \longmapsto x^p$ induces a well-defined epimorphism

$$\Phi : U^{(1)}/U^{(e+1)} \twoheadrightarrow (U^{(1)})^p/U^{(ep+1)},$$

with image of cardinality $p^{n/(p-1)-1}$.

Proof of Claim. Let π be a uniformiser in F. Using $v(p) = v(\pi^{e(p-1)})$, observe that

$$(1 + b\pi^{e+1})^p \equiv 1 \pmod{\pi^{ep+1}} \quad \text{for all } b \in \mathcal{O}_F,$$

which implies $(U^{(e+1)})^p \subseteq U^{(ep+1)}$. Thus, Φ is well-defined and surjective. As

$$\big|U^{(1)}/U^{(e+1)}\big| = p^{fe} = p^{\frac{n}{p-1}},$$

it suffices to show that Φ has kernel of order p. To this end, let $1 + a_1\pi + \cdots + a_e\pi^e$ represent an element in $U^{(1)}/U^{(e+1)}$, where each $a_i \in \mathcal{O}_F$ comes from a set of representatives for Fv (Corollary 2.1.7). Without loss of generality, assume that $a_i = 0$ represents $0 \in Fv$. Consider

$$(1 + a_1\pi + \cdots + a_e\pi^e)^p \equiv 1 \pmod{U^{(ep+1)}},$$

or equivalently (Remark 2.1.6),

$$(1 + a_1\pi + \cdots + a_e\pi^e)^p - 1 \equiv 0 \pmod{\pi^{ep+1}}. \tag{3.2.3}$$

We claim that $a_i = 0$ for all $i \leq e-1$. If not, let i be minimal such that $a_i \neq 0$. Expanding the expression in (3.2.3), we see that for $i < e$,

$$v(a_i\pi^{pi}) = pi = i(p-1) + i < e(p-1) + i = v(pa_i\pi^i).$$

It follows that $a_i^p\pi^{pi}$ is the unique term of minimal value, a contradiction. Therefore, (3.2.3) simplifies to

$$(1 + a_e\pi^e)^p - 1 \equiv a_e^p\pi^{ep} + pa_e\pi^e \equiv 0 \pmod{\pi^{ep+1}},$$

which is equivalent to $\overline{a_e} \in Fv$ being a solution of

$$X^p + \overline{\frac{p}{\pi^{e(p-1)}}}X = 0. \tag{3.2.4}$$

Using Lemma 2.1.8, one easily checks that

$$\{0\} \cup \left\{ \overline{\frac{\zeta_p - 1}{\pi^e}\zeta_{p-1}^i} : i = 0, \ldots, p-2 \right\}$$

is the solution set for (3.2.4). This proves that Φ is p-to-1, implying (3.2.2). □

Remark 3.2.5. As the proof of the Main Theorem will require a somewhat stronger version of the Degree Lemma for $q = p$, we examine which properties of $\mathbb{Q}_p$ were used in the arguments leading up to Lemma 3.2.4. We find that the following assumptions are needed: (K, v) is a henselian valued field of characteristic 0 satisfying

(i) $\zeta_p \in K$;

(ii) the value group has minimal positive element 1 and $v(p) = e(p-1) < \infty$;

(iii) the residue field is $\mathbb{F}_{p^f}$ with $f < \infty$.

If (K, v) satisfies these conditions, then the following general degree formula holds:

$$\dim_{\mathbb{F}_p}(K^\times/K^{\times p}) = e(p-1)f + 2$$

Let us briefly note that an alternative proof of this generalisation could proceed by reduction to the p-adic case: in the Standard Decomposition of v_K, the (0,0)-place does not contribute to the dimension of $K^\times/K^{\times p}$, and both the core field Kv_0 and its completion (which is a p-adic field) have the same p-rank by Hensel's Lemma.

Corollary 3.2.6. *$\mathbb{Q}_p$ has only finitely many extensions of degree n for any positive integer n.*

Proof (Kummer theory). It suffices to show that there are finitely many Galois extensions of degree n: any finite extension of degree n has a splitting field of degree at most $n!$ and any finite Galois extension has finitely many subfields by the Galois correspondence. We are done if we prove that all Galois extensions of degree n are contained in a single finite extension K.

Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be a prime decomposition of n such that $p_r = p$. Define an iteration of Kummer extensions

$$K_0 \coloneqq \mathbb{Q}_p(\zeta_{p^n-1}, \zeta_n)$$
$$K_{e_1+\cdots+e_{i-1}+l+1} \coloneqq K_{e_1+\cdots+e_{i-1}+l}\big((K^\times_{e_1+\cdots+e_{i-1}+l})^{1/p_i}\big)$$

for all $i = 1, \ldots, r$ and $l = 0, \ldots, e_i - 1$; let $K \coloneqq K_{e_1+\cdots+e_r}$ be the last field in the construction. By the Degree Lemma 3.2.4, K is a finite extension of $\mathbb{Q}_p$. We claim that any Galois extension $F/\mathbb{Q}_p$ of degree n lies in K. To prove the claim, consider the tower of field extensions

$$\mathbb{Q}_p = F^D \subseteq F^I \subseteq F^R \subseteq F$$

that corresponds to the ramification filtration. Note that $F^I/\mathbb{Q}_p$ is generated by ζ_{p^f-1}, where $f \mid n$ is the degree of inertia of $F/\mathbb{Q}_p$. Thus, $F^I \subseteq K_0$. Furthermore, F^R/F^I is abelian and of order dividing $p_1^{e_1} \cdots p_{r-1}^{e_{r-1}}$ (cf. Fact 3.1.23); the same is true for $F^R K_0/K_0$. By Kummer theory and the Galois correspondence, we may construct a tower

$$K_0 = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = F^R K_0,$$

such that each L_{i+1}/L_i is a Kummer extension — of which the first $s_1 \leq e_1$ are of degree p_1, followed by $s_2 \leq e_2$ Kummer extensions of degree p_2, and so on. This proves

$$F^R K_0 \subseteq K_{e_1+\cdots+e_{r-1}}.$$

Finally, note that F/F^R is a p-power extension, with the same being true for FK_0/F^RK_0. By considering a composition series for its Galois group, we may again write this extension as a tower of Kummer p-extensions (again using that the maximal proper subgroups of finite p-groups provide normal subgroups of index p, [Rot95, Theorem 4.6(ii)]). Therefore, $F \subseteq K$ as claimed. □

We say that $G_{\mathbb{Q}_p}$ is *small*, i.e., has finitely many open subgroups of index n, for any fixed n.

Remark 3.2.7. The alternative (standard) approach is to use continuity of roots (Fact 3.1.16), Krasner's Lemma 3.1.35, and the compactness of the space $\mathbb{Z}_p^n$ of integral polynomials of degree n to deduce that there are finitely many totally ramified extensions of degree n. The general statement then follows by considering inertia subfields.

We will later need the following converse statement of Lemma 3.2.4 about fields that have small absolute Galois group.

Lemma 3.2.8. *Let K be a field and q be any prime. If K has small absolute Galois group and* $\operatorname{char} K \neq q$, *then* $\dim_{\mathbb{F}_q}(K^\times/K^{\times q}) < \infty$.

Proof. Note that $L \coloneqq K(\zeta_q)$ is a Galois extension of K of degree $d \mid (q-1)$. The norm map induces an $\mathbb{F}_q$-vector space homomorphism

$$\overline{N_{L/K}} : L^\times/L^{\times q} \longrightarrow K^\times/K^{\times q}$$

that is surjective, since for any $x \in K^\times$, we have

$$\langle N_{L/K}(x)\rangle = \langle x^d\rangle \equiv \langle x\rangle \pmod{K^{\times q}}.$$

Hence,

$$\dim_{\mathbb{F}_q}(K^\times/K^{\times q}) \leq \dim_{\mathbb{F}_q}(L^\times/L^{\times q}) < \infty,$$

by Kummer theory, using the fact that L admits only finitely many C_q-extensions since G_K is small. □

We also prove the following result, which generalises Lemma 2.1.12 in a structural way and complements the pure counting results considered in this section.

Lemma 3.2.9. *Let $F/\mathbb{Q}_p(\zeta_p)$ be a finite extension with uniformiser π in F. Write e for the ramification index and f for the degree of inertia of this extension. Assume further that $\{b_1, \dots, b_f\} \subseteq \mathcal{O}_F$ represent an $\mathbb{F}_p$-basis of Fv. Then*

$$\{\pi\} \cup \{1 + b_i\pi^k : 1 \leq i \leq f,\ 1 \leq k \leq ep\}$$

represents a generating set of $F^\times/F^{\times p}$. Moreover, for $F = \mathbb{Q}_p(\zeta_p)$,

$$\{\pi\} \cup \{1 + b_1\pi^k : 1 \leq k \leq p\}$$

represents an $\mathbb{F}_p$-basis of $F^\times/F^{\times p}$.

Proof. By the direct sum decomposition of Fact 2.1.4, we obtain an isomorphism

$$F^\times/F^{\times p} \cong \pi^{\mathbb{Z}}/\pi^{p\mathbb{Z}} \times U_F^{(1)}/\left(U_F^{(1)}\right)^p,$$

where the first factor is generated by $\overline{\pi}$. We now focus on the second factor.

The idea is again to use Lemma 2.1.9 to compare sets modulo $U_F^{(ep+1)} \subseteq \left(U_F^{(1)}\right)^p$. It then suffices to show that the elements $1 + b_i\pi^k$ generate $U_F^{(1)}$ modulo $U_F^{(ep+1)}$.

Claim. $\langle 1 + b_i\pi^k : 1 \leq i \leq f, l \leq k \leq ep\rangle \equiv U_F^{(l)} \pmod{U_F^{(ep+1)}}$ *for any* $l = 1, \dots, ep+1$.

Proof of Claim. Via backward induction from $l = ep+1$ to $l = 1$. The case $l = ep+1$ is trivial. By Fact 2.1.5,

$$\langle 1 + b_1\pi^l, \dots, 1 + b_f\pi^l\rangle U_F^{(l+1)} = U_F^{(l)},$$

for any $l = 1, \dots, ep+1$. This identity proves the inductive step $l+1 \to l$. ◇

For $l = 1$, we recover our original claim.

Consider now the special case $F = \mathbb{Q}_p(\zeta_p)$. Recall that by Lemma 2.1.11,

$$U_F^{(1)}/\left(U_F^{(1)}\right)^p = U_F^{(1)}/U_F^{(p+1)}.$$

By the same proof, $\{1 + b_1\pi^k : 1 \leq k \leq p\}$ is a generating set of cardinality p for $U_F^{(1)}/U_F^{(p+1)}$. Hence, it must be a basis, since

$$\left|U_F^{(1)}/U_F^{(p+1)}\right| = |Fv|^p = p^p.$$ □

3.2.2 Fields with finite p-rank

The finiteness of $K^\times/K^{\times p}$ is a natural condition in the context of Kummer theory, and, as we have shown above, holds for $\mathbb{Q}_p$. In [Pop88, Korollar 2.7], Pop discovered that this simple condition implies strong structural properties whenever K comes with a valuation. See also [Efr06, 12.5], [GKS, Lemma 3.20].

Lemma 3.2.10 (Pop's Lemma)**.** *Let (K, v) be a valued field of mixed characteristic $(0, p)$. Assume that $K^\times/K^{\times p}$ is finite. Then:*

(i) Kv is perfect.

(ii) If v is of rank 1, then vK is either discrete or p-divisible.

(iii) If vK is discrete, then Kv is finite.

Proof. We have two identities,

$$\mathcal{O}_v^{\times p} = \mathcal{O}_v^\times \cap K^{\times p}$$
$$(1+\mathcal{M}_v)^p = \mathcal{O}_v^{\times p} \cap (1+\mathcal{M}_v),$$

where the first one is immediate; for the second one, note that $\operatorname{char} Kv = p$ implies that for any $x \in \mathcal{O}_v^\times$,

$$x^p \equiv 1 \pmod{\mathcal{M}_v} \iff \overline{x}^p = 1 \implies \overline{x} = 1 \iff x \equiv 1 \pmod{\mathcal{M}_v}. \tag{3.2.5}$$

The two identities above express the exactness of the following two sequences:

$$1 \longrightarrow \mathcal{O}_v^{\times p} \longrightarrow K^{\times p} \longrightarrow pvK \longrightarrow 1$$
$$1 \longrightarrow (1+\mathcal{M}_v)^p \longrightarrow \mathcal{O}_v^{\times p} \longrightarrow Kv^{\times p} \longrightarrow 1$$

Consequently, the two standard short exact sequences of (3.1.1) induce two additional short exact sequences by the nine lemma:

$$1 \longrightarrow \mathcal{O}_v^\times/\mathcal{O}_v^{\times p} \longrightarrow K^\times/K^{\times p} \longrightarrow vK/pvK \longrightarrow 1$$
$$1 \longrightarrow (1+\mathcal{M}_v)/(1+\mathcal{M}_v)^p \longrightarrow \mathcal{O}_v^\times/\mathcal{O}_v^{\times p} \longrightarrow Kv^\times/Kv^{\times p} \longrightarrow 1$$

The exactness of these sequences implies that all quantities in

$$|Kv^\times/Kv^{\times p}| \cdot |(1+\mathcal{M}_v)/(1+\mathcal{M}_v)^p| = |\mathcal{O}_v^\times/\mathcal{O}_v^{\times p}| \leq |K^\times/K^{\times p}|$$

are finite.

To prove (i), it suffices to consider the case that Kv is infinite. In that case, $(Kv)^p$ must be infinite as well. Now fix any $x \in Kv^\times$. Observe that $\{x + a^p : a \in Kv^\times\}$ is an infinite set, while $K^\times/K^{\times p}$ is finite. By the pigeonhole principle, there are $a, b, c, d \in Kv^\times$, $a \neq c$, $b \neq d$, such that $(x + a^p)b^p = (x + c^p)d^p$. Solving for x, we obtain

$$x = \frac{(cd - ab)^p}{(b - d)^p} \in Kv^{\times p}.$$

Hence, Kv is perfect.

For (ii), recall that we know $(1 + \mathcal{M}_v)/(1 + \mathcal{M}_v)^p$ is finite. We let $\{1 + a_i\}_{1 \leq i \leq n} \subseteq 1 + \mathcal{M}_v$ be a complete set of representatives for $(1 + \mathcal{M}_v)/(1 + \mathcal{M}_v)^p$ and define

$$\delta \coloneqq \min\{v(a_1), \ldots, v(a_n), v(p)\} > 0.$$

If δ is minimal positive in vK, then $vK = \delta\mathbb{Z}$ is discrete. If not, we may find an element $x \in \mathcal{M}_v$ with $v(x) < \delta$ and write

$$1 + x = (1 + a_i)(1 + y)^p$$

for some $i \in \{1, \ldots, n\}$ and $y \in \mathcal{M}_v$. Therefore,

$$v(x) = v\big(a_i(1 + y)^p + [(1 + y)^p - 1 - y^p] + y^p\big) \geq \min\{v(a_i), v(p), v(y^p)\}. \quad (3.2.6)$$

By the choice of x and the definition of δ, $v(y^p) < \delta$; in particular, we attain equality $v(x) = v(y^p) \in pvK$. Hence, the interval $(0, \delta) \subset vK$ is p-divisible and non-empty. Since vK is of rank 1, the interval generates vK, so vK must be p-divisible itself.

Finally, for (iii), we assume K has a uniformiser. It is easy to see that $(1 + \mathcal{M}_v)^p \subseteq 1 + \mathcal{M}_v^2$. In particular,

$$|(1 + \mathcal{M}_v)/(1 + \mathcal{M}_v^2)| \leq |(1 + \mathcal{M}_v)/(1 + \mathcal{M}_v)^p| < \infty.$$

Adapting Fact 2.1.5, we see that the left-hand side equals $|Kv|$, so Kv must be finite. □

3.2.3 Distinguishing characteristics of fields

In this section, we answer the question: *how does $G_{\mathbb{Q}_p}$ know that $\mathbb{Q}_p$ has characteristic $\neq p$?*

Galois cohomology provides an immediate answer if we consider cohomological p-dimensions:

$$\operatorname{cd}_p G_{\mathbb{Q}_p} = 2, \text{ while } \operatorname{cd}_p G_K \leq 1$$

for any field K of characteristic p, see [Ser97, II. §4, II. §2.2]. Since our goal is to give a self-contained answer, we present an elementary criterion—motivated by Galois cohomology—for distinguishing fields of characteristic zero from those of positive characteristic. This will make explicit the elementary ideas concealed by the cohomological formalism. The underlying idea finds its origin in Artin-Schreier's work [AS27b], where it is used to show that fields K with $G_K \cong C_2$ are of characteristic 0.

Idea 3.2.11. For a field K, consider the property of whether every C_p-extension of K embeds into a C_{p^2}-extension of K. We will show that this is true in general if K has characteristic p, and false for some p-adic field K.

Cyclic Galois extensions are well-understood by Hilbert 90, Kummer theory, and Artin-Schreier theory (in positive characteristic). For convenience, we state these classical results.

Theorem 3.2.12 (Hilbert 90)**.** *Let L/K be a finite cyclic Galois extension and σ a generator of $\mathrm{Gal}(L/K)$. Then for any $a \in L$:*

$$N_{L/K}(a) = 1 \iff \exists b \in L^\times \ a = \sigma(b) \cdot b^{-1} \quad (\text{“Multiplicative H90”})$$
$$\mathrm{Tr}_{L/K}(a) = 0 \iff \exists b \in L \quad a = \sigma(b) - b \quad (\text{“Additive H90”})$$

One can deduce the following characterisations of C_p-extensions, the first of which restates Theorem 2.2.3 from Chapter 2.

Theorem 3.2.13 (Kummer theory)**.** *Let K be a field with $\mathrm{char}\, K \neq p$ and $\zeta_p \in K$. Then there exists a bijection*

$$\{\text{one-dim. subspaces } \langle c\rangle K^{\times p} \leq K^\times/K^{\times p}\} \longleftrightarrow \{L/K \text{ Galois extensions of deg. } p\}$$
$$\langle c\rangle K^{\times p} \longmapsto K(\sqrt[p]{c})$$
$$(K^\times \cap L^{\times p})/K^{\times p} \longmapsto L.$$

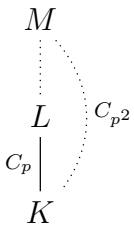
Theorem 3.2.14 (Artin-Schreier theory)**.** *Let K be a field of positive characteristic p. Then there exists a bijection*

$$\{\text{one-dim. subspaces } \langle c\rangle + \wp(K) \leq K/\wp(K)\} \longleftrightarrow \{L/K \text{ Galois ext. of deg. } p\}$$
$$\langle c\rangle + \wp(K) \longmapsto K(\alpha),$$

where $\wp(X) = X^p - X$ is the Artin-Schreier map and α is a root of the Artin-Schreier polynomial $\wp(X) - c$.

The next three lemmas realise Idea 3.2.11.

Lemma 3.2.15 ([AS27b, Satz 3])**.** *Let K be a field of positive characteristic p. Then any C_p-extension L/K is contained in a C_{p^2}-extension M/K.*



Proof. By Artin-Schreier theory, L is generated by a root x of an Artin-Schreier polynomial $X^p - X - a$. Dividing by $(-x^p a)$, we obtain

$$-a^{-1} + a^{-1}(x^{-1})^{p-1} + (x^{-1})^p = 0,$$

which implies $\mathrm{Tr}_{L/K}(x^{-1}) = -a^{-1}$. We also have $-x^{p-1} = -1 - ax^{-1}$, yielding

$$\mathrm{Tr}(-x^{p-1}) = \mathrm{Tr}(-1 - ax^{-1}) = -\mathrm{Tr}(1) - a\,\mathrm{Tr}(x^{-1}) = -p + 1 = 1. \tag{3.2.7}$$

Define $b \coloneqq -x^{p-1}$. In characteristic p, $\mathrm{Tr}(b^p) = \mathrm{Tr}(b)^p$ holds, and thus

$$\mathrm{Tr}(b^p - b) = \mathrm{Tr}(b^p) - \mathrm{Tr}(b) = \mathrm{Tr}(b)^p - \mathrm{Tr}(b) = 1 - 1 = 0.$$

Hence, we can apply (additive) Hilbert 90 to find $c \in L$ such that

$$b^p - b = \sigma(c) - c \tag{3.2.8}$$

for some generator σ of $\mathrm{Gal}(L/K)$. We claim that the Artin-Schreier extension $L(y)/L$, where y is a root of $X^p - X - c$, is the desired C_{p^2}-extension of K. Indeed, $M \coloneqq L(y)$ over K has degree p^2 and is Galois by (3.2.8). So we are left to prove $\mathrm{Gal}(M/K) \ncong C_p \times C_p$. Assume the contrary. By the Galois correspondence, there exists a C_p-extension $L' \neq L$ over K contained in M. By Artin-Schreier theory, $L' = K(z)$ where $z^p - z - d = 0$ for some $d \in K$. By construction, we have $L(z) = M$. Again, Artin-Schreier theory tells us that c and d generate the same $\mathbb{F}_p$-subspace in $L/\wp(L)$, so $c = id + e^p - e$ for some $i \in \{1, \dots, p-1\}$ and $e \in L$. Therefore,

$$b^p - b = \sigma(c) - c = (\sigma(id) + \sigma(e)^p - \sigma(e)) - (id + e^p - e) = (\sigma(e) - e)^p - (\sigma(e) - e).$$

In particular, $\sigma(e) - e = b + j$ for some $j \in \{0, \dots, p-1\}$. However,

$$\mathrm{Tr}(\sigma(e) - e) = 0 \neq 1 = 1 + pj = \mathrm{Tr}(b) + \mathrm{Tr}(j) = \mathrm{Tr}(b + j),$$

by (3.2.7), which yields a contradiction. □

As indicated by Idea 3.2.11, there is a p-adic field that admits a C_p-extension that does not embed into any C_{p^2}-extension. We will give an explicit example in Lemma 3.2.17. To facilitate the construction, we will first give an equivalent criterion in the presence of a primitive p-th root of unity.

Lemma 3.2.16. *Assume K is a field with $\operatorname{char} K \neq p$ and $\zeta_p \in K$. Let L/K be a C_p-extension. Then L can be embedded into a C_{p^2}-extension M/K if and only if $\zeta_p \in \operatorname{im} N_{L/K}$.*

Proof. $\Rightarrow$. Assume that L can be embedded into a C_{p^2}-extension M/K. Then M/L is Galois with $\operatorname{Gal}(M/L) \cong C_p$. Therefore, $M = L(\sqrt[p]{d})$ for some $d \in L^\times \setminus L^{\times p}$ by Kummer theory. Let σ be a generator of $\operatorname{Gal}(L/K)$. As $L(\sqrt[p]{d}) = L(\sqrt[p]{\sigma(d)})$, Kummer theory implies $\sigma(d) \in \langle d \rangle L^{\times p}$. Replacing σ by an appropriate power if necessary, we may assume $\sigma(d) \in dL^{\times p}$ without loss of generality. Let $e \in L^\times$ be such that $\sigma(d)d^{-1} = e^p$. Then

$$(N_{L/K}(e))^p = N_{L/K}(e^p) = N_{L/K}\left(\frac{\sigma(d)}{d}\right) = \frac{\sigma(d)}{d}\frac{\sigma(\sigma(d))}{\sigma(d)} \cdots \frac{\overbrace{\sigma^p(d)}^{=d}}{\sigma^{p-1}(d)} = 1.$$

It suffices to show that $N_{L/K}(e) \neq 1$. If instead $N_{L/K}(e) = 1$, then we could find $f \in L^\times$ such that $e = \sigma(f)f^{-1}$ by Hilbert 90. Thus,

$$\sigma(d)d^{-1} = e^p = \left(\sigma(f)f^{-1}\right)^p \Longrightarrow \sigma\left(df^{-p}\right) = df^{-p},$$

which implies $df^{-p} \in K$. But then $K(\sqrt[p]{df^{-p}}) = K(\sqrt[p]{d}/f) \neq L$ would be yet another C_p-extension of K contained in M, which is impossible by the Galois correspondence for M/K.

$\Leftarrow$. The line of reasoning is very similar, but with inverted order. Assume that $N_{L/K}(e) = \zeta_p$. Then $N_{L/K}(e^p) = (N_{L/K}(e))^p = 1$, so there exists some $d \in L^\times$ such that $\sigma(d)d^{-1} = e^p$. We claim that $d \notin L^{\times p}$. For otherwise, we could write $d = f^p$, so that

$$e^p = \sigma(d)d^{-1} = \left(\sigma(f)f^{-1}\right)^p \Longrightarrow e = \sigma(f)f^{-1}\zeta_p^i$$

for some $i \in \{0, \ldots, p-1\}$, which implies (similar to above)

$$\zeta_p = N_{L/K}(e) = N_{L/K}\left(\sigma(f)f^{-1}\right) N_{L/K}(\zeta_p^i) = 1,$$

a contradiction. Thus, $M \coloneqq L(\sqrt[p]{d})$ is indeed a C_p-extension of L. Moreover, using $\sigma(d) = de^p$, we see that $L(\sqrt[p]{d}) = L(\sqrt[p]{\sigma(d)})$, so M/K is a Galois extension of degree p^2 (as M contains all conjugates of $\sqrt[p]{d}$ over K). Note that $\operatorname{Gal}(M/K)$ is

either isomorphic to C_{p^2} or $C_p \times C_p$. We are left to exclude the latter case. So assume for a contradiction that $\mathrm{Gal}(M/K) \cong C_p \times C_p$. On account of the Galois correspondence, there exists a C_p-extension $L' \neq L$ of K inside M. By Kummer theory, $L' = K(\sqrt[p]{c})$ for some $c \in K$ and $L(\sqrt[p]{c}) = M$. Yet again, this means that c and d generate the same subgroup in $L^\times/L^{\times p}$. Thus, $d = c^i f^p$ with $i \in \{1, \dots, p-1\}$ and $f \in L^\times$. But then

$$e^p = \sigma(d)d^{-1} = \frac{\sigma(c^i f^p)}{c^i f^p} = \left(\sigma(f)f^{-1}\right)^p,$$

contradicting our earlier observation that this equality cannot hold. □

Lemma 3.2.17. *Let $p \neq 2$ be a prime. Consider $K = \mathbb{Q}_p(\zeta_p)$ with uniformiser $\pi = \zeta_p - 1$. Then, $L = K(\sqrt[p]{(1-p)\pi})$ is a C_p-extension of K that is not contained in any C_{p^2}-extension.*
Moreover, for $p = 2$, $L = \mathbb{Q}_2(i)$ is a quadratic extension of $\mathbb{Q}_2$ not contained in any C_4-extension.

Proof. The claim for $p = 2$ is precisely the content of Lemma 2.2.6, so it remains to consider the case $p \neq 2$. We write $c \coloneqq 1 - p \in \mathcal{O}_K^\times$ and let $\Pi \coloneqq \sqrt[p]{c\pi}$ be a root of $X^p - c\pi$. As an Eisenstein polynomial, $X^p - c\pi$ is irreducible, so L/K is a C_p-extension and we may choose Π as a natural uniformiser in L. By Lemma 3.2.16, we only need to verify that $\zeta_p \notin \operatorname{im} N_{L/K}$. Since $K^{\times p} \subseteq \operatorname{im} N_{L/K}$, it suffices to show that the induced map

$$\overline{N_{L/K}} : L^\times/L^{\times p} \longrightarrow K^\times/K^{\times p}$$

does not contain $\zeta_p K^{\times p}$ in its image. We will determine the image by direct calculation.

From Lemma 3.2.9, we know that

$$R = \left\{\Pi, 1 + \Pi, 1 + \Pi^2, \dots, 1 + \Pi^{p^2}\right\}$$

is a set of representatives generating $L^\times/L^{\times p}$. Consider an element $x_k = 1 + \Pi^k$ for $p \nmid k$. Note that x_k has minimal polynomial $(X-1)^p - (c\pi)^k$, and thus

$$N_{L/K}(x_k) = 1 + (c\pi)^k.$$

For $k \geq p + 1$, the norms $N_{L/K}(x_k) = 1 + (c\pi)^k$ already lie in $K^{\times p}$ by Lemma 2.1.9. Therefore, $\operatorname{im} \overline{N_{L/K}}$ is generated by the set of representatives

$$S = \{c\pi, 1 + c\pi, \dots, 1 + (c\pi)^{p-1}\}.$$

Hence, $\operatorname{im}\overline{N_{L/K}} \subseteq K^\times/K^{\times p}$ is a subgroup of index p (by the second part of Lemma 3.2.9).

Assume towards a contradiction that $\zeta_p = 1 + \pi \in \operatorname{im} N_{L/K}$. By Lemma 2.1.8,

$$1 + c\pi = 1 + \pi - p\pi \equiv 1 + \pi + \pi^p \equiv (1 + \pi)(1 + c^p\pi^p) \pmod{\pi^{p+1}}$$

and hence, by Remark 2.1.6,

$$\frac{1 + c\pi}{1 + \pi} \equiv 1 + (c\pi)^p \pmod{U_K^{(p+1)}}.$$

Note that, by Lemma 2.1.9, $U_K^{(p+1)} \subseteq K^{\times p}$. But this implies that $\overline{1 + (c\pi)^p}$ lies in the image of $\overline{N_{L/K}}$. This is impossible, since $S \cup \{1 + (c\pi)^p\}$ represents a basis of $K^\times/K^{\times p}$. □

3.2.4 Transfer of Galois groups between different characteristics

In the previous section, we established a group-theoretic criterion ensuring that certain Galois groups can occur only in characteristic 0. The complementary phenomenon arises when a group appears both in characteristic 0 and in positive characteristic p. It is not difficult to show that for every group that occurs as the absolute Galois group of a field of characteristic $p > 0$, one can naturally construct a field of characteristic 0 with the same absolute Galois group. To gain intuition for this construction—which relies on the Gauss valuation and complements of the inertia group—we refer the reader to the proof of Lemma 4.2.10 below.

The more interesting direction, therefore, is usually the reverse: given a field of characteristic 0, can one construct, in a natural manner, a field of characteristic p with the same absolute Galois group. Whenever such a procedure exists, we refer to it as *transfer*, as it provides a systematic way of transporting arithmetic information between fields of different characteristics. In recent years, transfer methods have become increasingly powerful and have appeared in several areas of mathematics.

A particularly important class of fields for which such transfers exist is provided by *perfectoid fields* of characteristic 0. For these fields, the *tilting construction* produces a natural field of characteristic p whose absolute Galois group is isomorphic to that of the original field. This phenomenon was first established in a special case by Fontaine and Wintenberger and was later generalised to perfectoid fields by Kedlaya–Liu and Scholze [Sch12, Theorem 1.3].

Independently, Koenigsmann [Koe04] introduced another example of such a construction. His approach can now be recognised as an early instance of the *saturation–decomposition method*, whose origins trace back to the work of Kochen [Koc75]. This method has since been extended by Jahnke and Kartas [JK25] to encompass perfectoid fields as well.

More recently, Gitin has developed a systematic framework for transfer methods, clarifying the connections between the approaches mentioned above. This framework is presented in [GKS, Section 4], to which we refer the reader for a detailed account of the various constructions. In the following, we shall only present aspects of Gitin's work that are directly needed for the proof of Theorem 3.0.1. In fact, for our purposes we require only the following result, which finds its origin in Koenigsmann's work [Koe04, Theorem 3.3] and to which we shall henceforth refer as the *Transfer Lemma*:

Lemma 3.2.18 (Transfer Lemma)**.** *Let (K, v) be a henselian valued field of mixed characteristic $(0, p)$. Assume that*

(i) G_K *is small,*

(ii) $vK = \mathrm{Conv}(v(p))$*, and*

(iii) vK *is p-divisible.*

Then there exists a field F of positive characteristic p such that $G_K \cong G_F$.

We now outline two proofs of the Transfer Lemma. The first follows Koenigsmann's original argument, which is based on the saturation–decomposition method, while the second is due to Gitin and relies on the tilting construction. Depending on the reader's mathematical background and perspective, one of these approaches may appear more natural than the other. A conceptual reconciliation of the two methods, as mentioned above, is developed in detail in [GKS, Section 4].

The Saturation-Decomposition Method Following the exposition in [GKS, Section 4], we summarise the saturation-decomposition method by the following slogan:

Slogan. *Given a valued field (K, v), study its structure in two steps:*

(i) ***Saturate*** *by passing to an extension with strong closure properties whilst preserving all elementary properties of the valued field (i.e., pass to a saturated elementary extension).*

(ii) ***Decompose*** *the saturated extension into places that can each be analysed individually.*

With this slogan at hand, we now give a sketch of Koenigsmann's original proof of the Transfer Lemma. As suggested by the slogan, we pass to an $\aleph_1$-saturated extension (K^*, v^*) of (K, v), and decompose it via the Standard Decomposition (Theorem 3.1.47):

$$v^* : K^* \xrightarrow{v_0^*} K^* v_0^* \xrightarrow{\overline{v_p^*}} K^* v_p^* \xrightarrow{\overline{\overline{v^*}}} K^* v_K^*.$$

Let us denote $(F, w) := (K^* v_0^*, \overline{v_p^*})$ for better readability. Then wF is of rank 1 (see Theorem 3.1.47) and p-divisible since vK (and hence v^*K^*) is p-divisible by assumption; in particular, wF is dense in $\mathbb{R}$. The fact that (K^*, v^*) is $\aleph_1$-saturated then implies that all Dedekind cuts are realised in the value group, meaning that $wF \cong \mathbb{R}$. Moreover since $G_K \cong G_{K^*}$ is small by assumption, we see that G_F, the absolute Galois group of the residue field F of K^*, is small as well, so Fw is perfect by Pop's Lemma 3.2.10.

Next, we claim that any finite extension E/F is defectless. If E_0 denotes the inertia subfield of E/F, then $f_{E/F} = f_{E_0/F}$, so any defect could be observed in E/E_0; as $wF \cong \mathbb{R}$ is divisible, this would hence be an immediate extension of E_0. Hence, we are reduced to showing that inert extensions of F are algebraically maximal. Using the fact that finite extensions of saturated extensions are again saturated, we can further reduce this to showing that F is algebraically maximal. So let us assume we could find a non-trivial simple finite immediate extension $F(\alpha)/F$. Then α is the root of a simple polynomial f over F, and we denote its roots by $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$, where $n \geq 2$. Observe that for any $c \in F$,

$$\widetilde{w}(c - \alpha_1) = \cdots = \widetilde{w}(c - \alpha_n)$$

by the Conjugacy Theorem 3.1.15, so $\frac{w(f(c))}{n} = \widetilde{w}(c - \alpha)$. Using Krasner's lemma, this implies that $w(f(F))$ must be bounded, and hence attains its maximum by saturation. However, as $F(\alpha)/F$ is immediate, for any $x_0 \in F(\alpha)$, there are $y, z \in F$ such that

$$w(y) = w(x_0 - \alpha) \quad \text{and} \quad \overline{z} = \overline{\frac{x_0 - \alpha}{y}}.$$

In particular, denoting $x_1 \coloneqq x_0 - yz \in F$, we get

$$w(x_1 - \alpha) = w(x_0 - \alpha - zy) > w(y) = w(x_0 - \alpha).$$

Together with the identity $w(x_i - \alpha) = \frac{w(f(x_i))}{n}$ for $i \in \{1, 2\}$ from before, this implies $w(f(x_1)) > w(f(x_0))$, which is the required contradiction.

Putting everything together, we see that $R_F = 1$, for otherwise any C_p-extension of F^R would give to rise to a defect C_p-extension of some finite extension of F (by p-divisibility of vF and perfectness of Fv). As vF is divisible, we further see $I_F = R_F = 1$, which implies $G_F \cong G_{Fw}$ by the First Exact Sequence (Fact 3.1.22).

To finish our construction, it hence remains to show that $G_F \cong G_K$. From the smallness of G_K, we first see that $G_K \cong G_{K^*}$. Now, as $\operatorname{char} F = 0$, we see that $R_{K^*} = 1$ by Fact 3.1.23. Hence, as $v_0^* K^*$ is divisible, we get $I_{K^*} = 1$ as well, so we get $G_{K^*} \cong G_F$ from the First Exact Sequence again.

Tilting Construction We now sketch Gitin's new proof of the Transfer Lemma based on the tilting construction developed in [GKS, Section 4], where it is observed that a similar construction also appears in an argument of Kuhlmann–Rzepka [KR23, Proposition 4.4]. As before, we restrict ourselves to the main ideas and refer the reader to the original sources for full details.

The tilting construction applies to *perfectoid fields*, which can be defined as follows:

Definition 3.2.19. A complete valued field (K, v) is called *perfectoid* if

(i) vK is of rank 1;

(ii) Kv is of characteristic $p > 0$;

(iii) $\mathcal{O}_v / p\mathcal{O}_v$ is semiperfect, that is, the Frobenius map $x \mapsto x^p$ is surjective.

The tilting construction associates, in a natural manner, to any perfectoid field of characteristic 0 a perfectoid field of characteristic p. The following result, which relates the absolute Galois groups of these two fields, was originally proved by Kedlaya–Liu and Scholze and is often referred to as the *Generalised Fontaine–Wintenberger Theorem*.

Theorem 3.2.20. *Let K be a perfectoid field of characteristic 0. There exists a perfectoid field $K^\flat$, called the* tilt *of K, which is naturally associated to K, such that* $\operatorname{char} K^\flat = p$ *and*

$$G_K \cong G_{K^\flat}.$$

We are now in a position to outline the second proof of the Transfer Lemma. Our goal is to show that the completion $\widehat{K}$ is perfectoid. Assuming this, we obtain

$$G_K \cong G_{\widehat{K}} \cong G_{\widehat{K}^\flat}$$

by Proposition 3.1.36 and Theorem 3.2.20, making $\widehat{K}^\flat$ the required field of characteristic p with absolute Galois group isomorphic to G_K. It therefore suffices to verify that $(\widehat{K}, \widehat{v})$ is perfectoid.

Properties (i) and (ii) in the definition of a perfectoid field follow immediately from the fact that $(\widehat{K}, \widehat{v})$ and (K, v) have isomorphic residue fields and value groups. For property (iii), note similarly that $\mathcal{O}_{\widehat{v}}/p\mathcal{O}_{\widehat{v}}$ is canonically isomorphic to $\mathcal{O}_v/p\mathcal{O}_v$. Thus, it remains to prove that $\mathcal{O}_v/p\mathcal{O}_v$ is semiperfect.

To establish semiperfectness of $\mathcal{O}_v/p\mathcal{O}_v$, we fix an element $x \in \mathcal{O}_v$ and construct a sequence of increasingly accurate approximations to a p-th root of x. We first observe that smallness of G_K implies $\dim_{\mathbb{F}_p} K^\times/K^{\times p} < \infty$ by Lemma 3.2.8. In particular, Kv is perfect by Pop's Lemma 3.2.10. Now let $\{a_1 K^{\times p}, \dots, a_n K^{\times p}\}$ be a set of representatives for $K^\times/K^{\times p}$. Since the value group vK is p-divisible, we may assume without loss of generality that $a_1, \dots, a_n \in \mathcal{O}_v^\times$; using the perfectness of Kv, we may assume such that $a_1, \dots, a_n \in 1 + \mathcal{M}_v$. Define

$$\gamma := \min\{v(a_i - 1) : 1 \leq i \leq n\} > 0.$$

As vK has rank 1, we can choose $m \in \mathbb{N}$ such that $m\gamma \geq v(p)$.

We now construct approximations to a p-th root of x. First, write

$$x = y_1^p(1 + z_1)$$

with $y_1, z_1 \in \mathcal{O}_v$ and $v(z_1) \geq \gamma$. Inductively, suppose that $z_i \in \mathcal{O}_v$ with $v(z_i) \geq \gamma$, and write

$$z_i = y_{i+1}^p(1 + z_{i+1})$$

for suitable $y_{i+1}, z_{i+1} \in \mathcal{O}_v$ with $v(z_{i+1}) \geq \gamma$.

Proceeding in this manner yields the decomposition

$$x = y_1^p(1 + y_2^p(1 + \cdots(1 + z_m)\cdots)),$$

which expands as

$$x = y_1^p + y_1^p y_2^p + \cdots + y_1^p y_2^p \cdots y_m^p + y_1^p y_2^p \cdots y_m^p z_m,$$

where

$$v(y_1^p y_2^p \cdots y_m^p z_m) = v(x) + v(z_1) + v(z_2) + \cdots + v(z_m) \geq m\gamma \geq v(p)$$

by construction. Thus, $y_1^p y_2^p \cdots y_m^p z_m \in p\mathcal{O}_v$, making $y_1 + y_1 y_2 + \cdots + y_1 y_2 \cdots y_m$ the required p-th root of x modulo $p\mathcal{O}_v$.

3.2.5 Galois characterisation of henselianity

The main result of this section provides a method for recovering certain henselian valuations—those we shall call *tamely branching*—from absolute Galois groups. We begin by stating the result. After giving some historical context, we motivate the definition of tamely branching valuations and then proceed to the proof.

Definition 3.2.21. Let (K, v) be a valued field and p any prime. We say v is *tamely branching at* p if

(i) $\operatorname{char} Kv \neq p$;

(ii) $vK \neq pvK$;

(iii) $p^2 \mid |G_{Kv}|$, whenever $(vK : pvK) = p$.

Theorem 3.2.22 (Galois characterisation of henselianity)**.** *A field K admits a henselian valuation, tamely branching at p, if and only if G_K has a Sylow p-subgroup $P \ncong C_2, \mathbb{Z}_p, \mathbb{Z}_2 \rtimes C_2$ that contains a non-trivial normal abelian closed subgroup N.*

Recovering valuations lies at the very heart of extracting arithmetic information from Galois-theoretic data. Both Neukirch's Theorem 1.1.1 and Pop's Theorem 1.1.6 crucially rely on this principle. For example, Neukirch's Theorem builds on the following result [Neu68, Satz 1], which can be viewed as an early precursor to the full Galois-theoretic characterisation of henselian valued fields.

Theorem 3.2.23 (Neukirch 1968)**.** *Let $K \subseteq \mathbb{Q}^{\mathrm{alg}}$ be a field such that*

(i) G_K is pro-solvable and

(ii) the Brauer group $\operatorname{Br}(K)$ is not a p-group for any prime p and not a $\{2,3\}$-group (i.e., a group where each element has order $2^n 3^m$).

Then K admits a henselian valuation.

Pop extended Neukirch's result [Pop88, Satz 1.13], keeping the assumption of pro-solvability of G_K, but replacing condition (ii) with a more general one. Incidentally, in [Koe95], this generalised result was used to show that fields K with $G_K \cong G_{\mathbb{Q}_p}$ admit a henselian valuation, leading to a complete proof of the Galois characterisation of p-adically closed fields, Theorem 3.0.1. Nevertheless, the full Galois characterisation of henselianity, as stated above, had not yet been established.

Further progress was made in [EK98], where the authors proved a p-henselian analogue of Theorem 3.2.22, extending earlier results in [EN94, Efr95b] for the case $p = 2$. A criterion for henselian valuations was later formulated in [Koe01], although it required the additional assumption that the Sylow p-subgroups of G_K are solvable. This restriction was subsequently removed in [Koe03] via the henseling down techniques discussed in Section 3.1.3.4. The result and its proof were also presented in Engler and Prestel's exposition [EP05, Section 5.4], which our treatment here generally follows. We adapt some of their arguments for clarity.

Before turning to the proof of Theorem 3.2.22, we will motivate Definition 3.2.21 by indicating why we can only expect to recover tamely branching henselian valuations from absolute Galois groups.

Remark 3.2.24. (a) Let k be a field of characteristic 0 that does not admit a non-trivial henselian valuation, e.g., $k = \mathbb{Q}$. Further, let (K, v) be a henselian valued field with divisible value group vK and residue field $Kv = k$, e.g., the field of Puiseux series over k (see Example 3.0.2). Then $G_K \cong G_k$ by Facts 3.1.22 and 3.1.23. By our assumption on k, we cannot expect to recover v from the isomorphism class of G_K. Therefore, we require vK to be non-p-divisible for at least one prime p, motivating (ii) in Definition 3.2.21.

(b) Consider $K = \mathbb{C}(\!(t)\!)$ with the t-adic valuation. We saw in Example 3.1.30 that $G_K \cong G_{\mathbb{F}_q}$ for any prime q. Therefore, we cannot expect to recover the t-adic valuation from the isomorphism class of G_K. In general, if $\operatorname{char} Kv \neq p$, $(vK : pvK) = p$, and $p \nmid G_{Kv}$, then G_K has Sylow p-subgroup $\mathbb{Z}_p$. However, this is the absolute Galois group of $\bigcup_{p \nmid n} \mathbb{F}_{q^n}$, which admits only the trivial valuation, hence motivating (iii).

(c) If $p > 2$, then $p \mid G_{Kv}$ implies $p^2 \mid G_{Kv}$ by the Artin-Schreier Theorem 1.1.2. There is yet another issue if $p = 2$ and $2 \mid G_{Kv}$, but $4 \nmid G_{Kv}$. The field $K = \mathbb{R}(\!(t)\!)$, endowed with the t-adic valuation v, is henselian with $\operatorname{char} Kv \neq 2$, $(vK : 2vK) = 2$, and $G_{Kv} \cong C_2$. By Theorem 3.1.27, its absolute Galois group is $\widehat{\mathbb{Z}} \rtimes C_2$ (which has Sylow 2-subgroup $\mathbb{Z}_2 \rtimes C_2$). However, it is possible

to construct a field L that does not admit a non-trivial henselian valuation with $G_L \cong \mathbb{Z}_2 \rtimes C_2$ as follows. Let L be the intersection of two distinct real closures of $\mathbb{Q}$ in $\mathbb{Q}^{\mathrm{alg}}$, and let σ and τ be the involutions in $G_{\mathbb{Q}}$ corresponding to the two real closures; by the Galois correspondence, they together topologically generate G_L. By Artin-Schreier, they do not commute and $\sigma\tau$ generates an infinite cyclic group Z, where σ acts on Z by conjugation via $\sigma\tau \mapsto \tau\sigma = (\sigma\tau)^{-1}$. Hence, $G_L = \langle \sigma, \tau \rangle$ is isomorphic to $\overline{Z} \rtimes \langle \sigma \rangle$. If we choose the two real closures such that σ and τ lie in the same Sylow 2-subgroup of $G_{\mathbb{Q}}$, then G_L will be of the form $\mathbb{Z}_2 \rtimes C_2$.

However, any henselian valuation v on L extends uniquely to the real closures used to construct L. If R is such a real closure and w denotes the extension of v to R, then Rw is real closed (it cannot be algebraically closed, since otherwise -1 would be a square in Rw and hence in R by Hensel's lemma). In particular, $\operatorname{char} Lv = 0$, so v is trivial on $\mathbb{Q}$, and hence on $L \subseteq \mathbb{Q}^{\mathrm{alg}}$.

Furthermore, note that condition (i) on the characteristic of the residue field allows for a natural choice of the group N in Theorem 3.2.22 (see below).

For the remainder of this section, we use the following notation. Given a field K and a closed subgroup $H \leq G_K$, we write $\operatorname{Fix} H$ for the (absolute) fixed field of H inside K^{sep}.

Lemma 3.2.25. *Let K be a field with a henselian valuation v, tamely branching at p, and w its unique extension to $L \coloneqq \operatorname{Fix} P$, where P is Sylow p-subgroup of G_K. Then, the absolute inertia group I_L is a non-trivial normal abelian closed subgroup of P. Moreover, $P \ncong C_2, \mathbb{Z}_p, \mathbb{Z}_2 \rtimes C_2$.*

Proof. By assumption and Fact 3.1.22, $D_L = G_L = P$ and I_L is a normal closed subgroup of P. Since $\operatorname{char} Kv \neq p$, the absolute ramification subgroup R_L is trivial by Fact 3.1.23. Using Theorem 3.1.27, we compute

$$I_L \cong \mathbb{Z}_p^{\dim_{\mathbb{F}_p} wL/pwL} \tag{3.2.9}$$

$$P = D_L \cong I_L \rtimes G_{Lw}. \tag{3.2.10}$$

As P is a Sylow p-subgroup of G_K, the extension L/K is prime-to-p, and hence $p \nmid [Lw : Kv]$ and $(wL : pwL) = (vK : pvK)$. Therefore, w is tamely branching at p as well, so I_L is indeed non-trivial abelian by (3.2.9) and $P \ncong C_2, \mathbb{Z}_p, \mathbb{Z}_2 \rtimes C_2$ by (3.2.10). □

This lemma proves the "only if" part in Theorem 3.2.22; we will now focus on the other direction. We prove it in two steps: First, we establish the theorem in the "classical" case where $G_K \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$ (the name stems from the fact that any Sylow p-subgroup of $G_{\mathbb{Q}_q}$ is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ for $p \neq q$, see Proposition 3.1.31). In a second step, we reduce the general case to the "classical" one.

Proposition 3.2.26 (Classical case)**.** *Let K be a field with $G_K \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$. Assume additionally that $\sqrt{-1} \in K$ if $p = 2$. Then K admits a henselian valuation tamely branching at p.*

Some of the ideas in the proof of the classical case are inspired by cohomological considerations; as such, they will look similar to those in Section 3.2.3. Otherwise, our main technical tool is the notion of rigid elements, as introduced in Section 3.1.4 (Theorem 3.1.68 will yield the desired valuation on K).

Before we establish the classical case, we prove the following basic lemma, which allows us to pass to finite extensions of K without changing the shape of the Galois group.

Lemma 3.2.27. *Let K be a field with $G_K \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$. Then for every finite extension L/K, also $G_L \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$ (with possibly different action in the semi-direct product).*

Proof. Let

$$1 \longrightarrow \mathbb{Z}_p \xrightarrow{\iota} G_K \xrightarrow{\pi} \mathbb{Z}_p \longrightarrow 1$$

be the short exact sequence associated to the semidirect product for G_K. As L/K is a finite extension, G_L is a closed subgroup of finite index in G_K. Hence, $\iota^{-1}(G_L)$ and $\pi(G_L)$ will also be closed of finite index in their respective copies of $\mathbb{Z}_p$. Therefore, $\iota^{-1}(G_L)$ and $\pi(G_L)$ are themselves isomorphic to $\mathbb{Z}_p$. The associated short sequence with maps $\iota|_{\iota^{-1}(G_L)}$ and $\pi|_{G_L}$ remains exact and split, so the claim follows. □

Recall that an element $x \in K^\times \setminus K^{\times p}$ is called p-rigid with respect to $K^{\times p}$ if

$$K^{\times p} + xK^{\times p} \subseteq \bigcup_{i=0}^{p-1} x^i K^{\times p}. \tag{3.2.11}$$

If all such x are p-rigid and $(K^\times : K^{\times p}) > p$, then Theorem 3.1.68 allows us to create a valuation for the choice of parameters $S = T_S = K^{\times p}$. The key idea of the proof is that the right-hand side of (3.2.11) is given by the image of the norm map for $K(\sqrt[p]{x})/K$.

We organise the proof into six steps.

Step 1. Show $\operatorname{char} K \neq p$ and $\zeta_p \in K$. Deduce $\dim_{\mathbb{F}_p} K^\times/K^{\times p} = 2$.

Step 2. Show that every $x \in K \setminus K^{\times p}$ is p-rigid via Kummer theory.

Step 3. Create a valuation v satisfying $vK \neq pvK$ using Theorem 3.1.68.

Step 4. Show that $\operatorname{char} Kv \neq p$.

Step 5. Show that v is henselian.

Step 6. Show that v is tamely branching at p.

Proof of Proposition 3.2.26. We follow the six steps outlined above.

Step 1. Note that K admits precisely two linearly disjoint C_p-extensions because $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ has rank two. Suppose for now that $\operatorname{char} K = p$. Then, by Artin-Schreier theory (Theorem 3.2.14),

$$\dim_{\mathbb{F}_p} K/\wp(K) = 2.$$

Let $a\wp(K)$ and $b\wp(K)$ be a basis for $K/\wp(K)$. The splitting fields of $X^p - X - a$ and $X^p - X - b$ are then linearly disjoint. If x is a root of $X^p - X - a$, then $\alpha := -x^{p-1}$ satisfies $\operatorname{Tr}(\alpha) = 1$ (as in (3.2.7) in the proof of Lemma 3.2.15), where $\operatorname{Tr} = \operatorname{Tr}_{K(x)/K}$.

We claim that $a\alpha$, $b\alpha$, and b are $\mathbb{F}_p$-linearly independent in $K(x)/\wp(K(x))$. Indeed, let $i_1, i_2, i_3 \in \mathbb{F}_p$ be such that

$$i_1 a\alpha + i_2 b\alpha + i_3 b = y^p - y$$

for some $y \in K(x)$. Taking the trace on both sides of the equation, we obtain

$$i_1 a + i_2 b + p(i_3 b) = i_1 a + i_2 b = \operatorname{Tr}(y^p) - \operatorname{Tr}(y) = \operatorname{Tr}(y)^p - \operatorname{Tr}(y),$$

which implies $i_1 = i_2 = 0$ by our choice of a and b. Hence, $y^p - y - i_3 b = 0$. By our choice of b, this implies $i_3 = 0$, and therefore, $\dim_{\mathbb{F}_p} K(x)/\wp(K(x)) \geq 3$. Recall that Lemma 3.2.27 tells us that $G_{K(x)} \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$, which contradicts our initial observation applied to $K(x)$. Therefore, $\operatorname{char} K \neq p$ and $\zeta_p \in K^{\mathrm{sep}}$.

Note that $[K(\zeta_p) : K] \leq p - 1$ and the assumption that G_K is a pro-p group imply $\zeta_p \in K$. In particular, $\dim_{\mathbb{F}_p} K^\times/K^{\times p} = 2$ by Kummer theory (Theorem 3.2.13).

Step 2. Let $x \in K^\times \setminus K^{\times p}$ and set $L := K(\sqrt[p]{x})$. Choose two cosets $xK^{\times p}$, $yK^{\times p}$ that form an $\mathbb{F}_p$-basis for $K^\times/K^{\times p}$. By Kummer theory, $\sqrt[p]{x}L^{\times p}$ and $yL^{\times p}$ are

linearly independent in $L^\times/L^{\times p}$ and hence form a basis by Lemma 3.2.27. Thus, we may write

$$L^\times = \bigcup_{0\le i,j<p} (\sqrt[p]{x})^i y^j L^{\times p}.$$

For any $a, b \in K^\times$, there hence exist $i, j \in \{0, \dots, p-1\}$ and $z \in L^\times$ such that

$$a + b\sqrt[p]{x} = (\sqrt[p]{x})^i y^j z^p.$$

Note that $a + b\sqrt[p]{x}$ has minimal polynomial $(X-a)^p - b^p x$. Applying the norm map to both sides yields

$$(-1)^{p-1} N_{L/K}(a + b\sqrt[p]{x}) = (-1)^{p-1}a^p + xb^p = x^i y^{jp} N_{L/K}(z)^p \in x^i K^{\times p}.$$

This proves the inclusion (3.2.11): x is p-rigid. (Note that we assumed $\sqrt{-1} \in K$ if $p = 2$.)

Step 3. By Step 2, any $x \in K^\times \setminus K^{\times p}$ is p-rigid. Moreover, $(K^\times : K^{\times p}) = p^2 > p$. By the creation of valuations from p-rigid elements (Theorem 3.1.68) for parameters $S = T_S = K^{\times p}$, we obtain a non-trivial valuation v with $vK \neq pvK$. Additionally, we replace v by the coarsening with respect to the maximal p-divisible convex subgroup. Then, v will not contain any non-trivial p-divisible convex subgroups and v remains non-p-divisible.

Step 4. We now prove $\operatorname{char} Kv \neq p$. Suppose for contradiction that $\operatorname{char} Kv = p$. Then, $\operatorname{Conv}(v(p))$ is a non-trivial convex subgroup. By our choice of v, we know that $\operatorname{Conv}(v(p))$ and hence $(0, v(p)] \subset vK$ is not p-divisible. So we may choose an element $x \in K$ such that

$$0 < v(x) \le v(p) \quad \text{and} \quad v(x) \notin pvK.$$

In particular, $x \in K^\times \setminus K^{\times p}$ is p-rigid, so there exist $i \in \{0, \dots, p-1\}$ and $y \in K^\times$ such that $1 + x = x^i y^p$. Note that $v(1+x) = 0$ implies

$$i = 0,\ v(y) = 0, \text{ and } y \equiv 1 \pmod{\mathcal{M}_v},$$

the latter as in (3.2.5). If we write $y = 1 + z$ with $z \in \mathcal{M}_v$, then

$$v(x) = v((1+z)^p - 1) \ge \min\{v(p) + v(z), v(z^p)\}.$$

But $v(x) < v(p) + v(z)$ implies $v(x) = v(z^p)$, and hence $v(x) \in pvK$, contrary to our choice of x.

Step 5. Assume that v is not henselian. By Lemma 3.1.39, there exists a Galois extension L/K of degree p with pairwise inequivalent prolongations $v_1, \dots, v_r$ of v to L with $r > 1$. By the fundamental equality (Corollary 3.1.25), $p = refd$ and therefore

$$e = f = d = 1 \quad \text{and} \quad r = p,$$

where $v_1, \dots, v_p$ are thus immediate, incomparable prolongations (cf. Fact 3.1.13). By Kummer theory, $L = K(\sqrt[p]{x})$ for some $x \in \mathcal{O}_v^\times$ (otherwise, we would have $e = p$). Set $x_0 \coloneqq \sqrt[p]{x} \notin L^{\times p}$.

Applying the weak approximation theorem (Fact 3.1.14), we may find for each $i \in \{1, \dots, p\}$,

$$x_i \in \mathcal{M}_{v_i} \cap \bigcap_{j \neq i} \mathcal{O}_{v_j}^\times. \tag{3.2.12}$$

As all v_i are immediate, we have $v_i L = vK$ for each i. We may assume without loss of generality, that $v_i(x_i) \notin pvK$, as follows: if $v_i(x_i) \in pvK$, use the fact that $\mathrm{Conv}(v_i(x_i))$ is non-trivial to find $y \in K$ with $v(y) \in (0, v_i(x_i))$ and $v(y) \notin pvK$ (otherwise, as in Step 4, $(0, v_i(x_i)] \subset vK$ would be p-divisible, which cannot happen). Replacing x_i by $x_i + y$, gives the desired element satisfying (3.2.12) and $v_i(x_i) \notin pvK$.

We claim that $L(\sqrt[p]{x_0}, \sqrt[p]{x_1}, \dots, \sqrt[p]{x_p})/L$ has Galois group C_p^{p+1}. By Kummer theory, it suffices to show that

$$x_0^{i_0} x_1^{i_1} \cdots x_p^{i_p} \in L^{\times p} \text{ with } i_0, \dots, i_p \in \{0, \dots, p-1\} \Longrightarrow i_0 = \cdots = i_p = 0.$$

Evaluating this product by v_j yields $i_j = 0$ for every $j = 1, \dots, p$. Finally, recall that $x_0 \notin L^{\times p}$, so $i_0 = 0$ as well. By Step 1 and Lemma 3.2.27, we know that L admits at most two linearly disjoint C_p-extensions, so our construction is impossible. We conclude that v must be henselian.

Step 6. Assume $(vK : pvK) = p$ and let $x \in K$ be such that $v(x) \notin pvK$. It remains to verify property (iii), that is, $p^2 \mid |G_{Kv}|$. If $G_{Kv} = 1$, then $\mathcal{O}_v^\times = \mathcal{O}_v^{\times p}$, since $Kv^\times = Kv^{\times p}$ and $1 + \mathcal{M}_v = (1 + \mathcal{M}_v)^p$ by henselianity. This would imply that there is only one C_p-extension, namely $K(\sqrt[p]{x})$. Hence $G_{Kv} \neq 1$ (and we are done by the Artin-Schreier Theorem 1.1.2 in the case $p \neq 2$).

Let $L \coloneqq K(\sqrt[p]{y})$, where $y \in \mathcal{O}_v^\times$ is such that $yv \notin Kv^{\times p}$. In particular, L/K is unramified of degree $f = p$. As before, we cannot have $G_{Lv} = 1$, because L admits more than one C_p-extension. This shows that $p^2 \mid G_{Kv}$. □

From this, we are able to deduce the general case. Our main tool will be henseling down (Theorem 3.1.54). In order to apply this theorem to a tamely branching valuation v, we require $\mathcal{O}_v \in H(K)$ and moreover, that no proper coarsening of v has real closed residue field. Conveniently, we may assume this extra condition without loss of generality:

Lemma 3.2.28 ([EP05, Lemma 5.4.6])**.** *Let (K, v) be a henselian valued field, v tamely branching at p. Then there exists a valuation ring in $H(K)$ tamely branching at p as well. If $p = 2$, we can find a henselian valuation on K, tamely branching at 2, such that furthermore, no proper coarsening has real closed residue field.*

Proof. It suffices to consider the case $\mathcal{O}_v \in H_2(K)$, i.e., Kv separably closed. We claim that the canonical henselian valuation v_K is tamely branching at p. Since $H_2(K) \neq \emptyset$, Kv_K is separably closed. As v_K is coarser than v, we consider the decomposition:

$$K \xrightarrow{v_K} Kv_K \xrightarrow{\overline{v}} Kv \qquad (v : K \to Kv)$$

We see that $\mathrm{char}(Kv_K) \neq p$. Moreover, $\overline{v}(Kv_K)$ is divisible as Kv_K is separably closed. Thus,

$$(v_K K : pv_K K) = (vK : pvK),$$

and therefore, $v_K K$ cannot be p-divisible. Note that since Kv is separably closed, $p^2 \nmid |G_{Kv}|$ and hence, $(v_K K : pv_K K) = (vK : pvK) \neq p$.

For $p = 2$, consider the case that some coarsening of v has real closed residue field. Let w denote the coarsest such coarsening, which exists by Fact 3.1.55. Then, $\mathcal{O}_w \in H(K)$ automatically satisfies the required property, and it remains to show that w is tamely branching at 2. We proceed as before, with w taking the place of v_K and real closedness of Kw playing the role of separable closedness of Kv_K. Since Kw is real closed, it follows that $\mathrm{char}(Kw) = 0$ and that the value group $\overline{v}(Kw)$ is divisible (for any $x \in Kw$, we have that x or $-x$ has a qth root for any prime q).

Again, $(wK : 2wK) = (vK : 2vK)$ holds as in the previous argument. The assumption that v is tamely branching at 2 implies $(vK : 2vK) \geq 4$ (since $|G_{Kv}| = 2$, cf. Fact 3.1.55). It follows that w is also tamely branching at 2. □

Similarly, we need to ensure that the process of henseling down also preserves the property of being tamely branching at a prime p.

Lemma 3.2.29. *Let (L, w) be a valued field, w tamely branching at p. If L/K is an algebraic extension of fields, then $v = w|_K$ is tamely branching at p as well.*

Proof. Recall that wL/vK is a torsion group and Lw/Kv an algebraic extension by Fact 3.1.11. In particular, $p^2 \mid G_{Lw}$ implies $p^2 \mid G_{Kv}$. The rest of the claim follows immediately from the following general fact about abelian groups: if $\Delta \leq \Gamma$ are p-torsion-free abelian groups such that Γ/Δ is a torsion group, then

$$\dim_{\mathbb{F}_p}(\Delta/p\Delta) \geq \dim_{\mathbb{F}_p}(\Gamma/p\Gamma).$$

See [EP05, Example 5.5.2] for a proof of this inequality. □

Corollary 3.2.30 (general case)**.** *Let K be a field and p any prime. Assume G_K has a Sylow p-subgroup $P \ncong C_2, \mathbb{Z}_p, \mathbb{Z}_2 \rtimes C_2$ that contains a non-trivial normal abelian closed subgroup N. Then K admits a henselian valuation, tamely branching at p.*

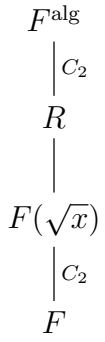
Proof. By Theorem 1.1.2, N is torsion-free unless $p = 2$ and $\sqrt{-1} \notin \operatorname{Fix} N$. In this exceptional case, the extension $K(\sqrt{-1})/K$ has degree 2. Hence, by henseling down (Theorem 3.1.54(ii)) together with Lemma 3.2.29, it suffices to show that $K(\sqrt{-1})$ admits a henselian valuation tamely branching at 2.

Thus, replacing K by $K(\sqrt{-1})$ if necessary, and correspondingly replacing P by $P' := P \cap G_{K(\sqrt{-1})}$ and N by $N' := N \cap G_{K(\sqrt{-1})}$, we may assume that N is torsion-free. This replacement may alter the original hypotheses on P and N. However, P' is again a Sylow 2-subgroup of $G_{K(\sqrt{-1})}$, and N' remains a closed normal abelian subgroup of P'. Moreover, $P' \ncong \mathbb{Z}_2$, for otherwise P/P' has order at most 2, so $P \cong \mathbb{Z}_2$ or $P \cong \mathbb{Z}_2 \rtimes C_2$, contrary to assumption. Finally, N' remains non-trivial. Indeed, if $N' = 1$, then $N \cap G_{K(\sqrt{-1})} = 1$, so N injects into $G_K/G_{K(\sqrt{-1})}$, hence $|N| \leq 2$, and therefore $N \cong C_2$. Thus it remains to exclude this case.

Claim (cf. [Gey69, Folgerung 1.11]). Let F be a field such that G_F is pro-2. Then G_F contains no proper non-trivial normal subgroup isomorphic to C_2.

Proof of Claim. Assume for contradiction that $C_2 \triangleleft G_F$ is a proper non-trivial normal subgroup, and let $R := (F^{\mathrm{alg}})^{C_2}$. Then R is real closed by Theorem 1.1.2, and since C_2 is normal in G_F, the extension R/F is Galois with $\mathrm{Gal}(R/F) \cong G_F/C_2$.

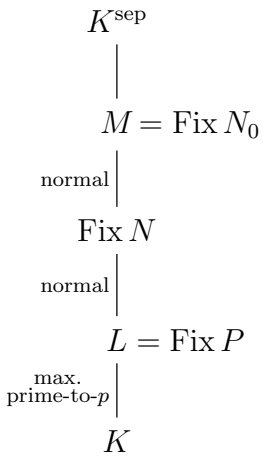
Since G_F/C_2 is a non-trivial pro-2 group, it has a quotient of order 2, so there is a quadratic extension $F(\sqrt{x})/F$ contained in R by the Galois correspondence.



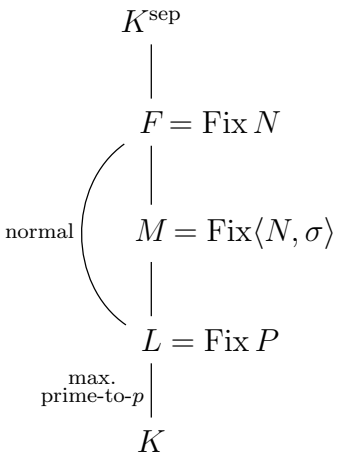
The non-trivial F-automorphism of $F(\sqrt{x})$ extends to an F-automorphism of R, since R/F is Galois. There are thus two F-embeddings of $F(\sqrt{x})$ into R, inducing two orderings on $F(\sqrt{x})$: in one, $\sqrt{x} > 0$, and in the other, $\sqrt{x} < 0$. But R is real closed, so it has a unique ordering, a contradiction. ◇

We have shown that, after replacing K by $K(\sqrt{-1})$ if necessary and replacing P, N accordingly, we may assume that P is a Sylow p-subgroup with $P \ncong \mathbb{Z}_p$, and that N is a non-trivial closed normal abelian subgroup of P. Moreover, we can now view N as a torsion-free $\mathbb{Z}_p$-module.

Case 1. Let us first consider the easier case that N is not topologically generated by a single element (i.e., $N \ncong \mathbb{Z}_p$), so there exists $N_0 \lhd N$ with $N_0 \cong \mathbb{Z}_p \times \mathbb{Z}_p$. By the Classical Case (Proposition 3.2.26), there exists a henselian valuation w on $M \coloneqq \operatorname{Fix} N_0$, tamely branching at p, which we may assume to lie in $H(M)$ by Lemma 3.2.28. Now, we may hensel down as indicated by the left diagram.



Case 1.



Case 2.

More precisely, two applications of henseling down (Theorem 3.1.54(i)) together with Lemma 3.2.29 show that $w|_L$ is in $H(L)$ and tamely branching at p, where $L \coloneqq \operatorname{Fix} P$. By Lemma 3.2.28, again, we may additionally assume that L admits

a henselian valuation w', tamely branching at p, such that no proper coarsening has real closed residue field if $p = 2$. Therefore, $w'|_K$ is the desired valuation by henseling down, Theorem 3.1.54(iii).

Case 2. Let us now consider the case that $N \cong \mathbb{Z}_p$. As $P \ncong \mathbb{Z}_p$, we may find some $\sigma \in P \setminus N$ such that $\langle\sigma\rangle \cong \mathbb{Z}_p$ and $\langle N, \sigma\rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$. By Proposition 3.2.26, there exists a valuation w on $M := \operatorname{Fix}\langle N, \sigma\rangle$, tamely branching at p, which we may assume to lie in $H(M)$. For $p = 2$, we additionally require that w does not have any proper coarsenings with real closed residue field. Let u denote the unique prolongation of w to $F := \operatorname{Fix} N$. If $\mathcal{O}_u \in H(F)$, we see that $u|_K$ is the desired valuation by henseling down (as indicated by the right diagram).

It remains to consider the case that $u, v_F \in H_2(F)$ with $\mathcal{O}_u \subsetneq \mathcal{O}_{v_F}$. By definition, Fv_F is separably closed, $\operatorname{char} Fv_F \neq p$ (as Fu is a residue field of Fv_F), and $v_F F$ is not p-divisible (otherwise $N = G_F$ would be trivial). Further, $\mathcal{O}_u \subsetneq \mathcal{O}_{v_F}$ implies $\mathcal{O}_w \subsetneq \mathcal{O}_{v_F|_M}$ (Fact 3.1.13), therefore, $\mathcal{O}_{v_F|_M} \in H_1(M)$ since $\mathcal{O}_w \in H(M)$. By henseling down, $u' := v_F|_L$ lies in $H(L)$ and is tamely branching at p (since $\operatorname{char} Fv_F \neq p$, $v_F F \neq pv_F F$, and $Mv_F|_M$ is not separably closed and $\sqrt{-1} \in Lu'$). Finally, applying henseling down to L/K shows that $v_F|_K = u'|_K$ is henselian and tamely branching at p. □

This completes the proof of Theorem 3.2.22, the Galois characterisation of henselianity.

3.3 Proof of the Galois characterisation of p-adically closed fields

We are finally in a position to prove Theorem 3.0.1. The direction asserting that every field elementarily equivalent to $\mathbb{Q}_p$ has absolute Galois group isomorphic to $G_{\mathbb{Q}_p}$ is substantially easier than the converse. Indeed, by the smallness of $G_{\mathbb{Q}_p}$ (Corollary 3.2.6), this direction follows immediately from the following lemma due to Klingen [Kli74, Proposition 4.2].

Lemma 3.3.1. *Let K be a field with small Galois group. Then for any field F,*

$$F \equiv K \Longrightarrow G_K \cong G_F.$$

Proof (Sketch). Let $n \geq 1$ be a natural number. Since G_K is small, K admits only finitely many extensions of degree at most n. Let K_n denote the compositum of these

finitely many extensions, and let $G_n \coloneqq \mathrm{Gal}(K_n/K)$ (which is finite too). Then K satisfies the first-order sentences φ_n saying "there exists an isomorphism between G_n and the Galois group of the compositum of all extensions of degree $\leq n$ that restrict to an isomorphism between G_{n-1} and the Galois group of the compositum of all extensions of degree $\leq n-1$". Any field $F \equiv K$ satisfies all φ_n. From this, an isomorphism of inverse systems may be recovered, so that

$$G_K = \varprojlim_n G_n \cong G_F. \qquad \square$$

By Theorem 1.1.5, the harder direction that $G_{\mathbb{Q}_p}$ encodes the first-order theory of $\mathbb{Q}_p$ boils down to showing that any field K with $G_K \cong G_{\mathbb{Q}_p}$ has a valuation v with the following properties:

(i) (K, v) is henselian of mixed characteristic $(0, p)$;

(ii) $vK \equiv \mathbb{Z}$;

(iii) $v(p)$ is minimal positive;

(iv) $Kv = \mathbb{F}_p$.

Recall that (ii) admits the following classical algebraic description:

Fact 3.3.2 ([Mar02, Chapter 3])**.** *For an ordered abelian group Γ, the following are equivalent:*

(i) $\Gamma \equiv \mathbb{Z}$*;*

(ii) Γ *has a convex subgroup* $\Delta \cong \mathbb{Z}$ *such that* Γ/Δ *is divisible;*

(iii) Γ *has a minimal positive element and* $[\Gamma : n\Gamma] = n$ *for all* $n \in \mathbb{N}$.

We will show that the canonical henselian valuation v_K, introduced in Section 3.1.3.3, satisfies all the required properties. The strategy is organised into three main steps:

Step 1. Show that the canonical henselian valuation v_K has mixed characteristic $(0, p)$.

Step 1.1. Find henselian valuations on K using the Galois characterisation of henselianity (Theorem 3.2.22). Infer that the canonical henselian valuation v_K is non-trivial and satisfies $Kv_K \neq (Kv_K)^{\mathrm{sep}}$ and $(v_K K : qv_K K) = q$ for all $q \neq p$.

Step 1.2. Deduce that $\mathrm{char}\, K = 0$ using Idea 3.2.11 (Lemmas 3.2.15 and 3.2.17).

Step 1.3. Prove that the prime-to-p roots of unity of K and $\mathbb{Q}_p$ coincide using Lemma 3.2.1.

Step 1.4. Show that $\operatorname{char} Kv_K \neq q$ for all primes $q \neq p$ via cyclotomic extensions.

Step 1.5. Deduce that $\operatorname{char} Kv_K = p$ using the previous steps and ramification-theoretic considerations (Section 3.1.2).

Step 2. Apply the Standard Decomposition (Section 3.1.3.2)

$$v_K : K \xrightarrow[(0,0)]{v_0} Kv_0 \xrightarrow[(0,p)]{\overline{v_p}} Kv_p \xrightarrow[(p,p)]{\overline{\overline{v}}} Kv_K$$

to decompose v_K into three places that can be treated separately. Show that $(Kv_0, \overline{v_p})$ has value group $\mathbb{Z}$ and finite residue field.

Step 2.1. Show G_{Kv_0} cannot be realised as an absolute Galois group in characteristic p. Use the Transfer Lemma 3.2.18 to conclude that $\overline{v_p}(Kv_0)$ is not p-divisible.

Step 2.2. Deduce $\overline{v_p}(Kv_0) \cong \mathbb{Z}$ and Kv_p is finite using Pop's Lemma 3.2.10.

Step 3. Conclude that (K, v_K) is p-adically closed.

Step 3.1. Observe that $Kv_K = \mathbb{F}_p$.

Step 3.2. Prove that $v_K K \equiv \mathbb{Z}$ using the elementary characterisation of $\mathbb{Z}$ (Fact 3.3.2).

Step 3.3. Prove that $v_K(p)$ is minimal positive by use of a counting argument (Lemma 3.2.4 and Remark 3.2.5).

Step 1. To say anything about the canonical henselian valuation v_K, we first need to find at least one sufficiently non-trivial henselian valuation on K.

Step 1.1. For primes $q \neq p$, any Sylow q-subgroups of $G_K \cong G_{\mathbb{Q}_p}$ is isomorphic to a semi-direct product $\mathbb{Z}_q \rtimes \mathbb{Z}_q$ (Proposition 3.1.31). The Galois characterisation of henselianity (Theorem 3.2.22) gives rise to henselian valuations v_q on K, tamely branching at q. In particular, $\operatorname{char} Kv_q \neq q$ and $v_q K \neq q v_q K$, i.e.,

$$r_q \coloneqq \dim_{\mathbb{F}_q}(v_q K / q v_q K) \geq 1.$$

For any $q \neq p$, let K_q be the fixed field of some Sylow q-subgroup of G_K. By henselianity, every v_q has a unique prolongation w_q to K_q. The q-rank r_q does not

change when we pass from K to K_q. By Fact 3.1.23, the ramification subgroup R_{K_q} is trivial (since $\operatorname{char} K_q w_q \neq q$), and

$$\mathbb{Z}_q^{r_q} \cong I_{K_q} \lhd G_{K_q} \cong \mathbb{Z}_q \rtimes \mathbb{Z}_q$$

by Theorem 3.1.27. Using the explicit description in Remark 3.1.32, one can check that the only non-trivial closed normal subgroups of $\mathbb{Z}_q \rtimes \mathbb{Z}_q$ are of the shape $q^s\mathbb{Z}_q \times 1$ and $q^{s_1}\mathbb{Z}_q \rtimes q^{s_2}\mathbb{Z}_q$. Since the latter are non-abelian, we conclude $r_q = 1$, $I_{K_q} \neq G_{K_q}$, and $K_q w_q$ is not separably closed.

We can further see that $G_{K_q w_q} \cong \mathbb{Z}_q$ as follows: If $I_{K_q} \cong q^s\mathbb{Z}_q \times 1$, then

$$G_{K_q w_q} \cong G_{K_q}/I_{K_q} \cong C_{q^s} \rtimes \mathbb{Z}_q.$$

We are done if $s = 0$, so assume for a contradiction that $s \geq 1$. By the Artin-Schreier Theorem 1.1.2, $C_{q^s} \rtimes \mathbb{Z}_q$ can only occur as an absolute Galois group of a field if $q = 2$ and $s = 1$. Moreover, as $\operatorname{Aut}(C_2) = 1$, $C_2 \rtimes \mathbb{Z}_2$ is a direct product in this case. In particular, C_2 is a proper non-trivial normal subgroup of $C_2 \rtimes \mathbb{Z}_2$, which contradicts the claim established in the proof of Corollary 3.2.30. We conclude $I_{K_q} \cong \mathbb{Z}_q \cong G_{K_q w_q}$ in all cases.

While we will continue working with (K, v_q) and (K_q, w_q) until Step 1.4, let us already make some observations about the canonical henselian valuation v_K. As the fields $K_q w_q$ are not separably closed, we have $\mathcal{O}_{v_K} \subseteq \mathcal{O}_{v_q}$ for all $q \neq p$ by Lemma 3.1.51. In particular, $v_q K$ is a quotient of $v_K K$ by a convex subgroup, so $v_K K$ cannot be q-divisible. By repeating the above reasoning for v_K, we deduce that

$$r_q = \dim_{\mathbb{F}_q}(v_K K/q v_K K) = 1,$$

so $(v_K K : q v_K K) = q$ and $K v_K$ is not separably closed.

Step 1.2. From $\operatorname{char} K v_q \neq q$, it follows that $\operatorname{char} K \neq q$ for all primes $q \neq p$. Therefore, to show $\operatorname{char} K = 0$, it only remains to exclude the case $\operatorname{char} K = p$.

By Lemma 3.2.17, the field $\mathbb{Q}_p$ satisfies the following property: it has a C_{p-1}-extension (namely, $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$), which itself admits a C_p-extension that is not embeddable into a C_{p^2}-extension. As $G_K \cong G_{\mathbb{Q}_p}$, the same property holds for K. However, this cannot happen in characteristic p by Lemma 3.2.15.

Step 1.3. Determining the prime-to-p roots of unity of K (from Galois theory alone) is a somewhat subtle affair. We would like to use Lemma 3.2.1, which gives

a Galois characterisation of the roots of unity of certain valued fields (K, v). Condition (iii) in this lemma requires knowledge of the Galois group of the maximal pro-q Galois extension of Kv, which we would typically construct (say, over $\mathbb{F}_p$) by looking at the appropriate cyclotomic extension. Such a direct argument is not available to us due to circularity (we still do not know the prime-to-p roots of unity of K yet). So instead, we will use an auxiliary construction.

Consider the field

$$\mathbb{Q}_{p,q} \coloneqq \mathbb{Q}_p\big(\zeta_{q^\infty}, \sqrt[q^\infty]{p}\big) = \bigcup_{n\geq 1} \mathbb{Q}_p\big(\zeta_{q^n}, \sqrt[q^n]{p}\big).$$

We compute its Galois group as

$$\mathrm{Gal}(\mathbb{Q}_{p,q}/\mathbb{Q}_p) = \mathrm{Gal}(\mathbb{Q}_{p,q}/\mathbb{Q}_p(\zeta_{q^\infty})) \rtimes \mathrm{Gal}(\mathbb{Q}_p(\zeta_{q^\infty})/\mathbb{Q}_p) \cong \mathbb{Z}_q \rtimes (\mathbb{Z}_q \times C),$$

where $C = \mathrm{Gal}(\mathbb{Q}_p(\zeta_q)/\mathbb{Q}_p)$ is a cyclic group of order dividing $q-1$ (the precise order depends on p and q) and the semi-direct product is again given by the Frobenius action as in Remark 3.1.32. Hence, there exists a Galois extension L/K with

$$\mathrm{Gal}(L/K) \cong \mathbb{Z}_q \rtimes (\mathbb{Z}_q \times C).$$

Let u_q be the unique prolongation of v_q to L. By considering possible closed normal abelian subgroups isomorphic to $I_{u_q}(L/K)$ as in Step 1.1, we obtain

$$\mathrm{Gal}(Lu_q/Kv_q) \cong \mathbb{Z}_q \rtimes (\mathbb{Z}_q \times C) \text{ or } \mathrm{Gal}(Lu_q/Kv_q) \cong C_{q^s} \rtimes (\mathbb{Z}_q \times C).$$

In either case, we see that Kv_q admits a Galois extension with Galois group $\mathbb{Z}_q$. Since $G_{K_q w_q} \cong \mathbb{Z}_q$, this must coincide with the maximal pro-q extension, which is only the case for $s = 0$ and $\mathrm{Gal}(Lu_q/Kv_q) \cong \mathbb{Z}_q \times C$. Similarly, one shows that the same holds true for the residue field Kv_K.

These considerations show that (K, v_q) satisfies the conditions of Lemma 3.2.1, and hence,

$$\begin{aligned} \zeta_{q^r} \in \mathbb{Q}_p &\iff \mathbb{Q}_p \text{ admits a } C_{q^r} \times C_{q^r}\text{-extension} \\ &\iff K \text{ admits a } C_{q^r} \times C_{q^r}\text{-extension} \iff \zeta_{q^r} \in K, \end{aligned}$$

for any prime $q \neq p$ and $r \geq 1$. In particular, the set of prime-to-p roots of unity in K is μ_{p-1} for $p \neq 2$ and μ_2 for $p = 2$ by Corollary 2.1.2.

Step 1.4. Assume that $\operatorname{char} Kv_K = q$ for some prime $q \neq p$. As v_K is a refinement of v_q, there exists an induced valuation $\overline{v_K}$ on Kv_q with residue field Kv_K and of mixed characteristic $(\operatorname{char} Kv_q, q)$.

$$K \xrightarrow{v_q} Kv_q \xrightarrow{\overline{v_K}} Kv_K, \qquad K \xrightarrow{v_K} Kv_K$$

Clearly, $\operatorname{char} Kv_q \neq q$ implies $\operatorname{char} Kv_q = 0$. We now derive a contradiction by considering the cyclotomic extension $K(\zeta_{q^\infty})/K$. By Lemma 3.2.3, such a cyclotomic extension can be finite only in one of two exceptional cases, namely $K(\zeta_{q^\infty}) = K(\zeta_q)$ or $K(\zeta_{2^\infty}) = K(\zeta_4)$. Neither of these occur: indeed, this follows by applying Lemma 3.2.1 to $K(\zeta_q)$ and $K(\zeta_4)$; see also Remark 3.2.2. Hence $K(\zeta_{q^\infty})/K$ is an infinite cyclotomic extension. By henselianity, this extension is unramified with respect to v_q. Therefore, by Lemma 3.2.3,

$$\operatorname{Gal}(K(\zeta_{q^\infty})/K) \cong \operatorname{Gal}(Kv_q(\zeta_{q^\infty})/Kv_q) \cong \mathbb{Z}_q \times C.$$

Thus, $Kv_q(\zeta_{q^\infty})$ must be q-closed (recall that the maximal pro-q Galois extension of Kv_q has Galois group $\mathbb{Z}_q$).

From $Kv_q(\zeta_{q^\infty})$ being q-closed and $\operatorname{char} Kv_K = q$, it follows that the residue field of $Kv_q(\zeta_{q^\infty})$ with respect to the unique prolongation of $\overline{v_K}$ is equal to Kv_K and must be q-closed as well. In positive characteristic q, cyclotomic extensions by $\zeta_{q^{q^n}-1}$ have degree dividing q^n. It follows that $\zeta_{q^{q^n}-1} \in Kv_K$ for all $n \in \mathbb{N}$. However, note that we have

$$\gcd\left(\frac{q^{q^{n+1}}-1}{q^{q^n}-1},\, q^{q^n}-1\right) = 1,$$

which is an instance of the well-known identity $\gcd((a^m-1)/(a-1), a-1) = \gcd(m, a-1)$. In conjunction with the above, this implies that there are infinitely many primes q' with $\zeta_{q'} \in Kv_K$. However, this contradicts Step 1.3, where we showed that Kv_K contains a q'-th primitive root of unity for primes $q' \neq p, q$ if and only if $q' \mid (p-1)$. We conclude $\operatorname{char} Kv_K \neq q$ for all primes $q \neq p$.

Step 1.5. To exclude the remaining case, assume that $\operatorname{char} Kv_K = 0$. Here, we will eventually arrive at a contradiction by considering the ramification data for explicit extensions of (K, v_K) implied by this assumption.[3]

[3] By a result of Pop [Pop88, Satz 1.4, Beweis], the Sylow-p subgroups of any non-trivial normal subgroup N of $G_{\mathbb{Q}_p}$ are not pro-cyclic. This provides an alternative argument to exclude the case $\operatorname{char} Kv_K = 0$: By Theorem 3.1.27, the assumption $\operatorname{char} Kv_K = 0$ would imply that G_K has a normal subgroup of the form $\prod_q \mathbb{Z}_q^{r_q}$. By Step 1.1, this implies in particular the existence of a non-trivial normal subgroup $N \cong \mathbb{Z}_q$ of G_K for any $q \neq p$. However, all Sylow-p subgroups of such an N are trivial, and hence pro-cyclic, which contradicts Pop's result.

1) We first show that $v_K K$ is p-divisible. Assume towards a contradiction that

$$r_p \coloneqq \dim_{\mathbb{F}_p}(v_K K/pv_K K) \geq 1,$$

and let K_p be the fixed field of some Sylow p-subgroup of G_K. By ramification theory (Facts 3.1.22, 3.1.23, and Theorem 3.1.27), the absolute ramification subgroup of K_p with respect to the unique prolongation of v_K to K^{sep} is trivial, so $I_{K_p} \cong \mathbb{Z}_p^{r_p}$ is a non-trivial closed normal abelian subgroup of G_{K_p}. Moreover, $G_{K_p} \ncong \mathbb{Z}_p, \mathbb{Z}_2 \rtimes C_2$; for instance, K_p admits C_p^3-extensions by the Degree Lemma 3.2.4. Hence, the absolute Galois groups $G_K \cong G_{\mathbb{Q}_p}$ satisfy the hypotheses of the Galois characterisation of henselianity (Theorem 3.2.22). In particular, both K and $\mathbb{Q}_p$ must admit a henselian valuation tamely branching at p. However, as we have seen in Example 3.1.53, the only henselian valuations on $\mathbb{Q}_p$ are the trivial valuation and the standard p-adic valuation (which has residue characteristic p), neither of which is tamely branching at p. Therefore, $v_K K$ is p-divisible.

2) Next, we claim that K admits a unique $C_{p-1} \times C_{p-1}$-extension L. The existence follows from the fact that $\mathbb{Q}_p$ admits a $C_{p-1} \times C_{p-1}$-extension, namely $\mathbb{Q}_p(\zeta_{(p-1)^2}, \zeta_p)/\mathbb{Q}_p$. To show uniqueness, observe that any such extension is the compositum of its $C_{q^r} \times C_{q^r}$-subextensions, where q^r ranges over the prime powers in the factorisation of $p-1$. At the same time, each $C_{q^r} \times C_{q^r}$-extension of K is unique, for otherwise, the Galois group of the compositum of two distinct $C_{q^r} \times C_{q^r}$-extensions would have q-rank at least 3. For primes $q \mid (p-1)$ this is incompatible with $G_{K_q} \cong \mathbb{Z}_q \rtimes \mathbb{Z}_q$ having q-rank 2.

3) We claim that K admits a unique C_{p-1}-extension unramified with respect to v_K, which can further be uniquely identified in Galois theoretic terms. From Step 1.3, we know that

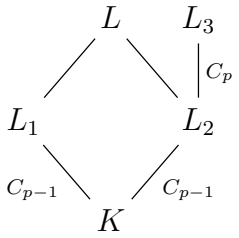
$$\text{Gal}(Kv_K(q)/Kv_K) \cong \mathbb{Z}_q.$$

In particular, Kv_K admits a unique C_{q^r}-extension for each prime power $q^r | (p-1)$. Arguing again via composita, we infer that Kv_K admits a unique C_{p-1}-extension that induces a unique unramified C_{p-1}-extension L_1/K. Using our description of the prime-to-p roots in Step 1.3 and the proof of Lemma 3.2.3, one can explicitly write $L_1 = K(\zeta_{(p-1)^2})$. By Lemma 3.2.1 and Remark 3.2.2, this gives rise to a Galois-theoretic description of L_1: it is the unique C_{p-1}-extension that itself admits a $C_{q^{2r}} \times C_{q^{2r}}$-extension for every prime power $q^r \mid (p-1)$. Moreover, we can identify totally ramified extensions: any C_{p-1}-extension of K that is linearly disjoint from L_1 over K must be totally ramified by the uniqueness of L_1.

4.1) We now derive the contradiction for $p \neq 2$. Consider the C_p-extension of $\mathbb{Q}_p(\zeta_p)$ obtained by adjoining $\sqrt[p]{p}$. Over $\mathbb{Q}_p$, it has a non-abelian Galois group

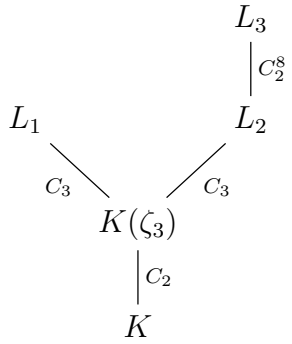
$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_p, \sqrt[p]{p})/\mathbb{Q}_p) \cong C_p \rtimes C_{p-1}.$$

Being totally ramified, it is linearly disjoint from $\mathbb{Q}_p(\zeta_{(p-1)^2})$ over $\mathbb{Q}_p$. Translating over to K, we find a Galois extension L_3/K with Galois group $C_p \rtimes C_{p-1}$ and C_{p-1}-subextension L_2/K, such that L_1 and L_3 are linearly disjoint over K (with L_1 uniquely determined by the above Galois property).



As noted before, L_2/K is totally ramified. Since $v_K K$ is p-divisible, the C_p-extension L_3/L_2 must be unramified. But then, L_3 is the compositum of L_2 and the inertia subfield of L_3/K. Therefore, $\mathrm{Gal}(L_3/K) \cong C_{p-1} \times C_p$ is abelian, contrary to our assumption.

4.2) Finally, consider the case $p = 2$. We need to modify the above constructions slightly to work around the triviality of the $C_{p-1} \times C_{p-1}$-extension. Let us instead start with the C_2-extension $\mathbb{Q}_2(\zeta_3)/\mathbb{Q}_2$. It admits a unique $C_3 \times C_3$-extension given by $\mathbb{Q}_2(\zeta_9, \sqrt[3]{2})/\mathbb{Q}_2(\zeta_3)$, where $\mathbb{Q}_2(\zeta_9)/\mathbb{Q}_2(\zeta_3)$ is the unique unramified C_3-extension and $\mathbb{Q}_2(\zeta_3, \sqrt[3]{2})/\mathbb{Q}_2(\zeta_3)$ is a totally ramified C_3-extension. By Kummer Theory and the Degree Lemma 3.2.4, the field $\mathbb{Q}_2(\zeta_3, \sqrt[3]{2})$ admits a C_2^8-extension.



Let $L_1 \coloneqq K(\zeta_9)$ be the unramified C_3-extension of $K(\zeta_3)$, uniquely identified as the only one that admits a $C_9 \times C_9$-extension. Furthermore, let $L_2/K(\zeta_3)$ be a C_3-extension such that L_1 and L_2 are linearly disjoint over $K(\zeta_3)$, $L_3/K(\zeta_3)$ is Galois, and L_3/L_2 has Galois group C_2^8. As before, $L_2/K(\zeta_3)$ is totally ramified, and L_3/L_2 is unramified by the 2-divisibility of $v_K K$. Therefore, the inertia subfield

of $L_3/K(\zeta_3)$ is a C_2^8-extension of $K(\zeta_3)$. This is, however, impossible: the degree of the maximal abelian Galois extension of exponent 2 of $K(\zeta_3)$ and $\mathbb{Q}_2(\zeta_3)$ must coincide. This degree is equal to 16, as can be seen by Kummer theory and the Degree Lemma 3.2.4,

$$\dim_{\mathbb{F}_2}\left(K(\zeta_3)^\times/K(\zeta_3)^{\times 2}\right) = \dim_{\mathbb{F}_2}\left(\mathbb{Q}_2(\zeta_3)^\times/\mathbb{Q}_2(\zeta_3)^{\times 2}\right) = 4.$$

This concludes our proof that $\operatorname{char} Kv_K = p$.

Step 2. As now $(\operatorname{char} K, \operatorname{char} Kv_K) = (0,p)$, we may consider the Standard Decomposition

$$v_K : K \xrightarrow{v_0} Kv_0 \xrightarrow{\overline{v_p}} Kv_p \xrightarrow{\overline{\overline{v}}} Kv_K.$$

Each place in the decomposition is henselian (Fact 3.1.46); by Theorem 3.1.47, the valuation $\overline{v_p}$ is of mixed characteristic $(0,p)$ and rank 1.

Step 2.1. We first show that G_{Kv_0} cannot be realised as the absolute Galois group of a field of characteristic p. To rule this out, we argue along the same lines as in Step 1.2. By Lemma 3.2.17, there exists a C_{p-1}-extension M_1 of K with the property that it admits a C_p-extension M_2 that does not embed into any C_{p^2}-extension of M_1. Let v_0' and v_0'' denote the unique prolongations of v_0 to M_1 and M_2, respectively. Since $\operatorname{char} Kv_0 = 0$, the value group v_0K is p-divisible by the same argument as in the first part of Step 1.5. In particular, $v_0'M_1$ is p-divisible, so M_2/M_1 must be unramified and M_2v_0'' is a C_p-extension of M_1v_0' that does not embed into any C_{p^2}-extension, as we could lift any such embedding to M_1 by henselianity. This is a property of the absolute Galois group $G_{M_1v_0'}$; by Lemma 3.2.15, this profinite group cannot be realised in characteristic p.

$$\begin{array}{ccc} M_2 & \xrightarrow{v_0''} & M_2v_0'' \\ {\scriptstyle C_p}\big| & & \big|{\scriptstyle C_p} \\ M_1 & \xrightarrow{v_0'} & M_1v_0' \\ {\scriptstyle C_{p-1}}\big| & & \big| \\ K & \xrightarrow{v_0} & Kv_0 \end{array}$$

At the same time, note that the absolute Galois group $G_K = D_K$ of K projects onto the absolute Galois group G_{Kv_0} of the residue field; in particular, G_K is small implies that G_{Kv_0} is small as well. Assume that $\overline{v_p}(Kv_0)$ is p-divisible. By the Transfer Lemma 3.2.18, the profinite group G_{Kv_0} can be realised as the absolute Galois group of a field of positive characteristic p. The same is true for the finite

index open subgroup $G_{M_1 v_0'}$. We arrive at a contradiction, proving that $\overline{v_p}(Kv_0)$ is not p-divisible.

Step 2.2. As G_{Kv_0} is small, $Kv_0^\times/Kv_0^{\times p}$ is finite by Lemma 3.2.8. By Pop's Lemma 3.2.10, $\overline{v_p}(Kv_0)$ is either discrete or p-divisible. We have shown the latter to be impossible. By the last part of Pop's Lemma, Kv_p is finite.

Step 3. As finite fields only admit trivial valuations, it follows that $\overline{\overline{v}}$ on Kv_p is trivial and $Kv_p = Kv_K$. In particular, the rank 1 valuation $\overline{v_p}$ is the same as the valuation $\overline{v_K}$ on Kv_0 induced by v_K.

Step 3.1. Using the finiteness of Kv_K, we can now identify the residue field Kv_K as $\mathbb{F}_p$: From Step 1.3, we know that the prime-to-p roots of unity of K are μ_{p-1}. This implies $Kv_K = \mathbb{F}_p$ by Hensel's Lemma.

Step 3.2. To prove $v_K K \equiv \mathbb{Z}$, it suffices to show that $v_K K$ has a convex subgroup $\Delta \cong \mathbb{Z}$ such that $v_K K/\Delta$ is divisible by Fact 3.3.2. By Step 2.2, the convex subgroup $\Delta := \overline{v_K}(Kv_0)$ is discrete. It remains to verify that $v_K K/\Delta \cong v_0 K$ is divisible.

We have already shown that $v_0 K$ is p-divisible in Step 2.1. We established $(v_K K : qv_K K) = q$ in Step 1.1 for all primes $q \neq p$, so the minimal positive element of Δ already generates $v_K K/qv_K K$. Therefore, $v_0 K$ is divisible.

Step 3.3. Let L again denote the unique $C_{p-1} \times C_{p-1}$-extension of K. The extension $K(\zeta_p)/K$ is abelian of degree dividing $p-1$, so it is contained in L, i.e., $\zeta_p \in L$. Write v_L for the unique extension of v_K to L, and assume v_K and v_L are normalised such that the minimal positive elements are both $1 \in \mathbb{Z}$. It follows from our analysis in Step 1.5 that L/K has ramification index $e(L/K) = p-1$ and degree of inertia $f := f(L/K) = p-1$. Therefore, the "absolute ramification index" of L is given by

$$v_L(p) = (p-1)v_K(p).$$

Additionally, write $F := \mathbb{Q}_p(\zeta_{(p-1)^2}, \zeta_p)$ for the unique $C_{p-1} \times C_{p-1}$-extensions of $\mathbb{Q}_p$. By the Degree Lemma 3.2.4 and Remark 3.2.5, we obtain

$$\begin{aligned} \dim_{\mathbb{F}_p}\left(F^\times/F^{\times p}\right) &= (p-1)^2 + 2 \\ \dim_{\mathbb{F}_p}\left(L^\times/L^{\times p}\right) &= (p-1)^2 v_K(p) + 2. \end{aligned}$$

By Kummer theory, these two quantities express the dimension of the maximal abelian Galois extension of exponent p of the unique $C_{p-1} \times C_{p-1}$-extensions of F and L. These dimensions are determined by the isomorphic absolute Galois groups G_K and $G_{\mathbb{Q}_p}$. Since they must therefore coincide, it follows that $v_K(p) = 1$ is minimal positive, as desired.

Chapter 4

Towards eliminating Case 4

After a brief review of selected statements and results from Galois cohomology, we present both classical and modern local–global principles in Section 4.1. In Section 4.2, we relate the elimination of Case 4 to Galois cohomology by reducing it to a statement about the cohomological dimension of certain fields. To approach this statement, we outline a local–global strategy and assess the applicability of the principles introduced earlier. Finally, in Section 4.3, we sketch an alternative approach to the elimination of Case 4 and compare it with the local–global method and other related work.

4.1 Local–global principles in Galois cohomology

In this section, we give an overview of local–global principles in Galois cohomology. We start by reviewing some of the key concepts of Galois cohomology in the next Section 4.1.1, culminating in the Albert–Brauer–Hasse–Noether Theorem for global fields, which will serve as a motivating example for the more general local–global principles that follow. In Section 4.1.2, we give an overview of the research on local–global principles for different cohomological degrees. This entails local–global principles for algebraic function fields over different base fields, including global fields, local fields, semi-global fields, and PAC fields. Finally, we present a general framework for extending local–global principles from algebraic function fields to not necessarily finitely generated extensions of those fields.

4.1.1 Review of Galois cohomology

We begin by reviewing some of the fundamental notions of Galois cohomology. Although our goal is to introduce the essential concepts from first principles, this

section is not intended as a comprehensive treatment. Rather, it serves to recall a selection of key ideas and themes that will be used later. For further reading, we refer the reader to Guillot's book [Gui18] for an introductory account of group and Galois cohomology with applications to class field theory; to Gille and Szamuely's text [GS06], which develops the subject with an emphasis on Brauer groups; to Serre's classical exposition [Ser97], which presents all the key concepts and notions of Galois cohomology; and to Roquette's book [Roq04], which provides a historical account of the Albert–Brauer–Hasse–Noether theorem, the archetype of cohomological local–global principles. The presentation here draws inspiration from all four sources, and we include precise references to more advanced results for the reader's convenience.

4.1.1.1 Definitions and examples

Group cohomology We start by reviewing some of the basic notions from group cohomology. Let G be a finite or profinite group, M be a discrete $\mathbb{Z}[G]$-module, and n be a non-negative integer. Then the *n-th cohomology group of G with coefficients in M* is defined as

$$H^n(G, M) \coloneqq \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

So far this is only a change of notation; we now unpack $\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M)$. We begin by fixing a *projective resolution* of $\mathbb{Z}$ (considered as a $\mathbb{Z}[G]$-module with trivial action of G), i.e., an exact sequence of the shape

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0, \tag{4.1.1}$$

where for each non-negative integer i, P_i is a *projective* $\mathbb{Z}[G]$-module. A module P is called *projective* if it has the property that any exact sequence

$$0 \to A \to B \to P \to 0$$

is split. In the case of the integers, there is a standard choice for such a projective resolution, often called the *bar resolution*.

Given a projective resolution of $\mathbb{Z}$ and another $\mathbb{Z}[G]$-module M, we can apply the functor $\mathrm{Hom}(_, M)$ to the projective resolution (4.1.1), giving rise to a *cochain complex*

$$\mathrm{Hom}(P_0, M) \xrightarrow{\delta^0} \mathrm{Hom}(P_1, M) \xrightarrow{\delta^1} \mathrm{Hom}(P_2, M) \xrightarrow{\delta^2} \cdots. \tag{4.1.2}$$

Unlike an exact sequence, a *cochain complex* does not satisfy the condition $\operatorname{im} \delta^{n-1} = \ker \delta^n$, but only the weaker condition $\operatorname{im} \delta^{n-1} \subseteq \ker \delta^n$. Hence, we can form the quotients $\ker \delta^n / \operatorname{im} \delta^{n-1}$, which measure the extent to which (4.1.2) fails to be an exact

sequence. This quotient is precisely the definition of $\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M) \coloneqq \ker \delta^n / \operatorname{im} \delta^{n-1}$ (it is part of the theory that the choice of the projective resolution of $\mathbb{Z}$ does not matter), with $\mathrm{Ext}^0_{\mathbb{Z}[G]}(\mathbb{Z}, M) \coloneqq \ker \delta^0$ for $n = 0$. Analogously, it is possible to define $\mathrm{Ext}^n_{\mathbb{Z}[G]}(N, M)$ for an arbitrary $\mathbb{Z}[G]$-module N by starting with a projective resolution of N instead of $\mathbb{Z}$.

The reason for choosing a specific projective resolution of $\mathbb{Z}$ is that it gives an explicit way of describing the maps δ^i, which yields explicit descriptions of $\ker \delta^i$ and $\operatorname{im} \delta^i$ as well. Without actually defining the bar resolution of $\mathbb{Z}$, let us give the description of $H^n(G, M)$ that follows from it.

We define the group of *inhomogeneous cochains* $C^n(G, M)$ as the group whose elements are the continuous[1] maps (of sets!)

$$f : G^n \to M.$$

We then define the maps

$$d^n : C^n(G, M) \to C^{n+1}(G, M)$$

by

$$\begin{aligned}(d^n(f))(\sigma_1, \dots, \sigma_{n+1}) =& \sigma_1 \cdot f(\sigma_2, \dots, \sigma_{n+1}) \\ &+ \sum_{i=1}^{n} (-1)^i f(\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \sigma_{i+2}, \dots, \sigma_{n+1}) \\ &+ (-1)^{n+1} f(\sigma_1, \dots, \sigma_n).\end{aligned}$$

For $n = 0$, $C^0(G, M)$ can be identified with M itself, so the definition becomes simply

$$(d^0(m))(\sigma_1) = \sigma_1 \cdot m - m.$$

It is an elementary exercise to show that

$$H^n(G, M) = \ker \delta^n / \operatorname{im} \delta^{n-1} \cong \ker d^n / \operatorname{im} d^{n-1}$$

(and $H^0(G, M) = \ker \delta^0 \cong \ker d^0$ for $n = 0$) directly from the definition of the bar resolution. In fact, Serre [Ser97, I.§2] uses the d^n directly to introduce group cohomology. However, since this definition may appear somewhat ad hoc, we decided to at least include an indication of where this sequence originates from.

[1] Note that continuity is only relevant when G is an infinite profinite group, as finite groups are endowed with the discrete topology, so every such map is automatically continuous.

Exact sequences in cohomology We will encounter several exact sequences of cohomology groups. They generally fall into one of two categories: Either the modules change while the groups stay the same, or the groups change while the modules remain fixed.

The first phenomenon is the more elementary one. In fact, most sequences of this type originate from a short exact sequence of $\mathbb{Z}[G]$-modules.

Proposition 4.1.1. *Let*

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of $\mathbb{Z}[G]$-modules. Then there is an associated long exact sequence in cohomology*:*

$$\begin{aligned} 0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \\ \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \cdots \end{aligned}$$

The second type of cohomological exact sequences generally find their origin in *spectral sequences*, which relate the cohomology of a group G to the cohomology of H and G/H, where H denotes a closed normal subgroup of G. Spectral sequences are not required for the understanding of our discussion below, so we refrain from introducing them here (we refer the interested reader to [NSW08, Chapter II]). Instead, we only highlight the following two consequences that can be deduced from the theory of spectral sequences.

Proposition 4.1.2 ([NSW08, Corollary 2.4.2])**.** *Let H be a closed normal subgroup of a profinite group G, and M be a G-module. If $H^m(H, M) = 0$ for all $m > 0$, then*

$$H^n(G/H, M^H) \cong H^n(G, M).$$

Proposition 4.1.3 (Five Term Exact Sequence (cf. [NSW08, Proposition 1.6.7]))**.** *Let H be a closed normal subgroup of a profinite group G, and M be a G-module. For $n > 0$, assume $H^i(H, M) = 0$ for $1 \leq i \leq n-1$ (vacuously true if $n = 1$). Then there is an exact sequence*

$$\begin{aligned} 0 \to H^n(G/H, M^H) \xrightarrow{inf} H^n(G, M) \xrightarrow{res} H^n(H, M)^{G/H} \\ \xrightarrow{tg} H^{n+1}(G/H, M^H) \xrightarrow{inf} H^{n+1}(G, M), \end{aligned}$$

which is called the five-term exact sequence in degree n.

Cohomology in small degrees To get a better feeling for the cohomology groups just introduced, let us describe $H^n(G, M)$ for small values of n.

For $n = 0$, we simply get the elements of M that are fixed by the action of G:

$$H^0(G, M) = \ker d^0 = \{m \in M : \sigma \cdot m - m = 0\} = M^G$$

For $n = 1$, we see

$$\begin{aligned} \ker d^1 &= \{f : G \to M : f(\sigma\tau) = f(\sigma) + \sigma f(\tau)\}, \text{ and} \\ \operatorname{im} d^0 &= \{f : G \to M : \exists m\, f(\sigma) = \sigma m - m\}. \end{aligned}$$

The elements of $\ker d^1$ are also known as (continuous) *crossed homomorphisms*, whereas the elements of $\operatorname{im} d^0$ are sometimes called *trivial homomorphisms*. In particular, if M has trivial G-action, then $\ker d^1$ becomes the group of all continuous (regular) homomorphisms $f : G \to M$ and $\operatorname{im} d^0$ becomes trivial, so $H^1(G, M) = \operatorname{Hom}(G, M)$ in this case.

An important result concerning the first cohomology groups is *Hilbert's Theorem 90* (commonly abbreviated as *Hilbert 90*). In stating this result, we finally enter the realm of *Galois cohomology*. This just means that we consider the case when $G = \operatorname{Gal}(L/K)$ is the Galois group of some Galois extension of fields L/K, and M is a subfield of L that G acts on. Hilbert 90 concerns the vanishing of the groups $H^1(\operatorname{Gal}(L/K), L^\times)$.

Theorem 4.1.4. *Let L/K be a (not necessarily finite) Galois extension of fields. Then*

$$H^1(\operatorname{Gal}(L/K), L^\times) = 0.$$

At first glance, this seems to clash with Theorem 3.2.12 from Section 3.2.3. In fact, the multiplicative form of Theorem 3.2.12 is Hilbert's historical statement, which looks completely different from Theorem 4.1.4. To see that the cohomological formulation actually implies Hilbert's historical statement, we note that in the special case where L/K is a finite cyclic extension and $G = \operatorname{Gal}(L/K)$ is generated by some element σ, we can identify elements $f \in \operatorname{im} d^0$ with their image $f(\sigma)$ since the values of $f(\sigma^i)$ are then determined via the following recursive relation (here we switch to multiplicative notation as $L^\times$ is a multiplicative group):

$$f(\sigma^i) = \frac{\sigma^i(m)}{m} = \frac{\sigma(m)}{m} \cdot \sigma\left(\frac{\sigma^{i-1}(m)}{m}\right) = f(\sigma) \cdot \sigma(f(\sigma^{i-1}))$$

In other words, we can identify $\operatorname{im} d^0$ with the group $\{\frac{\sigma(m)}{m} : m \in L^\times\}$. Similarly, using that $\sigma^{|G|} = 1$, we can identify

$$\ker d^1 = \left\{ x : \prod_{i=0}^{|G|-1} \sigma^i(x) = 1 \right\} = \{x : N_{L/K}(x) = 1\}.$$

The vanishing of $H^1(\mathrm{Gal}(L/K), L^\times)$ now expresses exactly that every element of $\ker d^1$ is also an element of $\operatorname{im} d^0$, which is precisely the content of Hilbert's original Theorem 90.

For $n = 2$, we could write out the expressions for $\ker d^2$ and $\operatorname{im} d^1$ as we did for $n = 0$ and $n = 1$. In that case, an elementary (but slightly tedious) analysis would reveal that the elements of $H^2(G, M)$ correspond exactly to equivalence classes $[\Gamma]$ of *extensions of G by M*. Γ is an *extension of G by M* if it fits into a short exact sequence

$$0 \to M \to \Gamma \to G \to 1.$$

Next, in analogy with our discussion of Hilbert 90 for $n = 1$, let us explicitly compute the cohomology groups $H^2(\mathrm{Gal}(L/K), L^\times)$ for finite cyclic extensions L/K. Let σ denote a generator of $G = \mathrm{Gal}(L/K)$. While we could calculate $H^2(\mathrm{Gal}(L/K), L^\times)$ directly from the descriptions of $\ker d^2$ and $\operatorname{im} d^1$ induced by the bar resolution, we can utilise a much simpler projective resolution of the $\mathbb{Z}[G]$-module $\mathbb{Z}$ when G is finite cyclic. Since $\mathbb{Z}[G]$ is free (and thus projective), a simple calculation (cf. [Gui18, Example 9.13]) verifies that we have the exact sequence

$$\cdots \xrightarrow{\cdot N} \mathbb{Z}[G] \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\cdot N} \mathbb{Z}[G] \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0,$$

where $N \coloneqq \sum_{i=0}^{|G|-1} \sigma^i$, and ϵ denotes evaluation at $\sigma = 1$.

Applying the functor $\mathrm{Hom}(_, L^\times)$ yields a cochain complex consisting of the objects $\mathrm{Hom}(\mathbb{Z}[G], L^\times)$. As before, any $f \in \mathrm{Hom}(\mathbb{Z}[G], L^\times)$ is fully determined by $f(1) \in L^\times$, allowing us to identify $\mathrm{Hom}(\mathbb{Z}[G], L^\times)$ with $L^\times$. The resulting cochain complex then takes the form

$$L^\times \xrightarrow{\delta^0(x)=\frac{\sigma(x)}{x}} L^\times \xrightarrow{\delta^1(x)=N_{L/K}(x)} L^\times \xrightarrow{\delta^2(x)=\frac{\sigma(x)}{x}} L^\times \xrightarrow{\delta^3(x)=N_{L/K}(x)} \cdots.$$

From this complex, we immediately recover the expression for $H^1(\mathrm{Gal}(L/K), L^\times)$ that we discovered in our discussion of Hilbert 90. Indeed, more generally, we see that the expression is identical for all odd degrees $H^{2k+1}(\mathrm{Gal}(L/K), L^\times)$. For $H^2(\mathrm{Gal}(L/K), L^\times)$ (and consequently all positive even degrees), we obtain

$$H^2(\mathrm{Gal}(L/K), L^\times) \cong \ker \delta^2 / \operatorname{im} \delta^1 = K^\times / N_{L/K}(L^\times). \tag{4.1.3}$$

When L/K is a general algebraic field extension, the most important feature of $H^2(\mathrm{Gal}(L/K), L^\times)$ is its connection with *Brauer groups*. We quickly recall the relevant notions and concepts.

Definition 4.1.5 (central simple K-algebra)**.** Let K be a field and A be a ring. The *center* of A is defined as

$$\mathcal{Z}(A) \coloneqq \{z \in A : xz = zx \text{ for all } x \in A\}.$$

A is a *K-algebra* if it comes equipped with a homomorphism $K \to \mathcal{Z}(A)$, giving it the structure of a K-vector space.

A K-algebra A is called *central* if $[A : K]$ is finite and $\mathcal{Z}(A) \cong K$. A is called *simple* if it contains no proper non-trivial two-sided ideals.

Definition 4.1.6 (division algebra)**.** A *division algebra* (or *skewfield*) is a ring R such that every non-zero $x \in R$ has a two-sided inverse $x^{-1} \in R$.

In particular, a commutative division algebra is just a field. Another important class of division algebras are *cyclic algebras*.

Definition 4.1.7 (cyclic algebra)**.** Let L/K be a cyclic Galois extension of degree n, and let σ be a generator of $\mathrm{Gal}(L/K)$. For $b \in K^\times$, the *cyclic algebra* $(L/K, \sigma, b)$ (or just (L, b) when K and σ are understood from the context) is the K-algebra generated by L and some element u, subject to the relations

$$u^n = b, \text{ and } xu = u\sigma(x) \text{ for all } x \in L.$$

In particular, when $n = 2$, $L = K(\sqrt{a})/K$ for some $a \in K^\times$ and $\sigma(\sqrt{a}) = -\sqrt{a}$, so $(L/K, \sigma, b)$ coincides with the *(generalised)*[2] *quaternion algebra* (a, b).

The following fundamental result provides a characterisation of central simple K-algebras via division algebras, and simultaneously serves as a motivation for the notion of *Brauer equivalence*.

Proposition 4.1.8. *Let A be a K-algebra. The following are equivalent:*

(i) A is a central simple K-algebra;

(ii) $A \cong M_n(F)$ for some division algebra F with $\mathcal{Z}(F) = K$ and $[F : K]$ finite, where $M_n(F)$ denotes the ring of $n \times n$-matrices with entries in F.

[2]For $K = \mathbb{R}$, $L = \mathbb{C}$, and $a = b = -1$, we recover the classical *Hamiltonian quaternions*, with u corresponding to j.

Definition 4.1.9 (Brauer equivalence)**.** Two central simple K-algebras A and A' are *Brauer equivalent* if $A \cong M_n(F)$ and $A' \cong M_m(F)$ for some division algebra F with $\mathcal{Z}(F) = K$ and positive integers n and m.

A simple exercise shows that for a division algebra F and a positive integer n, $M_n(F)$ is a division algebra if and only if $n = 1$. Hence, every Brauer-equivalence class contains exactly one division algebra up to isomorphism.

Definition 4.1.10. The *Brauer group* $\mathrm{Br}(K)$ of K is the set of all equivalence classes of central simple K-algebras, endowed with the group operation

$$[A] \cdot [A'] \coloneqq [A \otimes_K A']$$

and the neutral element $[K]$.

Of course, it remains to verify that the above operation actually gives rise to a group structure on the set of all equivalence classes of central simple K-algebras, but we will not do so here.

Next, let us see what happens to the Brauer group $\mathrm{Br}(K)$ under field extensions L/K. It is not hard to show that the map

$$\begin{aligned} \iota_{L/K} : \mathrm{Br}(K) &\to \mathrm{Br}(L) \\ [A] &\mapsto [A \otimes_K L] \end{aligned}$$

is a well-defined group homomorphism. We denote $\mathrm{Br}(L/K) \coloneqq \ker \iota_{L/K}$ and call it the *relative Brauer group* of the extension L/K. If $[A] \in \mathrm{Br}(L/K)$ for some central simple K-algebra A, we say that A *splits* in L. For example, if $\widetilde{K}$ denotes an algebraic closure of K, it is not difficult to see that $\mathrm{Br}(\widetilde{K})$ is trivial, so every central simple K-algebra splits in $\widetilde{K}$.

We can now relate Brauer groups and relative Brauer groups to the second cohomology group.

Proposition 4.1.11. *Let L/K be a finite Galois extension of fields. There is a group isomorphism*

$$H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathrm{Br}(L/K).$$

Taking colimits over all finite Galois extensions, this induces an isomorphism

$$H^2(G_K, (K^{\mathrm{sep}})^\times) \cong \mathrm{Br}(K).$$

Remark 4.1.12. In the special case that L/K is finite cyclic, Proposition 4.1.11 together with (4.1.3) gives rise to an isomorphism

$$K^\times/N_{L/K}(L^\times) \cong H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathrm{Br}(L/K).$$

An analysis of all the maps involved reveals that (cf. [GS06, Corollary 4.7.4]) this isomorphism is induced by the map $K^\times \to \mathrm{Br}(L/K)$ mapping $b \in K^\times$ to the cyclic algebra (L, b). In particular, this immediately gives rise to the following interesting splitting criterion for cyclic algebras.

Lemma 4.1.13. *Let L/K be a cyclic Galois extension with $b \in K^\times$. Then (L, b) splits if and only if $b \in N_{L/K}(L^\times)$.*

Finally, Proposition 4.1.11 together with (4.1.3) also allows us to give some explicit examples of Brauer groups:

Example 4.1.14.

(i) $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \cong C_2$, where $\mathbb{H}$ denotes the Hamiltonian quaternions. This follows immediately from (4.1.3) since $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) = \mathbb{R}_{>0}$, and $\mathbb{R}^\times/\mathbb{R}_{>0} \cong C_2$.

(ii) $\mathrm{Br}(\mathbb{F}_q) = 0$ for every finite field $\mathbb{F}_q$, a result known as *Wedderburn's little theorem*. Taking colimits, it is enough to show that $\mathrm{Br}(F/\mathbb{F}_q) = 0$ for all finite extensions $F/\mathbb{F}_q$. We leave it as an exercise to the reader to use (4.1.3) to establish this (cf. also [Gui18, Example 7.24]).

(iii) $\mathrm{Br}(F) = \mathbb{Q}/\mathbb{Z}$ for p-adic fields F, i.e., finite extensions of $\mathbb{Q}_p$ for some prime p. This is a fundamental result in local class field theory.

The groups $\mathbf{H^n(G_K, \mathbb{Z}/m\mathbb{Z}(i))}$ Finally, we introduce the cohomology groups $H^n(G_K, \mathbb{Z}/m\mathbb{Z}(i))$, which play a central role in the theory of Galois cohomology and will resurface multiple times in this chapter.

For m coprime[3] to $\mathrm{char}\, K$, $\mathbb{Z}/m\mathbb{Z}(i) \coloneqq \mu_m^{\otimes i}$ denotes the *i-th Tate twist* of $\mathbb{Z}/m\mathbb{Z}$. In other words, $\mathbb{Z}/m\mathbb{Z}(i)$ is equal to $\mathbb{Z}/m\mathbb{Z}$ as an abelian group, but is endowed with a twisted action induced by the cyclotomic character [NSW08, Definition 7.3.6]. In particular, in case $\mu_m \subseteq K$,

$$H^n(G_K, \mathbb{Z}/m\mathbb{Z}(i)) \cong H^n(G_K, \mathbb{Z}/m\mathbb{Z}) \cong H^n(G_K, \mu_m).$$

[3] In fact, there is a way to extend the definition of $\mathbb{Z}/m\mathbb{Z}(i)$ to the case when m is not coprime to $\mathrm{char}\, K$ due to Kato, but these groups are of no concern to us.

To get a better feeling for these groups, we compute some examples for small values of n, starting with the case $i = 1$ (i.e., $\mathbb{Z}/m\mathbb{Z}(1) = \mu_m$).

When $n = 0$, $H^0(G_K, \mu_m)$ is simply $\mu_m(K)$, the group of m-th roots of unity contained in K:

$$H^0(G_K, \mu_m) = (\mu_m)^{G_K} = \mu_m(K).$$

To compute $H^n(G_K, \mu_m)$ for $n = 1, 2$, we rely on the *Kummer exact sequence*

$$1 \to \mu_m \to \widetilde{K}^\times \xrightarrow{x \mapsto x^m} \widetilde{K}^\times \to 1. \tag{4.1.4}$$

By Proposition 4.1.1, the Kummer exact sequence induces the following segment of the long exact sequence in cohomology:

$$H^0(G_K, \widetilde{K}^\times) \xrightarrow{x \mapsto x^m} H^0(G_K, \widetilde{K}^\times) \to H^1(G_K, \mu_m) \to H^1(G_K, \widetilde{K}^\times).$$

By Hilbert 90 (Theorem 4.1.4), we see that $H^1(G_K, \widetilde{K}^\times) = 0$. Together with our description of cohomology groups in degree 0, the exact sequence thus simplifies to

$$K^\times \xrightarrow{x \mapsto x^m} K^\times \to H^1(G_K, \mu_m) \to 0,$$

from which we immediately see that $H^1(G_K, \mu_m) \cong K^\times / K^{\times m}$.

For $n = 2$, the group recovers the m-torsion part ${}_m\mathrm{Br}(K)$ of the Brauer group (cf. [Gui18, Theorem 11.7], [GS06, Corollary 4.4.9]).

Proposition 4.1.15. *Let m be a positive integer that is prime to $\operatorname{char} K$. Then*

$$H^2(G_K, \mu_m) \cong {}_m\mathrm{Br}(K).$$

Proof. We consider again a segment of the long exact sequence associated to the Kummer exact sequence (4.1.4):

$$H^1(G_K, \widetilde{K}^\times) \to H^2(G_K, \mu_m) \to H^2(G_K, \widetilde{K}^\times) \xrightarrow{x \mapsto x^m} H^2(G_K, \widetilde{K}^\times)$$

Hilbert 90, together with Proposition 4.1.11, then implies

$$H^2(G_K, \mu_m) = \ker(x \mapsto x^m) \cong {}_m\mathrm{Br}(K). \qquad \square$$

By letting $m = p^i$ for $p \neq \operatorname{char} K$ and passing to the limit $i \to \infty$, we get an alternative description of the p-primary part $\mathrm{Br}(K)(p)$ of the Brauer group $\mathrm{Br}(K)$.

Corollary 4.1.16. *Let K be a field and $p \neq \operatorname{char} K$ be a prime. Then*

$$\mathrm{Br}(K)(p) \cong H^2(G_K, \mu_{p^\infty}).$$

Let us return to the groups $H^n(G_K, \mathbb{Z}/m\mathbb{Z}(i))$ once more, and consider the case $i = n$.

When $n = i = 0$, $\mathbb{Z}/m\mathbb{Z}(0)$ is the G_K-module $\mathbb{Z}/m\mathbb{Z}$ endowed with the trivial action, so

$$H^0(G_K, \mathbb{Z}/m\mathbb{Z}(0)) \cong (\mathbb{Z}/m\mathbb{Z})^{G_K} = \mathbb{Z}/m\mathbb{Z}.$$

For $n = i = 1$, we saw above that

$$H^1(G_K, \mathbb{Z}/m\mathbb{Z}(1)) \cong H^1(G_K, \mu_m) \cong K^\times/K^{\times m}.$$

Surprisingly, there is an explicit description of the groups $H^n(G_K, \mathbb{Z}/m\mathbb{Z}(n))$ for all n and $(m, \operatorname{char} K) = 1$. This result is a very deep theorem, known for a long time as the *Bloch-Kato Conjecture*. It was finally proved by Voevodsky [Voe11], relying on machinery developed by Rost. Nowadays, it is usually called the *norm residue isomorphism theorem*.

Before we state the theorem, we briefly recall the definition of *Milnor K-groups*.

Definition 4.1.17 (Milnor K-group)**.** For a field F, the *n-th Milnor K-group*, denoted $K_n^M(F)$, is the quotient of the n-fold tensor product $F^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^\times$ divided by the subgroup generated by elements of the form $a_1 \otimes \cdots \otimes a_n$ with $a_i + a_j = 1$ for some $1 \leq i < j \leq n$. In particular, $K_1^M(F) \coloneqq F^\times$; by convention, also $K_0^M(F) \coloneqq \mathbb{Z}$. The equivalence classes of elements $a_1 \otimes \cdots \otimes a_n$ in $K_n^M(F)$ are denoted by $\{a_1, \ldots, a_n\}$ and referred to as *symbols*.

Theorem 4.1.18 (Norm residue isomorphism)**.** *Let F be a field and m be a positive integer with $(m, \operatorname{char} F) = 1$. There is an isomorphism*

$$K_n^M(F)/m \cong H^n(G_F, \mathbb{Z}/m\mathbb{Z}(n)).$$

The reader will quickly verify that this theorem agrees with our calculations above for $n = 0, 1$. For $n = 2$, the theorem is already significantly harder to prove. In fact, it was originally established by Merkurjev and Suslin [MS83] and is the central result proved in Gille and Szamuely's book [GS06].

4.1.1.2 Cohomological dimension

Definition and basic properties To measure the cohomological complexity of a group G, there is the notion of the *cohomological dimension of G*, denoted by $\operatorname{cd} G$.

It is defined in terms of the *p-th cohomological dimension* $\mathrm{cd}_p G$:

$$\mathrm{cd}_p(G) \coloneqq \inf\{n : H^q(G, M)(p) = 0 \ \forall q > n, \text{ discrete } \textbf{torsion } \mathbb{Z}[G]\text{-modules } M\};$$
$$\mathrm{cd}(G) \coloneqq \sup_p \mathrm{cd}_p(G),$$

where $A(p)$ denotes the p-primary component of the group A, and we let ∞ be the infimum of the empty set. A related notation is that of the *strict cohomological dimension of* G, denoted by $\mathrm{scd}\, G$. The definition is analogous to the one above, except that we drop the torsion assumption in the definition of $\mathrm{scd}_p(G)$.

Cohomological and strict cohomological dimension are related in a fundamental way [Ser97, I.§3, Proposition 13]:

Proposition 4.1.19.

$$\mathrm{cd}_p G \leq \mathrm{scd}_p G \leq \mathrm{cd}_p G + 1.$$

In particular,

$$\mathrm{cd}\, G \leq \mathrm{scd}\, G \leq \mathrm{cd}\, G + 1.$$

Most of the time, we will work with the (non-strict) cohomological dimension. Based on the theory of finite p-groups, it is possible to give the following characterisation [Ser97, I.§4, Proposition 21']:

Proposition 4.1.20. *Let G be a profinite group, p be a prime, and n be a non-negative integer. The following are equivalent:*

(i) $\mathrm{cd}_p G \leq n$;

(ii) $H^{n+1}(H, \mathbb{Z}/p\mathbb{Z}) = 0$ *for every closed subgroup H of G;*

(iii) $H^{n+1}(H, \mathbb{Z}/p\mathbb{Z}) = 0$ *for every open subgroup H of G.*

Here, $\mathbb{Z}/p\mathbb{Z}$ is endowed with the trivial G-action in (ii) and (iii).

Cohomology under field extensions The cohomological dimension of Galois groups behaves in a natural way under field extensions [Ser97, II.§4.1, Propositions 10 & 11]:

Proposition 4.1.21. *Let L/K be an algebraic field extension. Then $\mathrm{cd}_p G_L \leq \mathrm{cd}_p G_K$. Moreover, if the index $[L : K]$ is prime to p, then $\mathrm{cd}_p G_L = \mathrm{cd}_p G_K$.*

Proposition 4.1.22. *Let L/K be a field extension of relative transcendence degree $n < \omega$. Then $\mathrm{cd}_p G_L \leq \mathrm{cd}_p G_K + n$. Moreover, if L/K is finitely generated and $p \neq \mathrm{char}\, K$, $\mathrm{cd}_p G_L = \mathrm{cd}_p G_K + n$.*

Cohomology of valued fields Next, we highlight some results on the cohomological dimension of valued fields. The following is a classical result for local fields [Ser97, II.§4.3, Proposition 12], with a proof analogous to that of the previous Proposition 4.1.22.

Proposition 4.1.23. *Let (K, v) be a complete valued field with respect to a discrete rank-1 valuation v, and let $p \neq \operatorname{char} Kv$ be a prime. If $\operatorname{cd}_p G_K < \infty$, then*

$$\operatorname{cd}_p G_K = 1 + \operatorname{cd}_p G_{Kv}.$$

The following is an important generalisation to arbitrary henselian valued fields [MT85, Theorem 3].

Theorem 4.1.24. *Let (K, v) be a henselian valued field, and $p \neq \operatorname{char} Kv$ be a prime. If $\operatorname{cd}_p(G_K) < \infty$, then*

$$\operatorname{cd}_p G_K = \operatorname{cd}_p G_{Kv} + \dim_{\mathbb{F}_p} vK/pvK.$$

Finally, we mention the following result of Pop [Pop88, Theorem 2.4], which generalises classical results on the Galois cohomology of discretely valued fields originating in Witt's work [Wit37].

Proposition 4.1.25. *Let (E, v) be a henselian valued field with inertia field E_t (in some fixed separable closure). Then the following sequence is exact:*

$$0 \to \operatorname{Br}(Ev) \cong H^2(G_{Ev}, \widetilde{Ev}^\times) \to \operatorname{Br}(E_t/E) \cong H^2(G_{Ev}, E_t^\times) \to H^2(G_{Ev}, vE) \to 0.$$

Fields with projective Galois group Of particular importance to us are fields K whose absolute Galois group is *projective*, a concept that is defined analogously to the projectivity of modules.

Definition 4.1.26. A profinite group G is called *projective* if every short exact sequence

$$1 \to G' \to H \to G \to 1$$

of profinite groups is split via a continuous section.

As it turns out, projective profinite groups are precisely the profinite groups of cohomological dimension at most 1 [Ser97, I.§5, Corollary 2].

Proposition 4.1.27. *Let G be a profinite group. The following are equivalent:*

(i) G is projective;

(ii) $\operatorname{cd} G \leq 1$.

In this section, we will explore some of the equivalent ways in which fields K with a projective absolute Galois group can be characterised. For the p-th cohomological dimension of G_K, we distinguish between the cases $p = \operatorname{char} K$ and $p \neq \operatorname{char} K$. In the former case, $\operatorname{cd}_p G_K \leq 1$ is always satisfied [Ser97, II.§2.2, Proposition 3].

Proposition 4.1.28. *Let K be a field and $p = \operatorname{char} K$. Then $\operatorname{cd}_p G_K \leq 1$.*

For all other cases, there is the following result, which characterises $\operatorname{cd}_p G_K \leq 1$ in two alternative algebraic ways via Brauer groups or norm maps, respectively. [GS06, Theorem 6.1.8].

Proposition 4.1.29. *Let K be a field and $p \neq \operatorname{char} K$ be a prime. The following are equivalent:*

(i) $\operatorname{cd}_p G_K \leq 1$*;*

(ii) for all separable extensions L/K, $\operatorname{Br}(L)(p) = 0$*;*

(iii) for all separable extensions L/K and Galois extensions E/L with $\operatorname{Gal}(E/L) \cong C_p$*, the norm map $N_{E/L}$ is surjective.*

Proposition 4.1.29 continues to hold true if we restrict the separable extensions in items (ii), (iii) to *finite* separable extensions [Ser97, II.§3, Proof of Proposition 5].

The above results allow us to deduce the following characterisation of projective absolute Galois groups.

Proposition 4.1.30. *Let K be a field of characteristic p (where we allow $p = 0$). Then the following are equivalent:*

(i) G_K is projective;

(ii) $\operatorname{cd}_q G_K \leq 1$ *for all primes $q \neq p$;*

(iii) $H^2(G_L, \mathbb{Z}/q\mathbb{Z}) = 0$ *for all finite Galois extensions L/K and all primes $q \neq p$;*

(iv) $\operatorname{Br}(L)(q) = 0$ *for all finite separable extensions L/K and primes $q \neq p$;*

(v) $N_{E/L}$ is surjective for all finite separable extensions L/K and Galois extensions E/L with $\operatorname{Gal}(E/L) \cong C_q$ *for all primes $q \neq p$.*

Proof. For the equivalence of (i) and (ii), note that projectivity of G_K is equivalent to $\operatorname{cd} G_K \leq 1$ by Proposition 4.1.27. The equivalence then follows from Proposition 4.1.29 and Proposition 4.1.28.

The equivalence of (ii) and (iii) follows from Proposition 4.1.20, noting that under the infinite Galois correspondence, open subgroups of the absolute Galois group correspond to finite Galois extensions.

The equivalence of (ii), (iv), and (v) follows directly from Proposition 4.1.29 and the remark following it. □

It is important to note that projectivity of G_K is not quite the same as the vanishing of $\operatorname{Br}(L)$ for all separable extensions L/K because G_K can be projective while $\operatorname{Br}(L)(p) \neq 0$. Serre [Ser97, II.§3, Definition] calls fields with this stronger property *fields of dimension* ≤ 1. However, for our applications, we are mainly interested in the projectivity of G_K, so we will not adopt this notion here.

4.1.1.3 The Albert–Brauer–Hasse–Noether Theorem

The Albert–Brauer–Hasse–Noether Theorem from number theory is the prototype of cohomological local–global principles. In this section, we motivate this result by relating it to other classical local–global theorems.

Perhaps the most famous local–global theorem is the *Hasse–Minkowski Theorem*.

Theorem 4.1.31 (Hasse–Minkowski Theorem)**.** *Let $f(\mathbf{x})$ be a* quadratic form *(i.e., a homogeneous polynomial of degree 2) with coefficients in a number field K. Then f has a non-trivial root if and only if f has a non-trivial root in all completions K_v of K.*

It is well-known that the Hasse–Minkowski Theorem fails for homogeneous polynomials of degree $n > 2$. The cubic

$$3x^3 + 4y^3 + 5z^3 = 0$$

is a famous counterexample due to Selmer [Sel51] that has non-trivial solutions in $\mathbb{R}$ and all $\mathbb{Q}_p$ but none over $\mathbb{Q}$.

While the Hasse–Minkowski local–global theorem does not generalise to higher degrees, there is the following local–global principle of Hasse [Has31] that works for polynomials of arbitrary degree coming from certain norms:

Theorem 4.1.32 (Hasse Norm Theorem)**.** *Let L/K be a cyclic extension of number fields and $a \in K^\times$. If a is a norm for all completions L_v/K_v, then a is a norm in L/K.*

In light of Lemma 4.1.13, we can reformulate the Hasse Norm Theorem in terms of the splitting of cyclic algebras as follows:

Theorem 4.1.33. *Let L/K be a cyclic extension of number fields and $a \in K^\times$. If (L_v, a) splits for all completions L_v/K_v, then (L, a) splits as well.*

In their celebrated paper [BNH32], published in a special volume of Crelle's Journal dedicated to Hensel's 70th birthday, Brauer, Hasse and Noether enthusiastically proved the following result, which they call a *Hauptsatz in der Theorie der Algebren* (English: "a main theorem in the theory of algebras").

Theorem 4.1.34. *Every division algebra over a number field is cyclic.*

Combining Brauer, Hasse, and Noether's Main Theorem and Theorem 4.1.33, we get the following striking consequence, which is nowadays most commonly referred to as the *Albert–Brauer–Hasse–Noether Theorem*, including Albert, who discovered parts of the theorem independently.

Theorem 4.1.35 (Albert–Brauer–Hasse–Noether Theorem)**.** *Let K be a number field. The natural group homomorphism*

$$\mathrm{Br}(K) \to \prod_v \mathrm{Br}(K_v)$$

is injective, where v runs over all valuations and Archimedean norms on K, and K_v denotes the completion of K with respect to v.

The reduction map in the Albert–Brauer–Hasse–Noether Theorem is also known to be injective when K is a *global function field* (i.e., a finite extension of $\mathbb{F}_p(t)$) and hence for all *global fields*. In fact, we will obtain the Albert–Brauer–Hasse–Noether Theorem for global function fields as a corollary of our considerations in the next section.

Finally, as a stepping stone towards more general modern local–global principles, let us highlight the following immediate consequence of the Albert–Brauer–Hasse–Noether Theorem for the n-torsion subgroups (see Proposition 4.1.15):

Theorem 4.1.36. *Let K be a number field. The natural group homomorphism*

$$H^2(G_K, \mu_n) \to \prod_v H^2(G_{K_v}, \mu_n)$$

is injective, where v runs over all valuations and Archimedean norms on K, and K_v denotes the completion of K with respect to v.

4.1.2 Modern cohomological local–global principles

A lot of contemporary research has been focused on generalising the Albert–Brauer–Hasse–Noether local–global principle for the Brauer group of global fields to more general classes of fields. However, as we will see below, for more general fields K, we cannot expect a local–global principle to hold for the full Brauer group $\mathrm{Br}(K) \cong H^2(G_K, K^\times)$. Instead, modern local–global principles are concerned with arithmetically meaningful subgroups of $\mathrm{Br}(K)$, or more generally, cohomology groups $H^n(G_K, M)$ for a positive integer n and meaningful G_K-modules M. For instance, in the case $n = 2$, Propositions 4.1.30, 4.1.15, Corollary 4.1.16, and Theorem 4.1.36 indicate that the primary components $\mathrm{Br}(K)(p)$ or torsion parts ${}_n\mathrm{Br}(K)$ of $\mathrm{Br}(K)$ provide instances of such arithmetically interesting subgroups.

Generally speaking, given a field K and a G_K-module M, cohomological local–global principles express the injectivity of the reduction map

$$H^n(G_K, M) \to \prod_{v \in V} H^n(G_{K_v}, M_v) \tag{4.1.5}$$

for a suitable set of valuations V of K and a positive integer n, where K_v denotes the completion[4] of K with respect to v, and M_v a corresponding K_v-module.

In the following, we give an overview of the state of research on these local–global principles. As we will see later, our main interest in cohomological local–global principles stems from the fact that we are looking to prove that $F = \mathbb{F}_p(s,t)^{\mathrm{solv}}$, the solvable closure of $\mathbb{F}_p(s,t)$, has a projective absolute Galois group, so the presentation of the results below is biased towards results that are most relevant in potentially resolving this question.

4.1.2.1 Degree $n = 1$

Before we dive into cohomological local–global principles for $n = 1$, we note that it is possible to extend the definition of $H^1(G, A)$ from $\mathbb{Z}[G]$-modules A to *G-groups* A. A G-group is a discrete topological space with a continuous G-action and a

[4]Depending on the community and tradition, some authors use henselisations K_v^h and M_v^h instead of the completions in the statements of their local–global principles. Most of the time, especially when v is a discrete valuation, this distinction will not matter to us and completion and henselisation can be used interchangeably. To avoid confusion, we decided to generally follow the conventions of the papers we are referring to.

(not necessarily abelian) group structure that is compatible with G. The definition of $H^1(G, A)$ can be generalised to G-groups in a natural way, but it will lose its group structure in the process, instead becoming a pointed *cohomology set* with a distinguished element corresponding to the class of trivial homomorphisms.

The above construction gives meaning to $H^1(G_K, A)$ for general algebraic groups A over a field K. By a classical fact due to Lang and Tate [LT58, Proposition 4], the elements of $H^1(G_K, A)$ then correspond canonically to K-isomorphism classes of *principal homogeneous spaces* (or *torsors*) under A, i.e., varieties V over K with a simply transitive right action of A on V such that the map from $V \times V$ to A which maps (x, y) to the unique element $a \in A$ with $x = a(y)$ is rational over K. This correspondence maps the isomorphism class of a principal homogeneous space V to the trivial element of $H^1(G_K, A)$ if and only if V has a K-rational point. We refer the reader to [Ser97, I.§5.1, §2] or the original paper [LT58] for all the details. The key point for our purposes is that, through this perspective, the study of the cohomology sets (or groups, when A is abelian) $H^1(G_K, A)$ naturally becomes a geometric problem.

The following classical theorem of Lang [Lan56] provides a fundamental vanishing result for $H^1(G_K, A)$ when K is finite.

Theorem 4.1.37. *Let K be a finite field and A be a connected algebraic group over K. Then*

$$H^1(G_K, A) = 0.$$

For more general fields, however, the picture is far more intricate. A central theme in understanding the sets $H^1(G_K, A)$ for a field K and an algebraic K-group A is the study of the *local–global map*

$$H^1(G_K, A) \longrightarrow \prod_v H^1(G_{K_v}, A_v),$$

whose kernel (when v ranges over all valuations and Archimedean norms) measures the failure of a local–global principle and is called the *Tate–Shafarevich set* of A, usually denoted by $Ш(K, A)$.

The study of Tate–Shafarevich sets forms an active area of research in arithmetic geometry. For instance, when A is an abelian variety over K, the group $H^1(G_K, A)$ is known as the *Weil–Châtelet group* of A. In this context, several fundamental questions remain open. Notably, it is still unknown whether $Ш(K, A)$ is finite when K is a number field, as predicted by the *Tate–Shafarevich conjecture*. The closely

related *Birch and Swinnerton–Dyer conjecture*, one of the Millennium Prize Problems, further illustrates the depth and difficulty of these questions. Such problems lie far beyond the scope of this thesis. Instead, we restrict our attention to general ideas and results that are most relevant to our applications.

Having considered the case of abelian varieties, we now turn to another major class of algebraic groups, namely those whose underlying variety is affine. It is a classical fact that these are precisely the *linear algebraic groups*, that is, algebraic subgroups of some GL_n [Bor91, Proposition 1.10]. Despite this classification, the study of $Ш(K, A)$ for linear algebraic groups A remains an active area of research as well. For instance, it is only a relatively recent result that $Ш(K, A)$ is finite when K is a global field (see [BS65, Théorème 7.1] for number fields and [Con12, Theorem 1.3.3] for global function fields).

Most known results concerning $H^1(G_K, A)$ for linear algebraic groups A apply only when A is connected. For such groups, it is known how to compute $H^1(G_K, A)$ when K is a local field or a number field [PRR93, Chapter 6]. Another classical result of note is *Steinberg's Theorem* [Ste65, Theorem 1.9], which asserts that $H^1(G_K, A) = 0$ for any connected linear algebraic group A whenever $\operatorname{cd} G_K \leq 1$.

As mentioned above, our main interest lies in local–global principles related to the Brauer group. In this context, there is an interesting connection with principal homogeneous spaces under the connected algebraic K-group $\mathrm{PGL}_n(K)$: There is a natural bijection between $H^1(G_K, \mathrm{PGL}_n)$ and the set of K-isomorphism classes of central simple K-algebras of degree n [GS06, Theorem 2.4.3]. In particular, $\mathrm{Br}(K) = 0$ if and only if $H^1(G_K, \mathrm{PGL}_n) = 0$ for all n.

A special class of connected linear algebraic groups A is the group of *simply connected* ones. A famous open problem in this context is *Serre's Conjecture II*, which predicts that $H^1(G_K, A) = 0$ for every perfect field K with $\operatorname{cd} G_K \leq 2$ and every semisimple simply connected K-group A. This conjecture has been resolved for many types of fields and groups (see [Gil10] for a survey of known cases), but it remains open in full generality.

4.1.2.2 Degree $n = 2$

We now present local–global principles for the Brauer-group of 1-dimensional function fields over a field K. The presentation will allow us to deduce both the classical Albert–Brauer–Hasse–Noether theorem for global function fields as well as Efrat's local–global-principle over PAC fields [Efr01, Theorem 3.4]. Finally, we will connect

these concepts to a local–global principle that Pop [Pop88, Theorem 4.1] proved in his approach to the Galois characterisation of p-adically closed fields.

The following considerations are largely based on Efrat's paper [Efr01], and we will give the relevant references as needed. For the setup, let K be a perfect field and F be a function field in one variable over K (i.e., F/K is regular, finitely generated and of transcendence degree 1). Both the Albert–Brauer–Hasse–Noether theorem for global function fields and Efrat's local–global principle rely on the same exact sequence

$$1 \to (\widetilde{K}F)^\times/\widetilde{K}^\times \xrightarrow{\text{div}} \text{Div}(\widetilde{K}F/\widetilde{K}) \to \text{Pic}(\widetilde{K}F/\widetilde{K}) \to 0. \tag{4.1.6}$$

We briefly explain the terms in this sequence. For a field extension E/L, let $\mathbb{P}(E/L)$ denote the set of all non-trivial valuations on E that are trivial on L. Observe that all elements of $\mathbb{P}(\widetilde{K}F/\widetilde{K})$ are discrete rank-1 valuations with residue field $\widetilde{K}$ (an easy consequence of the Dimension Inequality, Fact 3.1.12). Then

$$\text{Div}(\widetilde{K}F/\widetilde{K}) := \bigoplus_{v\in\mathbb{P}(\widetilde{K}F/\widetilde{K})} vF \left(\cong \bigoplus_{v\in\mathbb{P}(\widetilde{K}F/\widetilde{K})} \mathbb{Z} \right).$$

We note that $\text{Div}(\widetilde{K}F/\widetilde{K})$ is naturally a $\text{Gal}(\widetilde{K}F/F)$-module and hence a G_K-module as $\text{Gal}(\widetilde{K}F/F) \cong G_K$. It is also not hard to see that for every $x \in \widetilde{K}F$, there are only finitely many $v \in \mathbb{P}(\widetilde{K}F/\widetilde{K})$ with $v(x) \neq 0$, making the following a well-defined exact sequence[5]:

$$\begin{aligned} \text{div} : (\widetilde{K}F)^\times/\widetilde{K}^\times &\to \text{Div}(\widetilde{K}F/\widetilde{K}) \\ x &\mapsto (w(x))_{w\in\mathbb{P}(\widetilde{K}F/\widetilde{K})} \end{aligned}$$

We then define $\text{Pic}(\widetilde{K}F/\widetilde{K}) := \text{coker}(\text{div})$, resulting in the short exact sequence (4.1.6). This gives rise to the following exact sequence in cohomology (see Proposition 4.1.1):

$$\begin{aligned} H^1(G_K, \text{Div}(\widetilde{K}F/\widetilde{K})) \to H^1(G_K, \text{Pic}(\widetilde{K}F/\widetilde{K})) \to H^2(G_K, (\widetilde{K}F)^\times/\widetilde{K}^\times) \\ \to H^2(G_K, \text{Div}(\widetilde{K}F/\widetilde{K})) \end{aligned} \tag{4.1.7}$$

Let us now further assume that $\text{cd}\, G_K \leq 1$. Using only elementary cohomological and valuation theoretic considerations and Proposition 4.1.25, we can prove the following list of isomorphisms (see [Efr01, Proposition 1.3, Corollary 2.2, Lemma 2.1 (c)]):

[5] For $x \in \widetilde{K}F\backslash\widetilde{K}$, note that every $v \in \mathbb{P}(\widetilde{K}(x)/\widetilde{K})$ with $v(x) \neq 0$ is either the x-adic or the degree-valuation v_∞ [EP05, Theorem 2.1.4]; in either case, there are only finitely many extensions to $\widetilde{K}F$ by the Fundamental Inequality, Fact 3.1.18.

(i) $H^1(G_K, \mathrm{Div}(\widetilde{K}F/\widetilde{K})) = 0$;

(ii) $H^2(G_K, (\widetilde{K}F)^\times/\widetilde{K}^\times) \cong H^2(G_F, \widetilde{F}^\times)$;

(iii) $H^2(G_K, \mathrm{Div}(\widetilde{K}F/\widetilde{K})) \cong \bigoplus_{v\in\mathbb{P}(F/K)} H^2(G_{Fv}, vF) \cong \bigoplus_{v\in\mathbb{P}(F/K)} H^2(G_{Fv^h}, \widetilde{Fv^h})$.

By Proposition 4.1.11, we can identify the last terms in (ii) and (iii) with $\mathrm{Br}(F)$ and $\bigoplus_{v\in\mathbb{P}(F/K)} \mathrm{Br}(Fv^h)$, respectively. Combined with (4.1.7), this gives rise to the following result [Efr01, Proposition 2.3]:

Proposition 4.1.38. *Let K be a perfect field with $\mathrm{cd}\, G_K \leq 1$ and let F be a function field in one variable over K. Then there is an exact sequence*

$$0 \to H^1(G_K, \mathrm{Pic}(\widetilde{K}F/\widetilde{K})) \to \mathrm{Br}(F) \to \bigoplus_{v\in\mathbb{P}(F/K)} \mathrm{Br}(Fv^h)$$

For any extension F/K as in the proposition, the obstruction to a local–global principle is therefore given precisely by $H^1(G_K, \mathrm{Pic}(\widetilde{K}F/\widetilde{K}))$. If C denotes the smooth projective model of F, then this group coincides with what is known as $\mathrm{Br}(C)$, the *Brauer group of* C [Lic69, Appendix].

Next, let us relate $H^1(G_K, \mathrm{Pic}(\widetilde{K}F/\widetilde{K}))$ to another geometrically meaningful object underlying Efrat's local–global principle. To this end, we define the *degree homomorphism*

$$\begin{aligned} \deg : \mathrm{Div}(F/K) &\to \mathbb{Z} \\ (n_v)_{v\in\mathbb{P}(F/K)} &\mapsto \sum_{v\in\mathbb{P}(F/K)} n_v[Fv : K]. \end{aligned}$$

If we define $\mathrm{Pic}^0(F/K) \coloneqq \ker(\deg)$, this leads to the exact sequence

$$0 \to \mathrm{Pic}^0(\widetilde{K}F/\widetilde{K}) \to \mathrm{Pic}(\widetilde{K}F/\widetilde{K}) \xrightarrow{\deg} \mathbb{Z} \to 0. \tag{4.1.8}$$

It is a classical fact that $\mathrm{Pic}^0(\widetilde{K}F/\widetilde{K})$ is isomorphic to $\mathrm{Jac}_{F/K}(\widetilde{K})$, where $\mathrm{Jac}_{F/K}$ denotes the Jacobian variety of F/K [Lic69, Lemma 1]. Hence, the above yields the following exact sequence in cohomology:

$$H^1(G_K, \mathrm{Jac}_{F/K}(\widetilde{K})) \to H^1(G_K, \mathrm{Pic}(\widetilde{K}F/\widetilde{K})) \to H^1(G_K, \mathbb{Z}). \tag{4.1.9}$$

As G_K acts trivially on $\mathbb{Z}$, we have $H^1(G_K, \mathbb{Z}) = \mathrm{Hom}(G_K, \mathbb{Z})$. Now, for any continuous homomorphism $\phi : G_K \to \mathbb{Z}$ and any $a \in \mathbb{Z}$, the preimage $\phi^{-1}(a)$ is open in G_K. Because G_K is compact, the image $\phi(G_K)$ must then be finite. However, since $\mathbb{Z}$ is torsion-free, this implies $\phi(G_K) = \{0\}$, so ϕ is trivial and $H^1(G_K, \mathbb{Z}) = 0$.

Together with (4.1.9), the previous paragraph implies that $H^1(G_K, \mathrm{Jac}_{F/K}(\widetilde{K}))$ surjects onto $H^1(G_K, \mathrm{Pic}(\widetilde{K}F/\widetilde{K}))$ [Efr01, Lemma 1.4(a)]. Hence, to remove the obstruction to a local–global principle, it suffices to show that

$$H^1(G_K, \mathrm{Jac}_{F/K}(\widetilde{K})) = 0.$$

Let us connect this back to what we saw in Section 4.1.2.1. If K is a finite field, then Theorem 4.1.37 shows that $H^1(G_K, A) = 0$ for all connected algebraic groups. In particular, $H^1(G_K, \mathrm{Jac}_{F/K}(\widetilde{K})) = 0$, thus proving the Albert–Brauer–Hasse–Noether Theorem for global function fields.

In general, the vanishing of $H^1(G_K, A)$ expresses that every principal homogeneous space for A over K admits a K-rational point. In particular, when K is a PAC field (hence automatically satisfying $\operatorname{cd} G_K \leq 1$ by [FJ08, Theorem 11.6.2]), every homogeneous space under a connected algebraic group possesses a K-rational point. As the Jacobian $\mathrm{Jac}_{F/K}$ is an example of a connected algebraic group, we consequently see that $H^1(G_K, \mathrm{Jac}_{F/K}(\widetilde{K}))$ is trivial, establishing Efrat's local–global principle for function fields over PAC fields [Efr01, Corollary 3.2]:

Proposition 4.1.39. *Let K be a perfect PAC field, and let F be a function field in one variable over K. Then the local–global principle holds; that is,*

$$0 \to H^2(G_F, \widetilde{F}^\times) \to \bigoplus_{v \in \mathbb{P}(F/K)} \mathrm{Br}(Fv^h)$$

is injective.

The exact sequence in Proposition 4.1.38, on which Efrat's local–global principle relies, assumes that F has cohomological dimension at most 1. It is therefore natural to ask what can be said for more general base fields K. A partial answer to this question is provided by Pop's work [Pop88], although it is not construed as such. For a function field F in one variable over K of characteristic 0 with smooth projective model C, Pop constructs a pairing

$$\Phi_F : \mathrm{Br}(C) \times \mathrm{Pic}(F) \to \mathrm{Br}(K),$$

inducing a map

$$\mathbf{\Phi}_F : \mathrm{Br}(C) \to \mathrm{Hom}(\mathrm{Pic}(F), \mathrm{Br}(K)). \tag{4.1.10}$$

In the case where $\mathbf{\Phi}_F$ is injective for all regular extensions F/K in one variable, Pop defines K to *possess the Φ-property*. He then shows that every field K possessing

the Φ-property satisfies a local–global principle [Pop88, Theorem 4.1]. Moreover, he proves that the Φ-property is a first-order property; that is, any field elementarily equivalent to a field K with the Φ-property also satisfies the Φ-property. In particular, using a result of Lichtenbaum [Lic69, Theorem 4], he deduces [Pop88, Theorem 3.7] that finite extensions of $\mathbb{Q}_p$ possess the Φ-property, thereby establishing a local–global principle for function fields over p-adically closed fields.

Relating Pop's local–global principle to Proposition 4.1.38, we observe that if K satisfies $\operatorname{cd} G_K \leq 1$, then $\operatorname{Br}(K)$ (and hence, $\operatorname{Hom}(\operatorname{Pic}(F), \operatorname{Br}(K))$) is trivial. Consequently, the injectivity in (4.1.10) reduces to the vanishing of

$$\operatorname{Br}(C) \cong H^1(G_K, \operatorname{Pic}(\widetilde{K}F/\widetilde{K})),$$

which coincides precisely with Proposition 4.1.38.

4.1.2.3 Higher dimensions

Looking back at the local–global principles for the Brauer group discussed so far, the fields or field extensions involved have all been of low dimension. Indeed, the Albert–Brauer–Hasse–Noether Theorem concerns precisely the case of global fields, that is, fields of Kronecker dimension 1. The other local–global principles from the previous section deal with function fields of curves, i.e., one-dimensional objects, where the fields of definition are either PAC fields (which resemble algebraically closed fields) or fields with the Φ-property, the main examples of which are $\mathbb{R}$ and finite extensions of $\mathbb{Q}_p$, i.e., one-dimensional local fields. A natural question, therefore, is what happens when one considers higher-dimensional objects instead.

Unfortunately, local–global principles for the Brauer group generally do not continue to hold in a higher-dimensional setting. For instance, as soon as one considers curves over number fields, counterexamples are known (see, for example, [Jan16, remark following Conjecture 1]). This example is not a mere exceptional case. As observed by Harbater et al., "a theme that has emerged in these investigations [of higher-dimensional local–global principles] is that as one adjoins a transcendental element to a field, one expects to find local–global principles one degree higher than previously" [HKP21, p. 177]. In this section, we provide an overview of such higher-dimensional local–global principles.

The first higher-dimensional generalisation of the classical Albert–Brauer–Hasse–Noether Theorem for global fields was Kato's local–global principle for function fields of curves over global fields [Kat86]. In analogy to Theorem 4.1.36, it is concerned

with the Galois cohomology groups $H^3(G_K, \mathbb{Z}/n\mathbb{Z}(2))$, which are just $H^3(G_K, \mu_n)$ in case $\mu_n \subseteq K$.

Apart from the cohomology groups themselves, we also need to generalise the norms or valuations over which the completions are taken. In geometric terms, the "local part" of the local–global principles presented so far was concerned with the completions or henselisations of F with respect to Archimedean and non-Archimedean places. In the higher-dimensional setting, local–global principles are often formulated and proved in terms of local rings of schemes: For a given function field F/K, let X denote a model of F and let X^i be the set of all points x such that $\overline{\{x\}}$ is of co-dimension i. Then the local–global principles most commonly range over all $x \in X^{(i)}$ for some i and take values in the fraction field F_x of the completion of the local ring $\mathcal{O}_{X,x}$. It is a standard fact from algebraic geometry (see, for example [Har77, II.§6]) that for $x \in X^{(1)}$, $\mathcal{O}_{X,x}$ is just a discrete rank-1 valuation ring, so in this case, F_x is indeed the completion F_{v_x} with respect to the valuation v_x corresponding to $\mathcal{O}_{X,x}$. In particular, every local–global principle of the shape

$$H^n(G_K, M) \to \prod_{x \in X^{(1)}} H^n(G_{K_{v_x}}, M_{v_x}),$$

automatically implies one where the product is taken over all discrete rank-1 valuations on K. Making use of this observation, we can see the next proposition as a direct consequence of Kato's local–global principle [Kat86, Theorem 0.8(ii), (iii)].

Proposition 4.1.40. *Let K be a global field, F/K be a function field of transcendence degree 1, and let n be a positive integer that is coprime to* $\operatorname{char} K$.

(i) If V denotes the set of all discrete rank-1 valuations on F, then

$$H^3(G_F, \mathbb{Z}/n\mathbb{Z}(2)) \to \prod_{v \in V} H^3(G_{F_v}, \mathbb{Z}/n\mathbb{Z}(2))$$

is injective.

(ii) If V denotes the set of all valuations on K, then

$$H^3(G_F, \mathbb{Z}/n\mathbb{Z}(2)) \to \prod_{v \in V} H^3(G_{FK_v}, \mathbb{Z}/n\mathbb{Z}(2))$$

is injective.

Other valuation-theoretic consequences of Kato's result can be formulated. For instance, Spiess [Spi96, Main Lemma 2.4]—essentially combining statement (i) of

Proposition 4.1.40 with an application of the Albert–Brauer–Hasse–Noether Theorem to the composed valuation—established a local–global principle over all *closed* valuations in the valuation spectrum; that is, valuations that admit no proper refinement (or equivalently, valuations whose residue field has Kronecker dimension 0, that is, an algebraic extension of $\mathbb{F}_p$). More recently, Jannsen [Jan16, Theorem 0.4] generalised item (ii) to d-dimensional function fields over global fields, where the cohomology groups $H^3(_, \mathbb{Z}/n\mathbb{Z}(2))$ are replaced by $H^{d+2}(_, \mathbb{Z}/n\mathbb{Z}(d+1))$.

In recent years, efforts have been made to generalise Kato's local–global principle for 2-dimensional global fields to other 2-dimensional objects. Here, a particular focus has been the *local* and the *semi-global case*, which can be defined as follows:

- The *semi-global case* concerns function fields of connected regular projective curves over the fraction field of a henselian excellent discrete valuation ring A.
- The *local case* concerns the fraction field of a two-dimensional henselian excellent normal local domain A.

Some of the concepts appearing in this description are very geometric in nature, and we shall not go into detail about their precise meaning here. Instead, we give the typical examples to keep in mind. The most important source of semi-global fields are one-variable function fields over complete discretely valued fields. Typical examples of local fields are the fields $F(\!(s,t)\!)$ for some field F, which are produced for $A = F[\![s,t]\!]$.

For fields K in either setting, Colliot-Thélène [CT11] asked whether the map

$$H^d(G_K, \mathbb{Z}/n\mathbb{Z}(d-1)) \to \prod_{v \in V} H^d(G_{K_v}, \mathbb{Z}/n\mathbb{Z}(d-1))$$

is injective for all $d \geq 2$, where V denotes the set of all discrete rank-1 valuations on K. This was motivated by the result being true for $d = 2$ in the semi-global setting [CTPS12, Theorem 4.3(ii)] and in the local setting [Hu12, Proof of Theorem 1.1].

In the semi-global case, Colliot-Thélène's question was first answered affirmatively for all $d \geq 2$ when A is equi-characteristic and complete [HHK14, Theorem 3.3.6] relying on patching machinery. It was subsequently generalised to general equi-characteristic A for both local and semi-global fields by using cohomological methods rather than patching [Hu16, Theorem 1.2]. Hu's argument was generalised to the mixed characteristic setting by Suresh (cited but unpublished for many years; argument now written up [HKP21, Theorem 4.3]), and by Sakagaito [Sak20, Theorem 2] using alternative methods. More recently, higher-dimensional analogues have

been found for the function fields of some curves over certain semi-global fields if $d \geq 3$. [HKP21, Theorem 5.2, Theorem 5.5].

4.1.2.4 Extending to non-finitely generated fields

The local–global principles presented in the previous sections share the feature that the fields in question are finitely generated over some base field. It is natural to ask whether similar local–global principles hold for algebraic extensions of these fields that are not necessarily finitely generated any more. A natural approach is attempting to reduce such cases to the finitely generated setting: Let F/K be a field extension, V be a collection of valuations on F, and write $F = \bigcup F_i$, where each F_i/K is finitely generated. Suppose that for each i, a local–global principle holds with respect to the valuations in V restricted to F_i. Does it then follow that a local–global principle holds for F with respect to V?

As it turns out, the answer to this question is negative in general. A classical counterexample is given by Pop [Pop88, Beispiel 4.2]: For $p \neq 2$, let v denote the *Gauss valuation* on $\mathbb{Q}_p(t)$, i.e., the valuation induced by

$$v(a_0 + a_1 t + \cdots + a_n t^n) = \min\{v_p(a_i)\},$$

and let (F, u) be a henselisation of $(\mathbb{Q}_p(t), v)$. Then $uF = \mathbb{Z}$ and $Fu = \mathbb{F}_p(t)$. In particular, using Lemma 4.1.13 and Hensel's Lemma, a simple calculation involving a comparison of coefficients reveals that the quaternion algebra $(F(\sqrt{t}), \zeta_{p-1})$ is not split over F, so $\mathrm{Br}(F) \neq 0$.

Now let V be the collection of all valuations on F that are trivial on $\mathbb{Q}_p$, and present F as the union of all function fields $F_i/\mathbb{Q}_p$ with $F_i \subseteq F$. As we saw in Section 4.1.2.2, all F_i satisfy a local–global principle with respect to the valuations in V restricted to F_i. However, for every $v \in V$, the fields F_v^h will be henselian with respect to both v and the unique extension of u to F_v^h. However, v is trivial on $\mathbb{Q}_p$ and u is not, so by Theorem 3.1.48, F_v^h is separably closed. In particular, $\mathrm{Br}(F_v^h) = 0$, so the local–global principle fails for F.

Nevertheless, there is a way to generalise many of the local–global principles we discussed above to certain infinite algebraic extensions of the fields in question. This includes Efrat's local–global principle over PAC fields and Spiess' local–global principle over number fields, but also Pop's local–global principle for p-adically closed fields [Pop88, Theorem 4.5]:

Theorem 4.1.41. *Let (K, v) be a p-adically closed field and L/K be a field extension of transcendence degree 1, and V be the set of all extensions of v to L. Then*

$$\mathrm{Br}(L) \to \prod_{w \in V} \mathrm{Br}(L_w^h)$$

is injective.

The main ingredient in Pop's proof is a model-theoretic compactness argument [Pop88, Lemma 4.4]; meanwhile, Wiesend [Wie95, Lemma 2] gave a purely topological proof of Pop's argument. Efrat [Efr01, Lemma 3.3] and Spiess [Spi96, Claim 2.4.2] used similar compactness arguments in their respective generalisations. In each of these cases, the argument crucially relies on the following property: In the case of finitely generated fields, the image of the local–global principle (which a priori, is contained in a product taken over valuations) is actually contained in a direct sum. Efrat [Efr01, Lemma 3.3] spells out this condition explicitly, and we restate it here for later reference.

Proposition 4.1.42. *Let $(F_i)_{i \in I}$ be a system directed by inclusion, $F = \bigcup_{i \in I} F_i$, and V be a set of valuations on F. Denote by V_i the set of the restrictions of V to F_i. Assume p is a prime number such that for every $i \in I$,*

$$\mathrm{Br}(F_i)(p) \to \prod_{v \in V_i} \mathrm{Br}((F_i)_v^h)$$

is injective with image contained in the direct sum $\bigoplus_{v \in V_i} \mathrm{Br}((F_i)_v^h)$. Then

$$\mathrm{Br}(F)(p) \to \prod_{v \in V} \mathrm{Br}(F_v^h)$$

is injective as well.

Proposition 4.1.42 can be used to generalise Proposition 4.1.39 to arbitrary extensions F/K of relative transcendence degree 1 of perfect PAC fields K [Efr01, Theorem 3.4]. Indeed, if K is a perfect PAC field, then so is $\widetilde{K} \cap F$ [FJ08, Corollary 11.2.5], so we are reduced to the case that F/K is regular of transcendence degree 1, in which case Proposition 4.1.42 applies. This gives rise to the final statement of Efrat's local–global principle for PAC fields:

Theorem 4.1.43. *Let K be a perfect PAC field and F/K be an extension of relative transcendence degree 1. Then the map*

$$\mathrm{Br}(F) \to \prod_{v \in \mathbb{P}(F/K)} \mathrm{Br}(F_v^h)$$

is injective.

4.2 Cohomological local–global approach to eliminate Case 4

We will now connect the cohomological considerations of the previous section with the elimination of Case 4. For reference, let us record once again that a field belongs to Case 4 if it is elementarily equivalent to a field $L((t^{\mathbb{Z}_{(p)}}))$, such that L satisfies the following properties:

- $\operatorname{char} L = 0$;
- $L/\mathbb{Q}$ is of finite transcendence degree;
- L admits no proper abelian extension;
- L has a henselian valuation with residue characteristic p;
- L is elementarily determined by G_L only among fields of characteristic not equal to p;
- $\operatorname{cd}_p G_L = 1$.

By Koenigsmann's classification theorem (Theorem 1.1.8), fields that belong to Case 4 are elementarily characterised by their absolute Galois group. Let us make a rather general observation about such fields.

In the previous chapter, we saw that, as in the case of the real numbers $\mathbb{R}$, the first-order theory of $\mathbb{Q}_p$ is encoded in the absolute Galois group of $\mathbb{Q}_p$. In the case of $\mathbb{Q}_p$, we saw that the elementary characterisation of $\mathbb{Q}_p$ by its absolute Galois group $G_{\mathbb{Q}_p}$ reduces to two facts: $\mathbb{Q}_p$ is elementarily determined by $G_{\mathbb{Q}_p}$, and $G_{\mathbb{Q}_p}$ is small. Based on Klingen's result Lemma 3.3.1, Koenigsmann observed [Koe04, Observation 2.1] that this is true more generally.

Proposition 4.2.1. *Let K be a field. Then the implication $(F \equiv K \implies G_F \cong G_K)$ holds for all fields F if and only if G_K is small.*

In what follows, we motivate and outline our cohomological approach to the elimination of Case 4. In Section 4.2.1, we reduce the problem to two well-known cohomological conjectures: Koenigsmann's conjectures on solvably closed fields, and Efrat's Elementary Type Conjecture. Section 4.2.2 then presents a further reduction to a weaker form of Koenigsmann's conjecture. Finally, in Section 4.2.3, we discuss attempts to address this weaker conjecture, focusing in particular on a local–global approach that culminates in a conditional elimination of Case 4.

4.2.1 Cohomological conjectures and Case 4

To understand the connection between Galois cohomology and the elimination of Case 4, we first remind the reader of the following theorem [FJ08, Corollary 23.1.2], which is a consequence of the work of Lubotzky and van den Dries [LvdD81].

Theorem 4.2.2. *Given a projective group G and any field K, there exists some extension F/K which is perfect and PAC with $G_F \cong G$.*

In the context of fields elementarily characterised by their absolute Galois group, this theorem has the important consequence that fields with a projective absolute Galois group can never be characterised by their absolute group: In the above theorem, K can be chosen of arbitrary characteristic, which means that G_K does not determine the characteristic of K.

Therefore, the following conjecture, which is already contained in Koenigsmann's original work [Koe04, Question 5.3], would immediately rule out Case 4:

Conjecture 4.2.3. *Let K be a field that does not admit a proper abelian extension. Then G_K is projective.*

This conjecture is known to hold in several special cases and is sometimes believed to be true in an even stronger form. Observe that the condition that K admits no proper cyclic extension is equivalent to requiring that K coincides with its maximal solvable extension. The stronger version of the conjecture asserts that the maximal *abelian* extension K^{ab} of any field K already has a projective Galois group. At present, this has been established only in a few specific situations. It follows from classical results when K is a global field (Proposition 4.1.22 when K is a global function field, and [Ser97, II.§3.3, Proposition 9] when K is a number field), or when K is a local field (trivial for the Archimedean local fields $K = \mathbb{R}, \mathbb{C}$, and a consequence of Proposition 4.1.23 in the non-Archimedean case). More recently, [CTOP02, Theorem 2.3] established that for two-dimensional local fields (as defined in Section 4.1.2.3), one has $\operatorname{cd} G_{K^{\mathrm{ab}}} \leq 1$, a notable example being $K = \mathbb{C}(\!(s,t)\!)$. Some conditional results concerning both conjectures have also been obtained in characteristic 0 in the context of Hilbert's 13th problem [CGR06], but to the best of our knowledge, the conjectures remain entirely open in general, both for maximal abelian and for maximal solvable extensions.

The fields L in Case 4 have of course more properties other than not admitting proper abelian extensions. For example, by Proposition 4.2.1, they have small absolute Galois groups. In this more restricted setting of fields with small absolute Galois

groups, Koenigsmann's conjecture would follow from Efrat's Elementary Type Conjecture (ETC). Let us explain why this is the case and clarify what is meant by ETC in this context.

For a field F, we denote by $F(p)$ its maximal pro-p Galois extension and let $G_F(p) \coloneqq \mathrm{Gal}(F(p)/F)$ be the corresponding maximal pro-p Galois group of F. Efrat's Elementary Type Conjecture is concerned with the setting in which $\zeta_p \in F$ and $G_F(p)$ is finitely generated (note that, by Kummer theory, $G_F(p)$ is finitely generated if and only if $|F^\times/F^{\times p}| < \infty$). The following conjecture, which was originally formulated in [Efr95a], gives a conjectural classification of all such groups.

Conjecture 4.2.4 (ETC, arithmetical version)**.** *Let F be a field with $\zeta_p \in F$ such that $G_F(p)$ is finitely generated. Then $G_F(p)$ is the free product in the category of pro-p groups of finitely many closed subgroups of the following forms:*

1. *$\mathbb{Z}_p$;*
2. *Decomposition groups of valuations on F with a nontrivial inertia group in $F(p)$;*
3. *C_2, when $p = 2$.*

The above version is known as the *arithmetical version of ETC*, but the reader might be more familiar with a different version, which is a consequence of the arithmetical version. In his recent survey [Efr25], which highlights the links of ETC to other conjectures in Galois theory, Efrat calls this consequence the *Lego version of ETC*.

Conjecture 4.2.5 (ETC, Lego version)**.** *Let F be a field containing a primitive p-th root of unity, and let $G_F(p)$ denote its maximal pro-p Galois group. If $G_F(p)$ is finitely generated, then it can be constructed from copies of $\mathbb{Z}_p$, of C_2 when $p = 2$, and of groups $G_L(p)$ for finite extensions L of $\mathbb{Q}_p(\mu_p)$, using free pro-p products and semidirect products of the form $\mathbb{Z}_p^n \rtimes _$.*

As explained in the same article, the arithmetical version of ETC is equivalent to the Lego version together with the *Demuškin Conjecture*. Stating the Demuškin Conjecture in full is somewhat technical, so we refer the reader to [Efr25, §12] for the full statement. Like the other two conjectures, the Demuškin Conjecture is open in general, but has recently been verified in a special case by Koenigsmann and Strommen [KS24].

We can now explain why the arithmetical version of ETC would eliminate Case 4. Let L be a field with a small absolute Galois group that admits no proper abelian extensions. Assume that G_L is not projective. By Proposition 4.1.30, this means that for some finite extension F/L and prime q, $H^2(G_F, \mathbb{Z}/q\mathbb{Z}) \neq 0$.

We would like to apply Conjecture 4.2.4 to F. We note that since L does not admit any proper abelian extensions, $\zeta_q \in L \subseteq F$. Moreover, as G_L is small and F/L is finite, we see that G_F is small as well; in particular, $G_F(q)$ is finitely generated.

Claim. $G_F(q)$ not projective (and in particular, not trivial)

Proof of Claim. By Proposition 4.1.27 and the definition of cohomological dimension, it suffices to show that $H^2(G_F(q), \mathbb{Z}/q\mathbb{Z}) \neq 0$. Note that since $\mu_q \subseteq L$, G_L acts trivially on μ_q, so $\mathbb{Z}/q\mathbb{Z} \cong \mu_q$ as G_L-modules. Assume now that we could show $H^m(G_{F(q)}, \mu_q) = 0$ for all $m > 0$. Then, by Proposition 4.1.2,

$$H^2(G_F(q), \mathbb{Z}/q\mathbb{Z}) \cong H^2(G_F/G_{F(q)}, \mu_q) \cong H^2(G_F, \mu_q) \cong H^2(G_F, \mathbb{Z}/q\mathbb{Z}) \neq 0.$$

To complete the proof, it thus remains to show that $H^m(G_{F(q)}, \mu_q) = 0$ for all $m > 0$. Observe that since $F(q)$ is the maximal pro-q extension of F, it admits no C_q-extensions. By Kummer theory, this implies $F(q)^\times = F(q)^{\times q}$. Now, let $\{a_1, \dots, a_m\}$ be any symbol in $K_m^M(F(q))/q$ with $a_1, \dots, a_m \in F(q)^\times$. As $F(q)^\times = F(q)^{\times q}$, we may write $a_1 = b^q$ for some $b \in F(q)^\times$. In particular,

$$a_1 \otimes \cdots \otimes a_m = b^q \otimes a_2 \cdots \otimes a_m = q \cdot (b \otimes a_2 \cdots \otimes a_m) \equiv 0 \pmod{q},$$

which means $K_m^M(F(q))/q = 0$, so $H^m(G_{F(q)}, \mu_q) = 0$ follows from the norm residue isomorphism, Theorem 4.1.18. ◇

Observe that $G_F(q)$ cannot contain a factor of C_2 by the Artin–Schreier Theorem 1.1.2 as $\sqrt{-1} \in L$ (otherwise, L would admit a proper abelian extension). Moreover, $G_F(q)$ cannot be a free product of finitely many copies of $\mathbb{Z}_q$ as such products are free and hence projective, in contradiction to the claim. Consequently, as $G_F(q)$ is non-trivial, it has a factor that is the decomposition group of a valuation on F with non-trivial inertia group. In particular, this implies that F admits a valuation v, for which vF is not q-divisible. Consequently, $w \coloneqq v|_L$ is a valuation on L with wL not q-divisible. So let $a \in wL$ such that $\frac{a}{q} \notin wL$ and choose an element $l \in L$ such that $w(l) = a$. Since L has no proper abelian extensions and $\zeta_q \in L$, it follows that $\sqrt[q]{l} \in L$, and hence, $w(\sqrt[q]{l}) = \frac{a}{q}$, which is the required contradiction.

4.2.2 Reducing Case 4 to weaker conjecture

In the previous section, we have connected the elimination of Case 4 to the Galois-cohomological Conjecture 4.2.3. We have further provided evidence for this conjecture, especially in the more restricted setting of Case 4. In this section, we will reduce the elimination of Case 4 to the following weaker form of Conjecture 4.2.3:

Conjecture 4.2.6. *Let $F/\widetilde{\mathbb{Q}}$ be a field extension of transcendence degree 2 such that F admits no proper abelian extensions, and assume that G_F is small. Then G_F is projective.*

Proposition 4.2.7. *If Conjecture 4.2.6 holds, then Case 4 is eliminated.*

Proof. Assume Case 4 is not empty and let $K = L((t^{\mathbb{Z}_{(p)}}))$ be a field as described in Case 4. In particular, $\operatorname{char} L = 0$, L is endowed with a henselian valuation v of mixed characteristic $(0, p)$, L admits no proper abelian extensions, $\operatorname{cd}_p G_L = 1$, and L is determined by G_L among fields of characteristic not equal to p.

We first show that L contains a copy of $\widetilde{\mathbb{Q}}$. Let (L', v') denote the intersection of (L, v) with $\widetilde{\mathbb{Q}}$. Then $L'v'$ has prime field $\mathbb{F}_p$. In particular, as L (and hence L') admits no proper abelian extensions, the same is true for $L'v'$, so that $L'v' = \widetilde{\mathbb{F}_p}$ by the Galois theory of finite fields. Similarly, we see that $v'L'$ is divisible: For any $a \in v'L'$, choose an element $l \in L'$ such that $v'(l) = a$. To show that $v'L'$ is q-divisible for every prime q, note that L' contains all q-th roots of unity, so $\sqrt[q]{l} \in L'$ by Kummer theory since L' has no proper abelian extensions; in particular $v'(\sqrt[q]{l}) = \frac{a}{q} \in v'L'$. By ramification theory, we see that $G_{L'} = I_{L'} = R_{L'}$. As $R_{L'}$ is a pro-p group, we see that it admits a non-trivial abelian quotient unless $R_{L'} = 1$, which means $G_{L'} = 1$, so $L' = \widetilde{\mathbb{Q}}$ as required.

Secondly, as L is determined among fields of characteristic not equal to p and $\operatorname{cd}_p G_L = 1$, Theorem 4.2.2 implies that there is a prime $q \neq p$ such that $\operatorname{cd}_q G_L > 1$. By Proposition 4.1.29, that means there is an extension E/L with a C_q-extension for which the norm is not surjective. As L admits no proper abelian extensions, it contains all roots of unity, so Kummer theory implies that this C_q-extension is given as $E(\sqrt[q]{t})/E$ for some $t \in E$.

Let $s \in E^\times$ denote an element which is not contained in the image of the norm map $N_{E(\sqrt[q]{t})/E}$, which means precisely that there is no element of the shape $a_0 + a_1\sqrt[q]{t} + \cdots + a_{q-1}(\sqrt[q]{t})^{q-1}$ with $a_i \in E$ such that the product of its Galois conjugates is equal

to s. Hence, if we let $E' \coloneqq L(s,t) \subseteq E$ and consider the C_q-extension $E'(\sqrt[q]{t})/E'$, we see that s is not contained in the image of $N_{E'(\sqrt[q]{t})/E'}$ either.

Similarly, letting $E'' \coloneqq E' \cap \widetilde{\mathbb{Q}(s,t)}$, s is not contained in the image of $N_{E''(\sqrt[q]{t})/E''}$; in particular, this means that $\mathrm{cd}_q G_{E''} \geq 2$. Moreover, as E'' is an algebraic extension of $\widetilde{\mathbb{Q}}(s,t)$, we see that $2 \leq \mathrm{cd}\, G_{E''} \leq \mathrm{cd}\, G_{\widetilde{\mathbb{Q}}(s,t)}$, so $\widetilde{\mathbb{Q}}(s,t)/\mathbb{Q}$ must be of transcendence degree 2 by Proposition 4.1.22.

If we denote $L'' \coloneqq L \cap \widetilde{\mathbb{Q}(s,t)} \supseteq \widetilde{\mathbb{Q}}(s,t)$, then E''/L'' is an algebraic extension, so we see that $\mathrm{cd}_q G_{L''} \geq 2$, and $\mathrm{td}(L''/\widetilde{\mathbb{Q}}) = 2$. At the same time, L'' does not admit any proper abelian extensions and continues to have small absolute Galois group, so the assumptions of Conjecture 4.2.6 are satisfied for $F = L''$. Thus, the conjecture would imply that L'' has projective Galois group, which contradicts $\mathrm{cd}_q G_{L''} > 1$. □

Conjecture 4.2.6 has the following analogue in positive characteristic.

Conjecture 4.2.8. *Let $F/\widetilde{\mathbb{F}_p}$ be a field extension of transcendence degree 2 such that F admits no proper abelian extensions, and assume G_F is small. Then G_F is projective.*

By slightly modifying the proof of Proposition 4.2.7, we can reduce the elimination of Case 4 to Conjecture 4.2.8.

Proposition 4.2.9. *If Conjecture 4.2.8 holds, then Case 4 is eliminated.*

Proof. Let L be as in the proof of Proposition 4.2.7. As before, we can find a prime $q \neq p$ such that $\mathrm{cd}_q G_L > 1$. Now observe that vL is q-divisible. Indeed, given $a \in vL$, we can find an element $l \in L$ with $v(l) = a$. As L admits no proper abelian extensions, this must mean that $\sqrt[q]{l} \in L$, which satisfies $v(\sqrt[q]{l}) = \frac{a}{q}$. Thus, vL is q-divisible, which implies $\dim_{\mathbb{F}_q} vL/qvL = 0$.

By Theorem 4.1.24, this implies that $\mathrm{cd}_q G_{Lv} = \mathrm{cd}_q G_L > 1$. In particular, by the same reasoning as in the previous proof, we can find a field extension $L''/\widetilde{\mathbb{F}_p}$ with $\mathrm{td}(L''/\widetilde{\mathbb{F}_p}) = 2$ such that L'' is solvably closed and has small absolute Galois group (smallness of G_L implies smallness of G_{Lv}) and $\mathrm{cd}_q G_{L''} > 1$, in contradiction to Conjecture 4.2.8. □

Finally, it is not difficult to show that Conjecture 4.2.6 implies Conjecture 4.2.8.

Lemma 4.2.10. *Let $F/\widetilde{\mathbb{F}_p}$ be a field extension of transcendence degree 2 such that F admits no proper abelian extensions, and assume G_F is small. If Conjecture 4.2.6 holds, then G_F is necessarily projective.*

Proof. It suffices to show that there is a field extension $L/\widetilde{\mathbb{Q}}$ of transcendence degree 2 such that $G_L \cong G_F$. Indeed, the fact that L admits no proper abelian extensions is witnessed by G_L, and G_L is small (as G_F is), so G_L would be projective by Conjecture 4.2.6.

To construct the field L, we require once again the construction of the *Gauss valuation*, which we already encountered in Section 4.1.2.4. Starting with $\mathbb{Q}$ endowed with the p-adic valuation v_p, this allows us to extend v_p to a valuation on $\mathbb{Q}(s,t)$ with residue field $\mathbb{F}_p(\overline{s},\overline{t})$. If we identify $\overline{s}$ and $\overline{t}$ with two algebraically independent transcendental elements in F, this allows us to view F as an algebraic extension of the residue field of $\mathbb{Q}(s,t)$. Now, by adjoining all necessary roots of polynomials whose reductions in F have a solution, we can extend $\mathbb{Q}(s,t)$ to a valued field (L_*, v_*) with $L_* v_* = F$.

Now, the henselisation (L_*^h, v_*^h) continues to have residue field F. Therefore,

$$G_{L_*^h} \cong I_{L_*^h} \rtimes G_F$$

by Corollary 3.1.29, so $\mathrm{Fix}(1 \rtimes G_F)$ will be a field of characteristic 0 and with absolute Galois group isomorphic to G_F. □

In view of Proposition 4.2.9 and Lemma 4.2.10, we see that Conjecture 4.2.8 is a weaker conjecture than Conjecture 4.2.6, which is why the following sections will focus on attempts to resolve Conjecture 4.2.8.

4.2.3 Attempts to resolve weaker conjecture

In this section, we make a few observations that may contribute towards resolving (a stronger form of) Conjecture 4.2.8. More precisely, our aim is to show that the field $F = \mathbb{F}_p(s,t)^{\mathrm{solv}}$ possesses a projective absolute Galois group. Since any field as in Conjecture 4.2.8 contains a copy of $\mathbb{F}_p(s,t)^{\mathrm{solv}}$, this would suffice to settle the conjecture by Proposition 4.1.21. We note, however, that the absolute Galois group of F is not small[6].

[6]Since $\mathbb{F}_p(s,t) = \mathbb{F}_p(s)(t)$ is a rational function field over the infinite field $\mathbb{F}_p(s)$, it is Hilbertian (cf. [FJ08, Proposition 13.2.1]). In particular, $\mathbb{F}_p(s,t)$ admits infinitely many pairwise linearly disjoint Galois extensions $L_i/\mathbb{F}_p(s,t)$ with Galois group S_5 (cf. [FJ08, Corollary 16.2.7]). But then L_iF/F is a non-trivial Galois extension with Galois group S_5 or A_5 for each i, inducing infinitely many non-isomorphic Galois extensions of degree at most 60.

We begin by making some general observations and indicating why certain straightforward approaches fail, before outlining a more promising local–global strategy.

Some general observations and direct attempts Let us from now denote $F \coloneqq \mathbb{F}_p(s,t)^{\mathrm{solv}}$. We have already noted that $\widetilde{\mathbb{F}_p} \subseteq F$ by the Galois theory of finite fields. In particular, since $\widetilde{\mathbb{F}_p}(s,t)$ has cohomological dimension at most 2, the same holds for F.

The fact that $\operatorname{cd} G_F \leq 2$ might suggest a possible connection with Serre's Conjecture II (see Section 4.1.2.1). Indeed, as observed above, the inequality $\operatorname{cd} G_F \leq 1$ would follow if one could establish that $H^1(E, \mathrm{PGL}_n) = 0$ for all finite separable extensions E/F and all positive integers n. However, although PGL_n is connected, it is not, in general, simply connected, and thus Serre's Conjecture II does not apply in this context.

Another observation is that it is a direct consequence of the Merkurjev–Suslin Theorem that fields without proper abelian extensions have a trivial Brauer group [MS83, Corollary 16.2]. In particular, $\mathrm{Br}(F) = 0$. Unfortunately, this alone is insufficient to show that $\operatorname{cd} G_F \leq 1$, as one must also establish the vanishing of $\mathrm{Br}(E)(q)$ for all finite separable extensions E/F and all primes $q \neq p$. In fact, there are known examples of fields K for which $\mathrm{Br}(K) = 0$ and $\operatorname{cd} G_K > 1$ (see, for example, [Ser97, II.§3.1, Exercise 1]).

A local–global approach We now motivate a local–global approach to eliminate Case 4. Let E/F be a finite separable extension, and let v be any non-trivial valuation on E. In analogy to the argument used in the proof of Proposition 4.2.9, we observe that vF (and hence vE) is q-divisible for all primes $q \neq p$. Furthermore, the transcendence degree $\mathrm{td}(Ev/\mathbb{F}_p)$ is at most 1, since $\mathrm{td}(Ev/\mathbb{F}_p) = \mathrm{td}(Fv/\mathbb{F}_p) = 2$ would imply that v is trivial by the Dimension Inequality (Fact 3.1.12).

As v is trivial on $\mathbb{F}_p$ and $\widetilde{\mathbb{F}_p} \subseteq F$, it follows that v is trivial on the entirety of $\widetilde{\mathbb{F}_p}$, so $\widetilde{\mathbb{F}_p} \subseteq Ev$. Consequently, either $Ev = \widetilde{\mathbb{F}_p}$, or $Ev/\widetilde{\mathbb{F}_p}$ is an extension of transcendence degree at most 1. In either case, G_{Ev} has cohomological dimension at most 1 by Proposition 4.1.22 and Proposition 4.1.21.

Combining the last two paragraphs, Theorem 4.1.24 implies that any henselisation E_v^h has cohomological dimension at most 1, which, by Proposition 4.1.27, is equivalent to the projectivity of its Galois group. Hence, in view of Proposition 4.1.30,

if we could show that for all finite separable extensions E/F and primes $q \neq p$, the reduction map

$$\mathrm{Br}(E)(q) \to \prod_{v \in V} \mathrm{Br}(E_v^h)$$

is injective for some set of valuations V, we could deduce that G_F is projective.

Next, let us examine the local–global principles discussed in Section 4.1.2 with regard to their applicability to our situation. We note that F is a field of Kronecker dimension 2 and not finitely generated. Following the strategy described in Section 4.1.2.4, in a first step, we should try to reduce to finitely generated subfields.

Since F is a transcendence degree-1 extension of a global function field, the most natural approach would be to apply Kato's framework of two-dimensional global fields. However, Kato's results concern cohomology groups in degree 3, whereas our interest lies in vanishing results in degree 2. Considering that the Albert–Brauer–Hasse–Noether Theorem provides a local–global principle for global fields in degree 2, this aligns with Harbater's heuristic cited above, that for curves over global fields, one would only expect a local–global principle in degree 3. Note also that for the field $\mathbb{Q}(s,t)^{\mathrm{solv}}$, the heuristic only predicts local–global principles in degree 4.

The preceding paragraph shows that it is not a promising strategy to attempt to eliminate Case 4 by viewing F as a union of function fields of global fields. An alternative approach would be to use Efrat's framework. In this setting, as observed in Proposition 4.1.42, to reduce to the finitely generated case, we must ensure that F is a regular transcendence degree-1 extension of its base field. Let us fix s as a natural choice of this transcendental element. Then the base field becomes

$$\mathbb{F}_p(s,t)^{\mathrm{solv}} \cap \widetilde{\mathbb{F}_p(t)} = \mathbb{F}_p(t)^{\mathrm{solv}}.$$

Hence, if we could apply Theorem 4.1.43 to $K = \mathbb{F}_p(t)^{\mathrm{solv}}$, we would successfully eliminate Case 4.

Two issues become apparent. First, K is not a perfect field (for example, it does not contain $\sqrt[p]{t}$). Second, it is unknown whether K is PAC. Fortunately, the first point poses no difficulty. As we observed above, since we are interested in $\operatorname{cd} G_F$, it suffices to examine the q-primary components $\mathrm{Br}(E)(q)$ for $q \neq p$ and finite extensions E/F. As Efrat shows [Efr01, Remark 3.5(a)], the local–global principle indeed also holds for imperfect fields of characteristic p, except possibly at the p-primary component. Note that this observation also makes sense intuitively as we expect purely inseparable extensions to only affect the p-primary component.

The second issue, whether K is a PAC field, appears to be considerably more difficult. Its natural analogue in characteristic 0, the question of whether $\mathbb{Q}^{\mathrm{solv}}$ is a PAC field, is a well-known open problem in field arithmetic [FJ08, Problem 11.5.9(a)], [BSF13, 3.2].

Beyond the question of whether $\mathbb{F}_p(t)^{\mathrm{solv}}$ is PAC, it is worth noting that Efrat [Efr01, Theorem 4.1] provides a necessary condition for a field to satisfy a local–global principle:

Proposition 4.2.11. *Let K be a perfect field such that the local–global principle stated in Theorem 4.1.43 holds for all extensions F/K of relative transcendence degree 1. Then for every non-trivial valuation v on K, vK is divisible and Kv is algebraically closed.*

While the proposition does not apply directly in our situation as $K = \mathbb{F}_p(t)^{\mathrm{solv}}$ is not perfect, we can at least verify it away from p. Indeed, for any non-trivial valuation v on K, we see that vK is q-divisible for all primes $q \neq p$ since K is solvably closed as above. To see that Kv is algebraically closed, we note that non-triviality of v means that Kv must be an algebraic extension of $\mathbb{F}_p$. As v is trivial on $\mathbb{F}_p$ and since $\mathbb{F}_p(t)^{\mathrm{solv}} \supseteq \widetilde{\mathbb{F}_p}$, we see that v is trivial on all of $\widetilde{\mathbb{F}_p}$, so $Kv = \widetilde{\mathbb{F}_p}$.

As an aside, since we are primarily interested in the absolute Galois group of F, an alternative method of resolving the issue of K not being perfect is to replace F by its perfect closure everywhere, which leaves G_F unaffected. In particular, this substitution results in the corresponding base field K becoming perfect, so that every element possesses a p-th root. By an argument analogous to the one above used to show q-divisibility, it then follows that for any non-trivial valuation v on K, vK is p-divisible, so that the conditions of Proposition 4.2.11 are fully satisfied in this case.

While it does not decide whether $\mathbb{F}_p(t)^{\mathrm{solv}}$ is PAC, Proposition 4.2.11 at least provides further evidence for our local–global principle. Hence, for the moment, our considerations yield the following conditional result:

Theorem 4.2.12. *Case 4 is eliminated if $\mathbb{F}_p(t)^{\mathrm{solv}}$ is a PAC field.*

4.3 Related work and discussion

We now discuss the results above in light of related work. First, we highlight some consequences of the question of whether $\mathbb{F}_p(t)^{\mathrm{solv}}$ is a PAC field and summarise rele-

vant developments concerning solvably closed fields. Next, we outline an alternative approach, which arose from discussions with Franziska Jahnke during visits to the University of Münster. Finally, we contrast this approach with the local–global perspective introduced above.

Is $\mathbb{F}_p(t)^{\mathrm{solv}}$ PAC? In the context of Case 4, our hope is, of course, that $\mathbb{F}_p(t)^{\mathrm{solv}}$ is indeed a PAC field. However, it is worth noting that even if $\mathbb{F}_p(t)^{\mathrm{solv}}$ were found not to be PAC, this would still resolve a different open question. Before stating this question, we recall the following fact [FJ08, Corollary 11.5.5], which provides the motivation for the question.

Theorem 4.3.1. *The henselisations K_v^h of a PAC field K with respect to any non-trivial valuation v are separably closed. Consequently, Kv is separably closed and vK is a divisible group.*

The question then reads [FJ08, Problem 11.5.9(b)]:

Question 4.3.2. *Does there exist an infinite non-PAC field K of a finite transcendence degree over its prime field such that K is not formally real and all of its henselisations are separably closed?*

If $\mathbb{F}_p(t)^{\mathrm{solv}}$ turned out not to be PAC, it would provide an example of such a field K.

Finally, let us place the question of whether $\mathbb{F}_p(t)^{\mathrm{solv}}$ is a PAC field in the context of current research on solvable points of varieties in geometry. As highlighted in a recent preprint by Gómez-Gonzáles and Wolfson [GGW25, p. 2], contemporary research on solvable points of varieties has been remarkably sparse. Indeed, the authors list only five papers ([Pá04, WÇ08, Pá13, Woo16, Raw24]), which, excluding their own, appear to constitute the entire body of work on solvable points over the past 25 years. Unfortunately, none of these six papers seems directly relevant to determining whether $\mathbb{F}_p(t)^{\mathrm{solv}}$ is PAC, as they either establish the existence of solvable points on certain varieties over general fields of definition ([Pá04], [Woo16], [GGW25]), or they demonstrate that curves over specific fields possess solvable points or describe corresponding obstructions ([WÇ08], [Pá13], [Raw24]).

An alternative approach The following is an alternative approach that can be seen as an instance of the *Saturation-Decomposition method*, which we briefly outlined in Section 3.2.4.

We let (L, v) be as in Case 4, and let $(L^*, v^*) \succcurlyeq (L, v)$ be an $\aleph_1$-saturated extension. We now consider the Standard Decomposition of v^*:

$$v^* : L^* \to L_0^* \xrightarrow{\overline{v_p^*}} L_p^* \to Lv^*$$

Let us denote the valuation $\overline{v_p^*}$ on L_0 by w for simplicity. We claim that (L_0^*, w) satisfies the assumptions of the Transfer Lemma 3.2.18. Indeed, we first note that $G_L \cong G_{L^*}$ by Proposition 4.2.1. Then, as L^* admits no proper abelian extensions, the same is true for L_0^*; in particular, $(L_0^*)^\times/(L_0^*)^{\times p}$ is trivial. Moreover, divisibility of v^*L^* implies divisibility of its convex subgroup $\overline{v^*}L_0^*$, which now implies that $wL_0^* \cong \overline{v^*}L_0^*/\overline{\overline{v^*}}L_p^*$ is divisible as well. Further, L^*v^* is perfect by Pop's Lemma 3.2.10. Finally, L_0^* is complete by saturation. Hence, L_0^* is perfectoid and we can consider its tilt $(F, u) := (L_0^*, w)^\flat$, which is a field of characteristic p with absolute Galois group isomorphic to that of L_0^* by Theorem 3.2.20. Hence,

$$G_F \cong G_{L_0^*} \cong G_{L^*} \cong G_L.$$

In particular, all the untilts $F^\sharp$ of F are fields of characteristic 0 whose Galois groups are isomorphic to G_L. In general, untilts of a field are not unique but are instead parametrised by a one-dimensional curve known as the *Fargues–Fontaine curve*. However, in the setting of Case 4, the field L is elementarily determined by G_L, which implies that all untilts of F must be elementarily equivalent and, in particular, share the same algebraic part. It would be interesting to investigate whether the Fargues–Fontaine curve could be used to understand when this phenomenon occurs, and thereby yield further insights into the structure of L.

The local–global approach and the saturation–decomposition approach complement each other in that they rely on different properties of the fields L arising in Case 4. Both approaches make essential use of the fact that L carries a mixed-characteristic valuation v, that it is solvably closed, and that it is elementarily determined among fields of characteristic different from p. However, cohomological considerations are specific to the local–global approach, whereas the saturation–decomposition approach additionally exploits the smallness of G_L. To the best of our knowledge, there is no existing work on local–global principles that examines the role of small Galois groups, nor on the cohomological implications of tilting, although both directions appear to be interesting avenues for further investigation.

Bibliography

[AEJ87] Jón Kr. Arason, Richard Elman, and Bill Jacob. Rigid elements, valuations, and realization of Witt rings. *Journal of Algebra*, 110(2):449–467, 1987.

[AK65] James Ax and Simon Kochen. Diophantine problems over local fields II. A complete set of axioms for p-adic number theory. *American Journal of Mathematics*, 87(3):631–648, 1965.

[AS27a] Emil Artin and Otto Schreier. Algebraische Konstruktion reeller Körper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):85–99, 1927.

[AS27b] Emil Artin and Otto Schreier. Eine Kennzeichnung der reell abgeschlossenen Körper. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):225–231, 1927.

[BNH32] R. Brauer, E. Noether, and H. Hasse. Beweis eines Hauptsatzes in der Theorie der Algebren. *Journal für die reine und angewandte Mathematik*, 1932(167):399–404, 1932.

[Bor91] Armand Borel. *Linear Algebraic Groups*. Springer New York, 2nd enl. ed. edition, 1991.

[Brö76] Ludwig Bröcker. Characterization of fans and hereditarily pythagorean fields. *Mathematische Zeitschrift*, 151(2):149–163, 1976.

[BS65] A. Borel and J.-P. Serre. Théorèmes de finitude en cohomologie galoisienne. *Commentarii mathematici Helvetici*, 39:111–164, 1964/65.

[BSF13] Lior Bary-Soroker and Arno Fehm. Open problems in the theory of ample fields. In *Geometric and Differential Galois Theories*, volume 27 of *Séminaire et Congrès*, pages 1–11. Société Mathématique de France, Paris, 2013.

[CGR06] V. Chernousov, P. Gille, and Z. Reichstein. Resolving G-torsors by abelian base extensions. *Journal of Algebra*, 296(2):561–581, 2006.

[Chi08] Nancy Childress. *Class Field Theory*. Universitext. Springer New York, 2008.

[Con12] Brian Conrad. Finiteness theorems for algebraic groups over function fields. *Compositio Mathematica*, 148(2):555–639, 2012.

[CT11] Jean-Louis Colliot-Thélène. Quelques problèmes locaux-globaux. Exposé, Université Paris-Saclay, Institut de Mathématiques d'Orsay, Lille, France, 2011. Journée Douai.

[CTOP02] Jean-Louis Colliot-Thélène, Manuel Ojanguren, and Raman Parimala. Quadratic forms over fraction fields of two-dimensional henselian rings and Brauer groups of related schemes. In *Algebra, Arithmetic and Geometry (Mumbai, 2000)*, volume 16 of *Tata Inst. Fund. Res. Stud. Math.*, pages 185–217. Tata Institute of Fundamental Research, 2002.

[CTPS12] Jean-Louis Colliot-Thélène, Raman Parimala, and Venapally Suresh. Patching and local-global principles for homogeneous spaces over function fields of p-adic curves. *Commentarii Mathematici Helvetici*, 87(4):1011–1033, October 2012.

[Cul07] Lucas Culler. The Kronecker-Weber theorem. http://www.math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Culler.pdf, 2007.

[Dem61] Sergei P. Demushkin. The group of a maximal p-extension of a local field. *Izv. Akad. Nauk SSSR Ser. Mat.*, 25(3):329–346, 1961.

[Efr95a] I. Efrat. Orderings, valuations and free products of Galois groups. In *Séminaire de Structures Algébriques Ordonnées, Lecture Notes*, volume 54. University of Paris VII, 1995.

[Efr95b] Ido Efrat. Abelian subgroups of pro-2 galois groups. *Proceedings of the American Mathematical Society*, 123(4):1031–1035, 1995.

[Efr95c] Ido Efrat. A Galois-theoretic characterization of p-adically closed fields. *Israel Journal of Mathematics*, 91(1–3):273–284, 1995.

[Efr01] Ido Efrat. A hasse principle for function fields over pac fields. *Israel Journal of Mathematics*, 122(1):43–60, December 2001.

[Efr06] Ido Efrat. *Valuations, Orderings, and Milnor K-Theory*. American Mathematical Society, 2006.

[Efr25] Ido Efrat. The elementary type conjecture for maximal pro-p galois groups, 2025. https://arxiv.org/abs/2509.10168.

[EK98] Antonio J. Engler and Jochen Koenigsmann. Abelian subgroups of pro-p galois groups. *Transactions of the American Mathematical Society*, 350(6):2473–2485, 1998.

[EN94] Antonio J. Engler and J. B. Nogueira. Maximal abelian normal subgroups of Galois pro-2-groups. *Journal of Algebra*, 166(3):481–505, 1994.

[End72] Otto Endler. *Valuation Theory*. Springer Berlin Heidelberg, 1972.

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

[Ers65] Yu. L. Ershov. On elementary theories of local fields (Russian). *Algebra i Logika, Seminar*, 4(2):5–30, 1965.

[FJ08] Michael D Fried and Moshe Jarden. *Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer, Berlin, Germany, 3 edition, May 2008.

[Gey69] Wulf-Dieter Geyer. Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist. *Journal of Number Theory*, 1(3):346–374, 1969.

[GGW25] Claudio Gómez-Gonzáles and Jesse Wolfson. Solvable points on intersections of quadrics, cubics, and quartics, 2025. https://arxiv.org/abs/2508.00215.

[Gil10] Philippe Gille. Serre's Conjecture II: A survey. In Jean-Louis Colliot-Thélène, Skip Garibaldi, R. Sujatha, and Venapally Suresh, editors, *Quadratic Forms, Linear Algebraic Groups, and Cohomology*, Developments in Mathematics, pages 41–56. Springer New York, New York, NY, 1 edition, 2010.

[GKS] Leo Gitin, Jochen Koenigsmann, and Benedikt Stock. Elementary characterization of $\mathbb{Q}_p$ by its absolute Galois group — a modern perspective. https://arxiv.org/abs/2602.08095.

[GS06] Philippe Gille and Tamás Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[Gui18] Pierre Guillot. *A Gentle Course in Local Class Field Theory: Local Number Fields, Brauer Groups, Galois Cohomology*. Cambridge University Press, 2018.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer New York, 1977.

[Has31] H. Hasse. Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1931:64–69, 1931.

[Haz75] Michiel Hazewinkel. Local class field theory is easy. *Advances in Mathematics*, 18(2):148–181, 1975.

[HHK14] David Harbater, Julia Hartmann, and Daniel Krashen. Local-global principles for Galois cohomology. *Commentarii Mathematici Helvetici*, 89(1), 2014.

[HJ95] Yoon Sung Hwang and Bill Jacob. Brauer group analogues of results relating the Witt ring to valuations and Galois theory. *Canadian Journal of Mathematics*, 47(3):527–543, 1995.

[HKP21] David Harbater, Daniel Krashen, and Alena Pirutka. Local–global principles for curves over semi-global fields. *Bulletin of the London Mathematical Society*, 53(1):177–193, 2021.

[Hu12] Yong Hu. Local-global principle for quadratic forms over fraction fields of two-dimensional henselian domains. *Annales de l'Institut Fourier*, 62(6):2131–2143, 2012.

[Hu16] Yong Hu. A cohomological Hasse principle over two-dimensional local rings. *International Mathematics Research Notices*, 2017(14):4369–4397, 07 2016.

[Jac81] Bill Jacob. On the structure of Pythagorean fields. *Journal of Algebra*, 68(2):247–267, 1981.

[Jan16] Uwe Jannsen. Hasse principles for higher-dimensional fields. *Annals of Mathematics*, 183(1):1–71, January 2016.

[JK25] Franziska Jahnke and Konstantinos Kartas. Beyond the Fontaine-Wintenberger theorem. *Journal of the American Mathematical Society*, 38:997–1047, 2025.

[Kat86] Kazuya Kato. A Hasse principle for two dimensional global fields. *Journal für die reine und angewandte Mathematik*, 366:142–180, 1986.

[Kli74] Norbert Klingen. Elementar äquivalente Körper und ihre absolute Galoisgruppe. *Archiv der Mathematik*, 25(1):604–612, 1974.

[Koc75] Simon Kochen. The model theory of local fields. In G. H. Müller, A. Oberschelp, and K. Potthoff, editors, *ISILC Logic Conference, Proceedings of the International Summer Institute and Logic Colloquium, Kiel 1974*, volume 499 of *Lecture Notes in Mathematics*, pages 384–425. Springer-Verlag, 1975.

[Koe95] Jochen Koenigsmann. From p-rigid elements to valuations (with a Galois-characterization of p-adic fields). *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 465:165–182, 1995.

[Koe01] Jochen Koenigsmann. Solvable absolute Galois groups are metabelian. *Inventiones mathematicae*, 144(1):1–22, 2001.

[Koe03] Jochen Koenigsmann. Encoding valuations in absolute Galois groups. In *Valuation Theory and Its Applications, Volume II*, page 107–132. American Mathematical Society, 2003.

[Koe04] Jochen Koenigsmann. Elementary characterization of fields by their absolute Galois group. *Siberian Advances in Mathematics 14*, pages 16–42, 2004.

[Koe22] Jochen Koenigsmann. Encoding arithmetic in Galois groups, Trinity Term 2022. Lecture notes, available at https://www.maths.ox.ac.uk/people/jochen.koenigsmann.

[Koz90] Kazuhito Kozuka. On the local Kronecker-Weber theorem. *Archiv der Mathematik*, 54(2):162–163, 1990.

[KPR86] F.-V. Kuhlmann, M. Pank, and P. Roquette. Immediate and purely wild extensions of valued fields. *Manuscripta mathematica*, 55:39–68, 1986.

[KR23] Franz-Viktor Kuhlmann and Anna Rzepka. The valuation theory of deeply ramified fields and its connection with defect extensions. *Transactions of the American Mathematical Society*, 376(4):2693–2738, 2023.

[KS22] Jochen Koenigsmann and Benedikt Stock. An elementary proof of the local Kronecker-Weber theorem, 2022. https://arxiv.org/abs/2206.05801.

[KS24] J Koenigsmann and K Strommen. Recovering p-adic valuations from pro-p galois groups. *Journal of the London Mathematical Society*, 109(5), 2024.

[Lab66] John P. Labute. Demuškin groups of rank $\aleph_0$. *Bulletin de la Société Mathématique de France*, 94:211–244, 1966.

[Lan56] Serge Lang. Algebraic groups over finite fields. *American Journal of Mathematics*, 78(3):555–563, 1956.

[Lic69] Stephen Lichtenbaum. Duality theorems for curves over p-adic fields. *Inventiones mathematicae*, 7(2):120–136, 1969.

[LT58] Serge Lang and John Tate. Principal homogeneous spaces over abelian varieties. *American Journal of Mathematics*, 80(3):659–684, 1958.

[LvdD81] A. Lubotzky and L. van den Dries. Subgroups of free profinite groups and large subfields of $\widetilde{Q}$. *Israel Journal of Mathematics*, 39(1):25–45, 1981.

[Mar02] David Marker. *Model Theory: An Introduction*, volume 217 of *Graduate Texts in Mathematics*. Springer-Verlag, 2002.

[Moc97] Shinichi Mochizuki. A version of the Grothendieck conjecture for p-adic local fields. *International Journal of Mathematics*, 8(4):499–506, 1997.

[MS83] A S Merkur'ev and A A Suslin. k-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Mathematics of the USSR-Izvestiya*, 21(2):307–340, April 1983.

[MT85] O. V. Mel'nikov and O. I. Tavgen. The absolute Galois group of a henselian field. *Dokl. Akad. Nauk BSSR*, 29:581–583, 667, 1985. (in Russian).

[Neu68] Jürgen Neukirch. Über eine algebraische Kennzeichnung der Henselkörper. *Journal für die reine und angewandte Mathematik*, 1968(231):75–81, 1968.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Springer-Verlag, 1999.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Springer Berlin Heidelberg, 2008.

[Pop88] Florian Pop. Galoissche Kennzeichnung p-adisch abgeschlossener Körper. *Journal für die reine und angewandte Mathematik*, 392:145–175, 1988.

[PRR93] Vladimir Platonov, Andrei Rapinchuk, and Rachel Rowen. *Algebraic groups and number theory*, volume 139. Academic press, 1993.

[Pá04] Ambrus Pál. Solvable points on projective algebraic curves. *Canadian Journal of Mathematics*, 56(3):612–637, 2004.

[Pá13] Ambrus Pál. Solvable points on genus-one curves over local fields. *Journal of the Institute of Mathematics of Jussieu*, 12(1):31–42, 2013.

[Raw24] James Rawson. Some Obstructions to Solvable Points on Higher Genus Curves. *Journal de théorie des nombres de Bordeaux*, 36(3):1009–1019, 2024.

[Roq04] Peter Roquette. *The Brauer-Hasse-Noether Theorem in Historical Perspective*. Schriften der Mathematisch-naturwissenschaftlichen Klasse. Springer, Berlin, Germany, 2005 edition, November 2004.

[Ros81] Michael Rosen. An elementary proof of the local Kronecker-Weber theorem. *Transactions of the American Mathematical Society*, 265(2):599–605, 1981.

[Rot95] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics, 148. Springer New York, 4th ed. 1995. edition, 1995.

[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete; 3. Folge, v. 40. Springer, 2nd ed. edition, 2010.

[Sak20] Makoto Sakagaito. A note on Gersten's conjecture for étale cohomology over two-dimensional henselian regular local rings. *Comptes Rendus. Mathématique*, 358(1):33–39, 2020.

[Sch12] Peter Scholze. Perfectoid spaces. *Publications mathématiques de l'IHÉS*, 116(1):245–313, 2012.

[Sel51] Ernst S. Selmer. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Mathematica*, 85(0):203–362, 1951.

[Ser64] Jean-Pierre Serre. Structure de certains pro-p-groupes. In *Séminaire Bourbaki : années 1962/63 - 1963/64, exposés 241-276*, number 8 in Astérisque, pages 145–155. Société mathématique de France, 1964.

[Ser97] Jean-Pierre Serre. *Galois cohomology*. Springer-Verlag, 1997.

[Sha47] Igor Shafarevich. On p-extensions. *Rec. Math. [Mat. Sbornik] N.S.*, 62(2):351–363, 1947.

[Spi96] Michael Spiess. An arithmetic proof of Pop's Theorem concerning Galois groups of function fields over number fields. *Journal für die reine und angewandte Mathematik*, 478:107–126, 1996.

[Ste65] Robert Steinberg. Regular elements of semisimple algebraic groups. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 25(1):49–80, 1965.

[Sza09] Tamás Szamuely. *Galois Groups and Fundamental Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2009.

[Voe11] Vladimir Voevodsky. On motivic cohomology with $\mathbf{Z}/l$-coefficients. *Annals of Mathematics*, 174(1):401–438, 2011.

[War81] Roger Ware. Valuation rings and rigid elements in fields. *Canadian Journal of Mathematics*, 33(6):1338–1355, 1981.

[War92] Roger Ware. Galois groups of maximal p-extensions. *Transactions of the American Mathematical Society*, 333(2):721–728, 1992.

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer New York, 1997.

[WÇ08] Andrew Wiles and Mirela Çiperiani. Solvable points on genus one curves. *Duke Mathematical Journal*, 142(3):381 – 464, 2008.

[Wie95] Götz Wiesend. Lokal-Global-Prinzipien für die Brauergruppe. *Manuscripta Mathematica*, 86(1):455–466, December 1995.

[Wit37] Ernst Witt. Schiefkörper über diskret bewerteten Körpern. *Journal für die reine und angewandte Mathematik*, 176:153–156, 1937.

[Woo16] Trevor D. Wooley. Solvable points on smooth projective varieties. *Monatshefte für Mathematik*, 180(2):391–403, 2016.