Galois Groups and Anabelian Reconstruction

Kristian John Strømmen

Keble College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy in Mathematics

Trinity 2015

This thesis is dedicated to Amy, with love.

Acknowledgements

This thesis would not have been possible without the continuous and invaluable support of my supervisor, Dr. Jochen Koenigsmann. I am very grateful to have received both his mathematical advice and his general encouragement.

This thesis has also profited from conversations with several of my colleagues, including Jan Vonk, Netan Dogra, and Emily Cliff. I would like to thank Emily in particular for going through the painful last stages of this thesis alongside me, and for numerous useful sessions of mutual complaining. Chapter 5 benefited in particular from numerous conversations with Alfonso Ruiz Guido, as well as several stimulating conversations with Prof. Boris Zilber. I would also like to thank Prof. Angus MacIntyre for taking time out of his busy schedule to meet with me on the topics of that chapter. This thesis also benefited from several insightful comments from Professor Jonathan Pila and Professor Jakob Stix.

I also wish to thank my family. In particular, my parents for their unconditional love and support, Sigrid for her lessons on lateral thinking, and Hannah for listening to my moaning on the phone. Finally, I wish to thank Amy Bilderbeck, for making life a constant joy, even during the most frustrating moments of work. You made it all worth it.

Abstract

In this thesis we investigate the problem of recovering arithmetic structure of a field F from small quotients of its absolute Galois group. In particular, we are interested in recovering the p-adic valuation on a p-adic field from such quotients. After establishing several such results, we apply this to obtain strong versions of the Birational Section Conjecture for curves over p-adic fields. We also discuss the model-theoretic interpretation of these results, as well as begin investigating the foundations of a model-theory of schemes.

Contents

Introduction

One of the most fruitful philosophies of modern number theory has been that one can understand the arithmetic of a field K by understanding the structure of its absolute Galois group $G_K := \mathrm{Gal(K^{sep}/K)}$. An influential early result of Neukirch ([21]) states that when K is a number field, G_K actually determines K completely. More precisely, if K_1 and K_2 are number fields, then $G_{K_1} \simeq G_{K_2} \iff K_1 \simeq K_2$. Pop later generalized this ([24]) to any two fields finitely generated over $\mathbb{Q}$. A similar result for p-adic local fields was obtained by Mochizuki in [19], provided one also adds in the information coming from the canonical filtration. Results like these which determine concretely what arithmetic structure is determined by G_K are usually referred to as 'anabelian' type results, after the yoga of anabelian geometry laid out by Grothendieck in his famous Esquisse d'un Programme (see the appendix in [31]). In this tour de force, Grothendieck greatly enlarges the scope of the above philosophy to the world of schemes. He conjectures the existence of a category of so-called 'anabelian schemes', the defining feature of which is that every object X in it should be determined up to isomorphism by its étale fundamental group $\pi_1^{et}(X)$. In the case when $X = Spec(K)$, K a field, then $\pi_1^{et}(X) \simeq G_K$ and so number fields constitute the first examples of anabelian schemes. Grothendieck also conjectured that hyperbolic curves X defined over number fields are anabelian: this was proved by Tamagawa for affine curves and by Mochizuki in full generality (see [37], [18], and also [20] for an excellent exposition of these results).

The other main conjecture put forward by Grothendieck was the so-called 'Section Conjecture'. For any hyperbolic curve X defined over a field K, where K is either a number field or a finite extension of a p-adic field, one can associate in a canonical manner an exact sequence[1]

$$1 \to \pi_1^{et}(\overline{X}) \to \pi_1^{et}(X) \to G_K \to 1 \tag{1}$$

where $\overline{X} = X \otimes_K K^{sep}$ is the base-change of X to K^{sep}. By functoriality of π_1, a K-rational point $a \in X(K)$ gives rise to a section $s : G_K \to \pi_1^{et}(X)$ of this sequence which is unique up to conjugation by elements in $\pi_1^{et}(\overline{X})$. The Section Conjecture states that conversely, every section of (1) is induced by a unique rational point, thereby establishing a bijection between $X(K)$ and (conjugacy classes of) sections of (1). This conjecture has potentially far-reaching consequences in arithmetic geometry, in particular when it comes to effective versions of Faltings' Theorem, as in the work on non-abelian Chabauty by Kim (see his chapter in [1]). Unfortunately, this conjecture remains entirely open and mysterious, although some strong partial results have been obtained ([27]). More well-understood is the so-called Birational Section Conjecture (hereby shortened to just 'BSC'), which replaces the exact sequence (1) with the following exact sequence:

$$1 \to G_{\overline{K}(X)} \to G_{K(X)} \to G_K \to 1 \tag{2}$$

where $K(X)$ is the function field of X. Since $\pi_1^{et}(X)$ is a small quotient of $G_{K(X)}$, one could hope that the extra structure available makes matters more tractable. Indeed, the first positive result obtained was a proof in [13] of the BSC for curves over p-adic fields. The main motivating goal of this thesis is about strengthening this result, by replacing the Galois groups occuring in (2) with very small quotients. Such strengthenings are clearly desirable from the perspective of applications: the absolute Galois group of a field is very big and complex, so being able to replace it with a very small quotient makes the possibility of an algorithmic approach to finding rational points on hyperbolic curves much more feasible.

The proof of the p-adic BSC has its origin in a different strand of 'anabelian' style results, namely those inspired by model theory. The classical result here, by Artin-Schreier et. al., says that a field K is real-closed if and only if $G_K \simeq \mathbb{Z}/2\mathbb{Z}$.

[1] Note that we will suppress any mention of base-points as they will not be important in our work.

The analogous result for p-adically closed fields was obtained in [10]. In particular, one finds that $G_K \simeq G_{\mathbb{Q}_p}$ if and only if K and $\mathbb{Q}_p$ are elementarily equivalent in the language of rings. The fact that the existence of a K-rational point on a curve is a first-order statement about the field K is the crucial observation which leads to a proof of the BSC. In both the case of real-closed fields and p-adically closed fields, the idea is to show that the abstract group-theoretic structure of the Galois group encodes the existence of an ordering, respectively a henselian valuation, and that these in turn determine the arithmetic of the field. For this reason the majority of this thesis is dedicated to recovering the existence of certain valuations from small amounts of Galois theoretic data. That is, given an abstract isomorphism of quotients of absolute Galois groups

$$G_K^c \simeq G_F^c$$

where F is a p-adic field, we will study to what extent the p-adic valuation on F can be transported to K. Once this can be done to a suitably strong degree, the BSC will follow more or less as a formality.

The quotients of G_K we will be studying are different pro-l quotients, where l is a prime. These are natural to study since for p-adic fields, these quotients are well understood group-theoretically, and their study was already an important part of the circle of ideas discussed above. In addition, a detailed understanding of these quotients is an essential part of the programme of completely classifying all pro-p Galois groups, which would be a major step towards the inverse Galois problem.

The thesis is organized as follows:

Chapter 1 provides some technical preliminaries and definitions which will be used in the thesis.

In **Chapter 2**, we introduce the formalism of 'canonical valuations'. This formalism, which should be of interest more broadly in valuation theory, shows how, given certain 'canonical' quotients of G_K, one can produce a Galois-theoretic characterisation for the existence of 'nice' valuations on K. In particular, we show how the maximal (p, q)-quotient[2] of a p-adic field already recovers the p-adic valuation up to

[2] See Section 1.2.

some indeterminacy of the residue field, and that the maximal pro-solvable quotient recovers it entirely.

Chapter 3 is devoted to the proof that if K is any field with $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$, then K admits a 2-henselian valuation with residue field $\mathbb{F}_2$, value group Γ discrete with $v(2)$ minimal positive, and $[\Gamma : 2\Gamma] = 2$. This involves the development of a new technique which we call 'norm combinatorics'. We discuss the wider conjecture of which this is a special case, and discuss the model-theoretic interpretation of this result.

In **Chapter 4**, we discuss the Birational Section Conjecture, and use the results of Chapter 2 and 3 to obtain strong versions of this. We also discuss the model-theoretic nature of the conjecture.

Chapter 5 moves in a very different direction. The proof of the Birational Section Conjecture for p-adic fields suggests that one possible long-term strategy to proving the full Section Conjecture is to develop a meaningful notion of the model theory of schemes. We outline the potential first steps of such a theory, by providing a framework within which to discuss schemes as model-theoretic objects, and prove some basic structural results, including a quantifier elimination statement. We also discuss the connection with Zariski geometries.

The **Appendix** at the end contains the calculations omitted from Chapter 3.

Chapter 1

Preliminaries

We recall some preliminary results and definitions which we will use later.

1.1 Galois cohomology, Kummer theory and Brauer groups

General references for these topics are [33] and [6].

Let p be a prime, G a pro-p group with rank n. That is, n is the minimal number of topological generators of G. Let $H^i(G) := H^i(G, \mathbb{Z}/p\mathbb{Z})$, $i \in \mathbb{N}$.

Proposition 1.1.1. *$H^i(G)$ is an $\mathbb{F}_p$-vector space. The $\mathbb{F}_p$-dimension of $H^1(G)$ equals the rank of G, while the dimension of $H^2(G)$ equals the minimal number of relations among a minimal set of generators of G.*

Proof. See [33] Chapter 2. □

Definition 1.1.2. Let p be prime. For a field F and $a \in F^\times \setminus (F^\times)^p$, define

$$N_F(a) := Norm_{F(\sqrt[p]{a})/F}(F(\sqrt[p]{a})^\times)$$

and $N_F(1) := F^\times$.

Since $F(\sqrt[p]{a}) = F(\sqrt[p]{b})$ whenever $a/b \in (F^\times)^p$, we will by abuse of notation also write $N_F(a)$ for $a \in F^\times/(F^\times)^p$, with a denoting both an element of $F^\times$ and its class modulo p-th powers.

Remark 1.1.3. If the base-field in question is clear, we will just write $N(a)$ for ease of notation.

Now suppose $G = G_K(p)$, the maximal pro-p quotient of G_K, is finitely generated, where K is a field containing ζ_p, a primitive p-th root of unity. Then Kummer Theory provides an isomorphism

$$H^1(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq K^\times/(K^\times)^p$$

and the theory of Brauer groups, along with the Merkurjev-Suslin Theorem, gives

$$H^2(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq {}_pBr(K) \simeq (\mathbb{Z}/p\mathbb{Z})^n$$

for some $n < \infty$, where ${}_pBr(K)$ is the p-torsion subgroup of the Brauer group of K. The cup-product pairing can be identified with the Hilbert symbol

$$K^\times/(K^\times)^p \times K^\times/(K^\times)^p \to (\mathbb{Z}/p\mathbb{Z})^n$$

sending the pair a, b to the symbol $(a, b)_K$ corresponding to the central simple K-algebra with generators x, y subject to the relations $x^p = a, y^p = b, xy = \zeta_p yx$. We have $(a, b)_K = 1$ iff $a \in N(b)$ iff $b \in N(a)$.

We will want to make use of a strengthening of the above observation. To this end we first make the following definition:

Definition 1.1.4. Given a field K containing ζ_p, let K' denote the maximal $\mathbb{Z}/p\mathbb{Z}$ elementary abelian extension of K: thus $K' = K(\sqrt[p]{K^\times})$. Let K'' denote the maximal $\mathbb{Z}/p\mathbb{Z}$ elementary meta-abelian extension of K. That is, $K'' = (K')'$.

If $G = G_K(p)$, we let $G' := \mathrm{Gal(K'/K)}$, $G'' := \mathrm{Gal(K''/K)}$.

Proposition 1.1.5. *Let $G = G_K(p)$ where K is a field containing ζ_p. Then*

(i) $H^1(G) \simeq H^1(G') \simeq K^\times/(K^\times)^p$*;*

(ii) *Given $a, b \in H^1(G)$, we have that $a \cup b = 0$ in $H^2(G)$ if and only if $a \cup b = 0$ in $H^2(G'')$.*

In particular, given a, b in $K^\times/(K^\times)^p$, whether or not $(a,b)_K$ is 1 or $\neq 1$ can be read off G''.

Proof. Part (i) is just Kummer theory. For part (ii), see [25], Lemma 1. □

We will also recall some basic facts about the cohomological dimension $cd(G)$ of a pro-p group G.

Proposition 1.1.6. *Let G be a pro-p group. Then*

(i) *$cd(G) \leq n$ if and only if $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$;*

(ii) *$cd(G) = 1$ if and only if G is a free pro-p group;*

(iii) *If $G = G_K(p)$, where K is a field containing ζ_p, then $cd(G) = 1$ if and only if for every $a \in K^\times \setminus (K^\times)^p$, the norm map*

$$N_{L/F} : L^\times \to K^\times$$

is surjective, where $L = K(\sqrt[p]{a})$. Equivalently, ${}_pBr(K) = 0$.

Proof. The first two items are standard (see [33]). For the last claim, Merkurjev-Suslin tells us that there is an isomorphism $H^2(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq {}_pBr(K)$ and that ${}_pBr(K)$ is generated by the symbols $(a,b)_K$, which are trivial exactly when $b \in N(a)$. □

1.2 Notions of henselianity

A general reference for this and anything else to do with valuations is [4].

Given a valuation v on a field K, we denote by its valuation ring by $\mathcal{O}_v$, its value group as Γ_v, its maximal ideal as $\mathcal{M}_v$, and its residue field by Kv. If $a \in \mathcal{O}_v$, we let $\bar{a}$ denote its image in Kv, and likewise if $f \in \mathcal{O}_v[x]$.

Definition 1.2.1. Let H be a field extension of K. Then we say that v is H-henselian if v has a unique extension to H.

Lemma 1.2.2. *(Hensel's Lemma) The following are equivalent:*

(i) v is H-henselian;

(ii) Let $f \in \mathcal{O}_v[x]$ be a polynomial which splits in H. Then for every $a \in \mathcal{O}_v$ with $\bar{f}(\bar{a}) = 0$ and $\bar{f}'(\bar{a}) \neq 0$, there exists $\alpha \in \mathcal{O}_v$ with $f(\alpha) = 0$ and $\bar{\alpha} = \bar{a}$.

(iii) Suppose the polynomial $x^n + x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0 \in \mathcal{O}_v[x]$, with $a_{n-2}, \ldots, a_0 \in \mathcal{M}_v$, splits in H. Then it has a zero in K.

Remark 1.2.3. Note that given any valued field (K, v), we can always find an H-henselization of it, that is, an immediate extension (K^h, v^h) of valued fields such that v^h is H-henselian.

The following choices of H will be of crucial importance in the rest of this thesis:

- $H = K^{sep}$. In this case we call an H-henselian valuation simply *henselian*.
- $H = K(p)$, the maximal p-power extension of K for some prime p (that is, the compositum of all Galois extensions of K of degree p^n for some n). In this case we call a H-henselian valuation *p-henselian*.
- $H = K(p, q)$: the compositum of all Galois extensions of K of degree $p^n q^m$. We call this the maximal (p, q)-extension of K. In this case an H-henselian valuation is called (p, q)-henselian.
- $H = K^{solv}$: the maximal pro-solvable extension of K. In this case we call a H-henselian valuation *solv-henselian*.

In the case of p-henselianity we have the following useful observation (see [4], Theorem 4.2.2).

Lemma 1.2.4. *A valuation v on a field K is p-henselian if and only if it extends uniquely to every Galois extension of K of degree p.*

We also record the following less known but very powerful 'absolute' version of Hensel's Lemma.

Lemma 1.2.5. *(Hensel-Rychlik) A valuation v on a field K is p-henselian if and only if for every $f \in \mathcal{O}_v[x]$ which splits in $K(p)$, whenever there exists $b \in K$ with $v(f(b)) > v(disc(f))$, then f has a root in K (not necessarily equal to b).*

Proof. See [14], Chapter 9, section 9.4. It is easy to check that the proof follows if we replace henselianity with p-henselianity as long as the polynomial splits in the p-closure. □

1.3 p-adically closed fields

The results of this section can all be found in [28].

We recall the main definitions and facts about formally p-adic fields and p-adically closed fields. In all that follows, p is a prime.

Definition 1.3.1. A valuation v on a field K is called *formally p-adic*, or just p-adic, if Kv is a finite field of characteristic p with p^{f_v} elements, and Γ_v has a minimal positive element α such that $v(p) = e_v\alpha$ for some natural number $e_v > 0$. The number $d_v := e_v f_v$ is called the *p-adic rank* of v.

Definition 1.3.2. Let K be a field with a p-adic valuation v. Then K is called *p-adically closed* if it has no proper, finite immediate extensions.

The canonical examples of such fields are $\mathbb{Q}_p$, $\mathbb{Q}_p \cap \overline{\mathbb{Q}}$, and finite extensions of both. Note that $\mathbb{Q}_p \cap \overline{\mathbb{Q}}$ is the henselization of $\mathbb{Q}$ with respect to the p-adic valuation.

We have the following equivalent characterisation.

Lemma 1.3.3. *Given a p-adic valuation v on a field K, let w denote the unique coarsening*[1] *of v with valuation ring $\mathcal{O}_v[1/p]$. Then K is p-adically closed if and only if v is henselian and Γ_w is divisible.*

[1] Recall that given two valuation rings $\mathcal{O}$ and $\mathcal{O}'$, $\mathcal{O}$ is said to be 'coarser' than $\mathcal{O}'$ if $\mathcal{O}' \subset \mathcal{O}$.

Given a p-adic valuation on a field one can always 'p-adically close' the field.

Lemma 1.3.4. *Let K be a field with a p-adic valuation v. Then there exists a field $\tilde{K}$ over K and an extension $\tilde{v}$ of v such that $\tilde{v}$ is p-adic and $\tilde{K}$ is p-adically closed.*

The notion of p-adically closed fields captures the first-order theory of the p-adic fields, as the next lemma shows.

Lemma 1.3.5. *If (K, v) is p-adically closed field, and k is a subfield relatively algebraically closed in K, then $w := v \restriction_k$ is a p-adic valuation on k. Furthermore, (k, w) is p-adically closed, v and w have the same p-adic rank, and K is elementarily equivalent to k in the ring-language.*

In particular, if (K, v) is p-adically closed then K is elementarily equivalent to a finite extension of $\mathbb{Q}_p$. Indeed, if we put[2] $k := K \cap \overline{\mathbb{Q}}$, then by the above Lemma, k admits a p-adic valuation w of the same rank as v. The completion of k with respect to w is a finite extension F of $\mathbb{Q}_p$, again with the same p-adic rank, and is of course p-adically closed. Hence by Lemma 1.3.5, K is elementarily equivalent to k, which is itself elementarily equivalent to F, and so K is elementarily equivalent to F.

[2] Note that any field admitting a p-adic valuation must have characteristic 0 since the residue characteristic is p and $v(p)$ is finite.

Chapter 2

Canonical Valuations

In this chapter we aim to prove that the p-adic valuation on a finite extension F of $\mathbb{Q}_p$ is encoded in a very small quotient of G_F. We will show that the maximal pro-solvable quotient G_F^{solv} encodes the valuation precisely, while the maximal (p, q)-quotient $G_F(p, q)$ encodes it up to some indeterminacy of the residue field. We even show that a very small quotient of $G_F(p, q)$ already suffices for this purpose.

The techniques here are based upon the fundamental characterization in [12]. With F as above, provided F contains ζ_l, where l is a prime not equal to p, then one can show that

$$G_F(l) \simeq \mathbb{Z}_l \rtimes \mathbb{Z}_l.$$

In [12] it is shown that any field L with the same maximal pro-l quotient must admit an l-henselian valuation so-called tamely branching at l. Since l is arbitrary, it is clear that this criterion alone cannot recover a fully p-adic valuation. We aim to show that as soon as you add in some knowledge of p-power extensions in the Galois group, you can recover it almost completely. This will allow us to strengthen the main results of [10] and [12]. To do so we will introduce the formalism of 'canonical valuations'. As we shall see, once this formalism has been set up, the proofs from the original cases follow also in this more general setting. Let us say a few words about this formalism.

Given a field which has at least one non-trivial henselian valuation, it is possible (see [4] p. 103) to single out a distinguished such valuation, referred to as the *canonical* *henselian valuation*. The properties enjoyed by this valuation ensure that it behaves nicely upon restriction to subfields. As a consequence, one can show that if L/K is finite or normal, then the existence of a non-trivial henselian valuation on L descends to K. One can analogously define a notion of a canonical p-henselian valuation (see [12]). In this chapter we will realize both these notions as special cases of a more general framework, namely that of *canonical valuations*.

We will then apply this formalism to deduce a Galois theoretic characterization of certain non-trivial valuations. Finally, we will apply this in the case of a p-adic field F to recover p-adic valuations from small quotients of the absolute Galois group.

2.1 Canonical classes

Definition 2.1.1. Let $\mathcal{C}$ be a class of finite groups closed under extensions, subgroups and quotients. If G is a profinite group, we let G^c denote the maximal pro-$\mathcal{C}$ quotient of G. If $G = G_K$, we define K^c to be the unique subextension of K^{sep} with $G_K^c = \mathrm{Gal(K^c/K)}$. For any field K, we let $\mathcal{C}(K)$ denote the set of Galois subextensions of K^c/K.

By Galois theory, the following properties are immediate:

(i) If $L, F \in \mathcal{C}(K)$ then the compositum $LF \in \mathcal{C}(K)$;

(ii) If $L \in \mathcal{C}(K)$ and F/K is a subfield of L, then $F \in \mathcal{C}(K)$;

(iii) If $L \in \mathcal{C}(K)$ and $M \in \mathcal{C}(L)$ then $M \in \mathcal{C}(K)$;

(iv) $(K^c)^c = K^c$.

From now on $\mathcal{C}$ will always refer to such a class.

Definition 2.1.2. A valuation on K which is K^c-henselian with respect to a class $\mathcal{C}$ is called $\mathcal{C}$-henselian or simply *c-henselian*. We also say that K is c-closed if $K = K^c$.

We have the following proto-typical examples:

- $\mathcal{C} = \mathcal{C}_{sep}$, the class of all finite groups. Then $K^c = K^{sep}$ and c-henselianity is the same as henselianity.
- $\mathcal{C} = \mathcal{C}_p$, the class of all p-groups. Then $K^c = K(p)$ and c-henselianity is the same as p-henselianity.
- $\mathcal{C} = \mathcal{C}_{solv}$, the class of all solvable finite groups. Then we write $K^c = K^{solv}$, and call a c-henselian valuation *solv-henselian.*

Definition 2.1.3. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two classes. We say that $\mathcal{C}_1$ *contains* $\mathcal{C}_2$ if, for any profinite group G, G^{c_2} is obtained from G^{c_1} as the quotient by a characteristic subgroup. Note that in this case, the class of finite groups in $\mathcal{C}_1$ actually contains the finite groups in $\mathcal{C}_2$.

On the field-theory side, if $\mathcal{C}_1$ contains $\mathcal{C}_2$, then for any field K, if $L \in \mathcal{C}_2(K)$, also $L \in \mathcal{C}_1(K)$.

Example 2.1.4. We have that $\mathcal{C}_{solv}$ contains $\mathcal{C}_p$ for any p. Indeed, let G^p denote the maximal pro-p quotient, and G^s the maximal solvable quotient. Then G^p is the quotient of G^s by the normal subgroup generated by all its Sylow q subgroups, $q \neq p$, which is characteristic (since any automorphism sends a Sylow q-subgroup to another Sylow q-subgroup).

Since isomorphisms descend to quotients by characteristic subgroups, we get that if $\mathcal{C}_1$ contains $\mathcal{C}_2$, then

$$G_F^{c_1} \simeq G_K^{c_1} \Rightarrow G_F^{c_2} \simeq G_K^{c_2}$$

for any two fields F and K.

Definition 2.1.5. Call a class $\mathcal{C}$ *canonical* if the following conditions hold for any field K.

(L) Let v be a c-henselian valuation on K, and assume $K^c v/Kv$ is separable. Then $K^c v \in \mathcal{C}(Kv)$, and for any $L \in \mathcal{C}(Kv)$, there exists a (not necessarily unique) $L' \in \mathcal{C}(K)$ such that $L'w = L$, where w is the unique extension of v. In particular, if $K^c = K$ then $(Kv)^c = (K^c)v = Kv$.

(S) If $\mathcal{O}_1$ and $\mathcal{O}_2$ are two independent c-henselian valuations on a field K, then $K = K^c$.

(R) If K^c is a finite extension of K, then $[K^c : K] \leq 2$.

Note: From now on, when we refer to a class $\mathcal{C}$ it will always refer to a canonical class, and a c-henselian valuation will always be with respect to some canonical class $\mathcal{C}$.

As indicated (see [4] p.103 and [12]), we have the following known result:

Fact 2.1.6. *The classes $\mathcal{C}_{sep}$ and $\mathcal{C}_p$ are canonical.*

Remark 2.1.7. To explain condition (R), recall the following classical results: K is real-closed (resp. Euclidean) if and only if $\overline{K}$ (resp. $K(2)$) is a finite, non-trivial extension of K, and in this case, the extension is of degree 2. Therefore this condition will allow us to keep close control over the behaviour of K in the unusual cases where K^c is a finite extension of K.

The following simple observation is crucial:

Proposition 2.1.8. *Let $\mathcal{C}_{solv}$ be the class of solvable finite groups. Then $\mathcal{C}_{solv}$ is a canonical class.*

Proof. Since $\mathcal{C}_{solv}$ is closed under extensions, subgroups and quotients, it is a class in the sense of this chapter. It remains to show that this class is canonical.

Suppose v is a solv-henselian valuation on a field K. We need to show that we can lift solvable Galois extensions of Kv to solvable Galois extensions of K. By Galois theory, the solvable Galois extensions are exactly the radical ones. Since v is solv-henselian, and every Galois extension of degree p is solvable, v is p-henselian for every prime p, by Lemma 1.2.4. Since $\mathcal{C}_p$ is canonical, any Galois extension of degree p of

Kv can be lifted to K. Because any radical Galois extension can be written as a succession of extensions of prime degree, we can thus lift any radical Galois extension of Kv to K. Note that for a field of characteristic p, a radical extension of degree p is to be interpreted as an Artin-Schreier extension of degree p, i.e., an extension obtained by adjoining the roots of a polynomial of the form $x^p - x - a$. In the case when the valued field (K, v) is of mixed characteristic $(0, p)$, assuming $\zeta_p \in K$, then such extensions of the residue field become 'actual' radical extensions of K, namely the extension of degree p obtained by adjoining a p-th root of $1 + (\zeta_p - 1)^p a$. Hence $\mathcal{C}_{solv}$ satisfies property (L).

Next, suppose v_1 and v_2 are two independent solv-henselian valuations on a field K. As remarked in the above argument, v_1 and v_2 are in particular p-henselian for every prime p. Since $\mathcal{C}_p$ is a canonical class, it follows that K does not admit any non-trivial extensions of degree p. Hence it does not admit any radical extensions, whence $K = K^c$, implying that $\mathcal{C}_{solv}$ satisfies property (S).

Finally, if $[K^c : K] < \infty$, then $[K(p) : K] < \infty$ for every prime p. Again using that $\mathcal{C}_p$ is canonical, we find that $K^c = K(2)$ and $[K(2) : K] \leq 2$. Hence $\mathcal{C}_{solv}$ satisfies (R). □

In an entirely analogous fashion we can prove the following:

Proposition 2.1.9. *Given two primes p, q, let $\mathcal{C}_{p,q}$ be the class of finite (p, q)-groups, i.e., groups of cardinality $p^n q^m$ for some n, m. Then $\mathcal{C}_{p,q}$ is a canonical class.*

We shall see that $\mathcal{C}$-henselian valuations with respect to a canonical class $\mathcal{C}$ admit a notion of a canonical c-henselian valuation. The first property we will need in this direction is that c-henselianity behaves well with respect to compositions of valuations. Indeed, let v_1 and v_2 be valuations on a field K with valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively. If $\mathcal{O}_1 \subset \mathcal{O}_2$, so v_2 is a coarsening of v_1, we get an 'exact sequence of valuations

$$1 \to v_2 \to v_1 \to v_1/v_2 \to 1 \tag{2.1}$$

Here v_1/v_2 is the induced valuation on Kv_2 with valuation ring $\overline{\mathcal{O}_1} := \mathcal{O}_1/\mathcal{M}_2$ and maximal ideal $\overline{\mathcal{M}_1} := \mathcal{M}_1/\mathcal{M}_2$. The 'lifting' property (L) is the key to the following

Lemma 2.1.10. *Given an exact sequence of valuations as above, then v_1 is c-henselian if and only if v_2 and v_1/v_2 is.*

Proof. Suppose v_1 is c-henselian. Let

$$f = x^n + x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_0 \in O_2[x]$$

be such that $a_i \in \mathcal{M}_2$. If f splits in K^c then since $\mathcal{M}_2 \subset \mathcal{M}_1$, Lemma 1.2.2 implies that f has a zero in K and so v_2 is c-henselian. Next, assume that $\bar{a}_i \in \mathcal{M}_1/\mathcal{M}_2$, and suppose $\bar{f}$ splits in $Kv_1^c = (K^c)v_1$. We may assume that f splits in K^c. Indeed, without loss of generality suppose f is irreducible. If $\bar{f}(\alpha) = 0$ for $\alpha \in (Kv)^c$, then by property (L), there is an extension $F \in \mathcal{C}(K)$ such that Fv is the splitting field of $\bar{f}$. Then we can simply replace f by the minimal polynomial of $a \in F$ with $\bar{a} = \alpha$. Hence f has a zero in $\mathcal{O}_1$ by c-henselianity, and so also in Kv_1. Thus v_2 and v_1/v_2 are both c-henselian.

The other direction is straightforward. Let $f \in \mathcal{O}_1[x]$ be a polynomial which splits in K^c and has a root in Kv_1. Then using c-henselianity of first v_1/v_2 and then v_2 one lifts the root first to $\mathcal{O}_1/\mathcal{M}_1$ and then to K. □

2.2 Constructing the canonical c-henselian valuation

We mimic the classical construction.

Definition 2.2.1. Define subsets C_1 and C_2 of the set of all valuation rings of a field by

$$\begin{aligned} C_1 &:= \{\mathcal{O} : \mathcal{O} \text{ is } c\text{-henselian and } \mathcal{O}/\mathcal{M} \text{ is not } c\text{-closed}\} \\ C_2 &:= \{\mathcal{O} : \mathcal{O} \text{ is } c\text{-henselian and } \mathcal{O}/\mathcal{M} \text{ is } c\text{-closed}\}. \end{aligned}$$

If we want to emphasize the ambient field in question, we write $C_1(K)$, resp. $C_2(K)$.

Note: Since K itself is always a c-henselian valuation ring of K, the set $C_1 \cup C_2$ is never empty.

Remark 2.2.2. Suppose that $\mathcal{O} \subset \mathcal{O}'$ are valuation rings of K and $\mathcal{O}'$ has c-closed residue field $\mathcal{O}'/\mathcal{M}'$. Then by the Lifting Property (L), we know that the valuation ring $\mathcal{O}/\mathcal{M}'$ of $\mathcal{O}'/\mathcal{M}'$ has c-closed residue field $\mathcal{O}/\mathcal{M}$. Hence $\mathcal{O}$ also has a c-closed residue field.

Recall that two valuation rings $\mathcal{O}$ and $\mathcal{O}'$ are called 'comparable' if one is a subset of the other.

Proposition 2.2.3. *Any two valuation rings from C_1 are comparable. If C_2 is non-empty, then C_2 contains a valuation ring which is coarser than every valuation ring from C_2 and strictly finer than every valuation ring from C_1. If C_2 is empty, then there is a finest valuation ring in C_1.*

Proof. We first show that two rings from C_1 are always comparable. Indeed, assume $\mathcal{O}_1, \mathcal{O}_2$ are incomparable c-henselian valuations. We will show that they are both in C_2, i.e. they have c-closed residue fields. It follows from the assumed incomparability that $\mathcal{O} := \mathcal{O}_1\mathcal{O}_2$ is a proper coarsening of $\mathcal{O}_1$ and $\mathcal{O}_2$ and that the valuation rings $\mathcal{O}_1/\mathcal{M}$ and $\mathcal{O}_2/\mathcal{M}$ of $\mathcal{O}/\mathcal{M}$ are independent. Furthermore, by Lemma 2.1.10, they are both c-henselian. Thus by the (S)-property of $\mathcal{C}$, $\mathcal{O}/\mathcal{M}$ is c-closed. By Remark 2.2.2, the residue fields of $\mathcal{O}_1$ and $\mathcal{O}_2$ are also c-closed: that is, they are in C_2.

Now, if C_1 is non-empty, then since all rings in C_1 are comparable, the intersection $\mathcal{O}^* := \bigcap_{\mathcal{O} \in C_1} \mathcal{O}$ is a valuation ring with maximal ideal $\bigcup_{C_1} \mathcal{M}$, which is clearly finer than every valuation ring in C_1. By Lemma 1.2.2, it is easy to see that $\mathcal{O}^*$ is c-henselian, so if $C_2 = \emptyset$, then $\mathcal{O}^*$ is a finest valuation ring in C_1, proving the last claim of the proposition.

Next suppose $C_2 \neq \emptyset$. Then a simple Zorn's Lemma construction shows that C_2 has a maximal element $\mathcal{O}^{**}$. Property (S) implies this element is unique. For supposing $\mathcal{O}_1$ and $\mathcal{O}_2$ are two distinct maximal elements, then their compositum $\mathcal{O}_3 := \mathcal{O}_1\mathcal{O}_2$ is c-henselian and Kv_3 has two independent c-henselian valuation rings $\mathcal{O}_1/\mathcal{M}_3$ and $\mathcal{O}_2/\mathcal{M}_3$. Hence $\mathcal{O}_3$ is in C_2, contradicting maximality. □

Definition 2.2.4. The *canonical c-henselian valuation* of K, denoted by $\mathcal{O}_c$ (or v_c), is defined to be $\mathcal{O}^*$ if $C_2 = \emptyset$, and $\mathcal{O}^{**}$ otherwise. We also put

$$C := C_1 \cup \{\mathcal{O}_c\}.$$

Thus the canonical c-henselian valuation is the finest valuation ring in C. If we want to emphasize the ambient field, we write $C(K)$.

The point of this construction is that the canonical valuation enjoys many good structural properties not enjoyed by an arbitrary c-henselian valuation. The main such properties are summarized in the following

Proposition 2.2.5. *The canonical c-henselian valuation satisfies the following properties.*

- *$\mathcal{O}_c$ is non-trivial if and only if K is not c-closed and admits a non-trivial c-henselian valuation.*
- *If $\mathcal{O} \in C$ then $\mathcal{O}$ is comparable to any other c-henselian valuation*
- *If $\mathcal{O}_c$ does not have c-closed residue field, then neither does any other c-henselian valuation ring on K*
- *If $\mathcal{O}$ is strictly coarser than $\mathcal{O}_c$, then $\mathcal{O}/\mathcal{M}$ is not c-closed. If $\mathcal{O}$ is finer than $\mathcal{O}_c$, it has c-closed residue field.*
- *If K is c-closed, then $C = \{K\}$.*

Proof. Follows easily from the construction. For example, for the second property, since C_1 and C_2 partition the set of c-henselian valuations, and $\mathcal{O}_c$ is comparable to every element in C_1 and C_2 by construction, it is comparable to every c-henselian valuation. □

2.3 Three ‘Going-Down’ results

The formal properties of the canonical valuation are all that is required to prove the analogues of the three ‘Going-Down’ theorems from [4] for c-henselian valuations. We prove the two we will need later and leave the third as an exercise to the reader. The proofs follow those in [4].

Proposition 2.3.1. *Let $L \in \mathcal{C}(K)$ be a normal extension, and suppose $\mathcal{O}' \in C(L)$. Then $\mathcal{O} := \mathcal{O}' \cap K \in C(K)$.*

Proof. If $L = L^c$ then $\mathcal{O}' = L$ and $\mathcal{O} = K$, and the claim is trivial.

Suppose then that $L \neq L^c$ and $\mathcal{O}'$ is non-trivial. We will show that $\mathcal{O}'$ is the unique extension of $\mathcal{O}$ to L, and hence that $(K, \mathcal{O})$ is c-henselian. Indeed, let $\mathcal{O}''$ be any extension of $\mathcal{O}$ to L. Then there is some $\sigma \in \mathrm{Gal(L/K)}$ such that $\mathcal{O}'' = \sigma(\mathcal{O}')$. Hence $\mathcal{O}''$ is also c-henselian, and so by Proposition 2.2.5, is comparable, and hence equal to, $\mathcal{O}'$: indeed, distinct prolongations of a valuation to an algebraic extension are never comparable, by Lemma 3.2.8 in [4].

We finally show that $\mathcal{O}_c(K) \subseteq \mathcal{O}$. Assume for a contradiction that $\mathcal{O}$ is strictly contained in $\mathcal{O}_c(K)$. By Prop 2.2.3, $\mathcal{O} \in C_2(K)$. Now, by standard valuation theoretic arguments, we can find an extension $\mathcal{O}'''$ of $\mathcal{O}_c(K)$ to L containing $\mathcal{O}'$: in particular, $\mathcal{O}'''$ contains $\mathcal{O}_c(L)$. In fact, it strictly contains it, since otherwise, upon restricting to K, we would get $\mathcal{O} = \mathcal{O}_c(K)$, contrary to assumption. Hence, by Prop. 1.11, $\mathcal{O}'''$ does not have c-closed residue field. Hence neither does $\mathcal{O}_c(K)$, implying $C_2(K) = \emptyset$, contradiction. □

Proposition 2.3.2. *Suppose L is not c-closed, and let $L \in \mathcal{C}(K)$ be a finite extension. If $\mathcal{O}' \in C(L)$, then $\mathcal{O} := \mathcal{O}' \cap K \in C(K)$.*

Proof. One first passes to the normal hull of L/K, and then proceeds as above. □

For the last Going-Down result, we first introduce the following terminology: given a field F, we say $L \in \mathcal{C}(F)$ is a *Sylow p-extension* if G_L^c is a Sylow p-subgroup of G_F^c. That is, the profinite degree of $[L : F]$ is not divisible by p, while the degree $[F^c : L] = p^n$ for some n. We will also need to add some extra technical conditions in the case $p = 2$ (see [4] page 108-109). Recall (see [4] p. 109) that if there is a c-henselian valuation with real-closed residue field, then there exists a valuation ring $\mathcal{O}^+ \in C_1(L)$ maximal with respect to the property of having a real-closed residue field.

Proposition 2.3.3. *Let $L \in \mathcal{C}(K)$ be a Sylow p-extension and let $\mathcal{O}' \in C(L)$. If $p = 2$ and the residue field of $\mathcal{O}'$ is real-closed, we also assume $\mathcal{O}'$ is coarser than $\mathcal{O}^+$. Then $\mathcal{O} := \mathcal{O}' \cap K \in C(K)$.*

Proof. Assume $\mathcal{O}'$ is non-trivial, so $L \neq L^c$ by Proposition 2.2.5. Let $\mathcal{O}^c$ be the unique extension of $\mathcal{O}'$ to L^c. Now let $M \in \mathcal{C}(L)$ be finite over L, and set $\mathcal{O}_1 = \mathcal{O}^c \cap M$, evidently a c-henselian valuation. We claim that $\mathcal{O}_1$ is the only c-henselian valuation ring of M restricting to $\mathcal{O}$.

Indeed, assume $\mathcal{O}_2$ is another such ring. Then we first claim $\mathcal{O}_1$ and $\mathcal{O}_2$ are not independent. Otherwise, $M = M^c$ by the (S) property, so $L^c = M$ is finite. By the (R) property, $[L^c : L] = 2$, and since L is the fixed field of a Sylow p-subgroup, $[M : L] = [L^c : L] = p^n$ for some n. It follows that $p = 2$ and $L^c = L(2)$, so L, and hence also its residue field with respect to $\mathcal{O}'$, is real-closed. But note that we assumed $\mathcal{O}'$ was coarser than $\mathcal{O}^+$, and so L cannot be real-closed: contradiction. Therefore $\mathcal{O}_1$ and $\mathcal{O}_2$ are not independent.

They are also incomparable, since they are distinct valuation rings both restricting to $\mathcal{O}$. Hence $\mathcal{O}_3 := \mathcal{O}_1\mathcal{O}_2$ is non-trivial, and its residue field $k := \mathcal{O}_3/\mathcal{M}_3$ has independent valuations $\mathcal{O}_1/\mathcal{M}_3$ and $\mathcal{O}_2/\mathcal{M}_3$. Note that these valuations are c-henselian by Lemma 2.1.10. Hence, by the (S)-property, $k = k^c$. Now since $\mathcal{O}_1$ and $\mathcal{O}_2$ are non-comparable, $\mathcal{O}_1$ is a proper subset of $\mathcal{O}_3$, implying that $\mathcal{O}_3 \cap L$ is strictly coarser than $\mathcal{O}_c(L)$. Indeed, otherwise, upon restricting both to L, we find $\mathcal{O}' = \mathcal{O}_3 \cap L$, and since the former is c-henselian, this forces $\mathcal{O}_1 = \mathcal{O}_3$, contradicting the fact that $\mathcal{O}_1$ and $\mathcal{O}_2$ are not comparable. Hence $\mathcal{O}_3 \cap L$ does not have c-closed residue field k''. Since $[M : L]$ is finite, so is $[k : k'']$, with $k = (k'')^c$. It follows from the (R)-property that the degree of the extension is 2, and so by Lemma 2.6.2, 2 divides $[M : L]$. As L is the fixed field of a Sylow p-subgroup, $[M : L]$ must be of degree p^n for some n. This implies that $p = 2$: in this case we have assumed that $\mathcal{O}'$ is coarser than $\mathcal{O}^+$. But then $\mathcal{O}''$ is strictly coarser than $\mathcal{O}^+$ and still has real-closed residue field, which gives a contradiction.

It is now straightforward to show that $\mathcal{O}$ is c-henselian, since it has a unique extension to M, which is itself c-henselian. □

2.4 Rigid elements

We recall the fundamental results from the theory of so-called 'rigid elements'. This will be the key input to recover any sort of valuation whatsoever from the absolute Galois group. The theory developed above will then be used to bootstrap this valuation up to what we want.

Let $\mathcal{O}_v$ be a valuation ring of a field K. Then if $x \in K^\times \setminus \mathcal{O}_v^\times$, the ultrametric inequality implies the additive and multiplicative action of $\mathcal{O}_v^\times$ on x possesses a certain rigidity, in the sense that one can never move too far away from x. Precisely, one has

$$\mathcal{O}_v^\times + x\mathcal{O}_v^\times \subseteq \mathcal{O}_v^\times \cup x\mathcal{O}_v^\times \tag{2.2}$$

It turns out that any subgroup $T \leq K^\times$ which acts in a similarly rigid fashion on elements of $K^\times \setminus T$ must be induced by a valuation ring. To this end we make the following definition.

Definition 2.4.1. If $x \in K^\times \setminus T$, then we call x T-rigid if

$$T + xT \subseteq T \cup xT$$

For simplicity we restrict now to the special case where $(K^\times)^p \leq T$ for some prime p. In this case, define the sets

$$\begin{aligned} \mathcal{O}_1(T) &:= \{x \in K \setminus T : 1 + x \in T\} \\ \mathcal{O}_2(T) &:= \{x \in T : x\mathcal{O}_1(T) \subseteq \mathcal{O}_1(T)\} \end{aligned}$$

and

$$\mathcal{O}(T) := \mathcal{O}_1(T) \cup \mathcal{O}_2(T).$$

Proposition 2.4.2. *Given the setup as above, suppose in addition that every element in $K^\times \setminus T$ is T-rigid, and if $p = 2$, assume that $-1 \in T$. Then if $p \neq 2$, $\mathcal{O}(T)$ defines a valuation ring of K with $\mathcal{O}(T)^\times \subseteq T$. If $p = 2$, there exists a subgroup $T' \leq K^\times$ containing T such that $[T' : T] = 2$ and $\mathcal{O}(T')$ is a valuation ring of K with $\mathcal{O}(T')^\times \subseteq T'$.*

Proof. This is Theorem 2.2.7 in [4]. □

So provided $p \neq 2$, the valuation ring will be non-trivial if and only if $T \neq K^\times$.

The next lemma gives a powerful method for detecting the existence of subgroups T satisfying the criterion of proposition 2.4.2.

Lemma 2.4.3. *Let p be an odd prime, K a field. Suppose $S \leq K^\times$ is a subgroup of index $[K^\times : S] \geq p^2$, such that for any $x \in K^\times \setminus S$,*

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

Then there is a subgroup $T \leq K^\times$ with $S \subseteq T$, $[T : S] \leq p$, and every $x \in K^\times \setminus T$ is T-rigid.

Proof. This is Lemma 2.14 in [12]. □

For later use, we also make the following definition:

Definition 2.4.4. Given a field K and a prime p, an element $a \in K \setminus K^p$ is called *strongly p-rigid* iff it is $(K^\times)^p$-rigid, i.e., iff

$$K^p + aK^p \subseteq K^p \cup aK^p.$$

Proposition 2.4.2 shows sufficiently many strongly p-rigid elements induce the existence of a non-trivial valuation ring. In fact, in [13] it was shown, using model theory, that even just a single strongly p-rigid element already implies the existence of such a valuation.

2.5 A Galois-theoretic characterization of c-henselianity

A Galois theoretic characterization for a field to admit a non-trivial p-henselian valuation was obtained in [10], provided the field contains a primitive p-th root of unity ζ_p. The formal properties of canonical valuations established above allow us to obtain an analogous characterization for the existence of a c-henselian valuation in terms of the maximal $\mathcal{C}$-quotient of the absolute Galois group.

Definition 2.5.1. A valuation v on a field K is said to be *tamely branching* at the prime p if $char(Kv) \neq p$, $\Gamma_v \neq p\Gamma_v$. If $[\Gamma_v : p\Gamma_v] = p$, we also require that Kv is not p^2-closed, that is, there exists a separable extension of Kv of degree divisible by p^2.

Notice that if $p = 2$ and Kv is formally real, then Kv admits an extension of degree 2 but not degree 4, as $[Kv^{sep} : Kv] = 2$. This is however the only case for which having an extension of degree p does not imply that there is also an extension of degree p^2. So outside of this case, the last condition is equivalent to Kv not being p-closed.

The following observation will be crucially used later.

Lemma 2.5.2. *Let F be a finite extension of $\mathbb{Q}_p$. Then F does not admit any p-henselian valuation tamely branching at p.*

Proof. Let v_p denote the p-adic valuation, and suppose w is another valuation which is p-henselian tamely branching at p. As v_p is a rank 1 valuation and has a residue field which is not p-closed, w must be a refinement of v_p, and hence must have residue characteristic p: contradiction. □

We now present a sharpening of the Galois-characterization for p-henselian valuations tamely branching at p obtained in [10]. Recall Definition 1.1.4 of the maximal elementary $\mathbb{Z}/p\mathbb{Z}$ meta-abelian extension.

Proposition 2.5.3. *Let p be a prime, and let K be a field with a primitive p-th root of unity. Let K'' denote the maximal elementary $\mathbb{Z}/p\mathbb{Z}$ meta-abelian extension of K. Then K admits a p-henselian valuation tamely branching at p whenever* $\mathrm{Gal(K''/K)} \simeq \mathbb{Z}/\mathrm{p}^2\mathbb{Z} \rtimes \mathbb{Z}/\mathrm{p}^2\mathbb{Z}$.

Proof. We will only treat the case $p > 2$ in what follows. The case $p = 2$ follows using the same method as in [4] Lemma 5.4.4.

Let us suppose first of all that $G := \mathrm{Gal(K''/K)} \simeq \mathbb{Z}/\mathrm{p}^2\mathbb{Z} \rtimes \mathbb{Z}/\mathrm{p}^2\mathbb{Z}$. Then by Kummer theory,

$$\dim_{\mathbb{F}_p} K^\times/(K^\times)^p = \mathrm{rank}(G) = 2.$$

Suppose $H \leq G$ is a subgroup of index p. Then we claim that $H \simeq \mathbb{Z}/p^i\mathbb{Z} \rtimes \mathbb{Z}/p^j\mathbb{Z}$ where $i, j \in \{1, 2\}$. Indeed, the embedding $H \hookrightarrow \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$ induces the following commutative diagram with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r, hook, "g"] & G \arrow[r, two heads, "f"] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r] & 1 \\
1 \arrow[r] & H'' \arrow[r, hook] \arrow[u, hook] & H \arrow[r, two heads] \arrow[u, hook] & H' \arrow[r] \arrow[u, hook] & 1
\end{tikzcd}$$

where $H'' = im(g) \cap H$, $H' = f(H)$, and since H' is cyclic, the splitting of the top sequence induces one for the bottom one. So $H \simeq H' \rtimes H''$. If H' or H'' were trivial, then H would have index greater than p, contradicting our assumption.

If L is an extension of K of degree p, applying the above in the case when $H = \mathrm{Gal(K''/L)}$, we see that

$$\dim_{\mathbb{F}_p} L^\times/(L^\times)^p = \mathrm{rank}(H) = 2 \tag{2.3}$$

as well. Armed with this crucial observation, we now wish to use Lemma 2.4.3 with $S = (K^\times)^p$.

If we let

$$\langle x \rangle := \bigcup_{i=0}^{p-1} x^i (K^\times)^p$$

then we need to show that for every $x \in K^\times \setminus (K^\times)^p$, $(K^\times)^p + x(K^\times)^p \subset \langle x \rangle (K^\times)^p$, where this last set denotes the multiplicative group generated by x and $(K^\times)^p$. Notice that for any $a, b \in K^\times$, $z := a + \sqrt[p]{x} b \in L := K(\sqrt[p]{x})$ has norm $N_{L/K}(z) = a^p + xb^p$. Therefore the conditions of Lemma 2.4.3 are met if we can show that

$$N_{L/K}(L^\times) = \langle x \rangle (K^\times)^p \tag{2.4}$$

for any such L. Since $N_{L/K}(\sqrt[p]{x}) = x$, we have that $\langle x \rangle (K^\times)^p \subset N_{L/K}(L^\times)$ and, since $x \notin K^p$, $\sqrt[p]{x} \notin L^p$. Now, since $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ has cohomological dimension 2, and the elementary $\mathbb{Z}/p\mathbb{Z}$ meta-abelian quotient is $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$, Lemma 1.1.5 implies that ${}_pBr(K)$ is non-trivial. Again by Lemma 1.1.5, $N_{L/K} : L \to K$ is not surjective. Thus we may find $y \in K^\times \setminus \langle x \rangle (K^\times)^p$. Since $L^p \cap K = K^p$, $y \notin \langle \sqrt[p]{x} \rangle (L^\times)^p$. Thus y and $\sqrt[p]{x}$

are independent elements in the $\mathbb{F}_p$-vector space $L^\times/(L^\times)^p$, which is 2-dimensional by (2.3). Thus

$$L^\times = \langle y\rangle\langle \sqrt[p]{x}\rangle(L^\times)^p$$

from which, by taking norms, we obtain (2.4) as desired.

Since $[K^\times : (K^\times)^p] = p^2$, we can use Lemma 2.4.3 together with Proposition 2.4.2 to see that K admits a valuation $\mathcal{O}$ with $\mathcal{O}^\times \leq T$, for some $T \subsetneq F^\times$ containing $(K^\times)^p$. Since then $\mathcal{O}^\times(K^\times)^p \subset T \neq K^\times$, we have $\Gamma_v \neq p\Gamma_v$.

The rest of the proof now proceeds exactly as in [10]. □

Remark 2.5.4. In particular, the conditions of the proposition are satisfied if $G_K(p) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$.

Remark 2.5.5. It is a consequence of the proof that if K is as above, then the norm map induces a bijection between extensions of K of degree p and subgroups of $K^\times$ of index p. We will see in Chapter 3 that this is a general property of Demushkin groups, of which $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ is an example.

We are now ready to deduce the first main result of this chapter, giving a Galois theoretic characterization for a field to admit a c-henselian valuation. We will assume in the proof that $p > 2$ for simplicity.

Theorem 2.5.6. *Let K be any field, and let $\mathcal{C}$ be a canonical class containing $\mathcal{C}_p$ for some prime p, such that $K(\zeta_p) \in \mathcal{C}(K)$.*[1] *Then there is a c-henselian valuation v on K tamely branching at p if and only if* $\mathrm{Gal(K^c/K)}$ *has a non-procyclic p-Sylow subgroup with a non-trivial abelian normal subgroup.*

Proof. ("⇒"): If K admits such a valuation, then the valuation extends to a c-henselian valuation on the fixed field of *any* p-Sylow subgroup S of $\mathrm{Gal(K^c/K)}$. By Hilbert ramification theory, the inertia subgroup of this extended valuation is a non-trivial normal abelian subgroup, and S is not procyclic.

("⇐"): Let S be such a Sylow subgroup, with fixed field F. By assumption S admits a non-trivial abelian normal subgroup $A \simeq \mathbb{Z}_p^r$ where $r = rank(A)$.

[1] Note that if $\zeta_p \in K$ then this last condition always holds.

If $r > 1$, then A has a normal subgroup of the form $\mathbb{Z}_p \rtimes \mathbb{Z}_p$, and so its fixed field is a *normal* field extension L/F inside K^c such that

$$\mathrm{Gal(K^c/L) = Gal(L^c/L) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p.}$$

Since

$$cd_p(\mathbb{Z}_p \rtimes \mathbb{Z}_p) = 2$$

we find $char(L) \neq p$, since the p-cohomological dimension of a field of characteristic p is always ≤ 1 (see [33] Chapter 2, Section 2.2). By construction[2], $L(p) = L^c = K^c$, and $\mathrm{Gal(L^c/L)(p) = Gal(L(p)/L) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p}$. By assumption $K(\zeta_p) \in \mathcal{C}(K)$. We have that $[K(\zeta_p) : K]$ divides $p - 1$. Since $\zeta_p \in K^c$, but there are only p-power extensions between L and K^c, it must therefore be that $\zeta_p \in L$. Then by Proposition 2.5.3, there is a p-henselian valuation w on L tamely branching at p. Since $L(p) = L^c$, the valuation is actually c-henselian. Let v be the canonical c-henselian valuation on L. By Proposition 2.2.5, v is still tamely branching at p. By Proposition 2.3.1, its restriction to F is again c-henselian, and clearly still has residue characteristic not p and value group not p-divisible. Finally, by Proposition 2.3.3, we may once more restrict to K and obtain a c-henselian valuation tamely branching at p as desired.

If $r = 1$, then since S is not pro-cyclic, there is $g \in S \setminus A$ such that

$$A \rtimes \langle g \rangle \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p.$$

Letting L be the fixed field of this semidirect product, we find in the same way as above that L has a c-henselian valuation tamely branching at p. Its unique prolongation w to the fixed field $Fix(A)$ of A has non-p-divisible value group and residue characteristic not p, and so the same will be true for w_c, the canonical c-henselian valuation on $Fix(A)$. By the 'Going-Down' results, the restriction of w_c to L is c-henselian and tamely branching, and therefore so is its restriction to F, which gives us the desired valuation. □

Remark 2.5.7. For example, we may take $\mathcal{C}$ to be $\mathcal{C}_{solv}$ in the above. Since $K(\zeta_p)$ is a solvable extension, we do not in this case need to assume anything about K

[2] Noting that since $\mathcal{C}$ contains $\mathcal{C}_p$, K^c is p-closed.

containing ζ_p. Alternatively, if we assumed K contains ζ_p, then we could also have taken $\mathcal{C} = \mathcal{C}_{p,q}$.

We record the following strengthening of the above utilizing the full sharpening obtained in Proposition 2.5.3.

Definition 2.5.8. We denote by K^{pq} the compositum of all elementary abelian $\mathbb{Z}/q\mathbb{Z}$ extensions of K'', the elementary $\mathbb{Z}/p\mathbb{Z}$ meta-abelian extension of K. We call K^{pq} the maximal (p, q)-meta-abelian extension of K.

Corollary 2.5.9. *Let K be any field containing ζ_p and let $\mathcal{C} = \mathcal{C}_{p,q}$, the class of all finite groups of order $p^n q^m$ for some n, m. Then there is a c-henselian valuation v on K tamely branching at p if and only if* $\mathrm{Gal(K^{pq}/K)}$ *has a non-procyclic p-Sylow subgroup with a non-trivial abelian normal subgroup.*

Proof. This follows in the exact same way as the proof of the above Theorem. □

2.6 Recovering the p-adic valuation

Now let $\mathcal{C}$ be any canonical class containing $\mathcal{C}_{p,q}$: for example $\mathcal{C}_{p,q}$ or $\mathcal{C}_{solv}$. Thus Theorem 2.5.6 can be applied in this context. We will now show that if we impose extra structure on the groups in question, we are rewarded with extra structure on the valuations obtained in this way. We will first need some preliminary technical results.

Proposition 2.6.1. *Let (K, v) be a valued field of mixed characteristic $(0, p)$ such that $\mathcal{O}_v[1/p] = K$, $K^\times/(K^\times)^p$ is finite. Then Kv is perfect. If in addition $\Gamma_v \neq p\Gamma_v$, then $\Gamma_v \simeq \mathbb{Z}$ and Kv is a finite field.*

Proof. This is just [25] Lemma 2.4. □

Before proving the next technical result, recall the following basic result from valuation theory:

Lemma 2.6.2. *Let L/K be a Galois extension with $[L : K] = n < \infty$, and let v be a valuation on K with m extensions to L. Then the ramification indices e and relative degrees f of all the m extensions of v agree with each other, and $n = mefd$ where d is 1 if $char(Kv) = 0$, and a power of $char(Kv)$ otherwise.*

Proposition 2.6.3. *Let (K, v) be a p-henselian valued field of mixed characteristic $(0, p)$ with $\mathcal{O}_v[1/p] = K$ and suppose that $G_K(p)$ is finitely generated. Then if $\Gamma_v = p\Gamma_v$, there exists a field F of characteristic p such that $G_K(p) \simeq G_F(p)$.*

Proof. Assume $\Gamma_v = p\Gamma_v$. We will construct a field F of characteristic p such that $G_F(p) \simeq G_K(p)$. By [33] 2.2 Prop 3., this will prove the statement of the proposition. The construction of F is a modification of Theorem 3.3. in [11].

Let $\widetilde{K}$ be an $\aleph_1$-saturated elementary extension of K, with valuation $\tilde{v}$. Consider the 'exact sequence' of valuations

$$1 \to \tilde{v}_0 \to \tilde{v}_p \to w \to 1$$

where $\tilde{v}_0$ is the finest coarsening of $\tilde{v}$ with residue characteristic 0, $\tilde{v}_p$ the coarsest coarsening of $\tilde{v}$ with residue characteristic p. By definition, w is the valuation induced by $\widetilde{v}_p$ on $E := \widetilde{K}\tilde{v}_0$ with residue field $Ew \simeq \widetilde{K}\tilde{v}_p$ of characteristic p. By Lemma 2.1.10 it is p-henselian, and necessarily has rank 1 as $\tilde{v}_p$ was chosen maximal.

Now let $\mu^{(p)}_{E(p)}$ denote the prime to p part of $\mu_{E(p)}$. Assume for the time being that we have the following commutative diagram:

$$\begin{tikzcd}
G_E(p) \arrow[r, "\simeq"'] \arrow[d] & G_{E_w}(p) \arrow[d] \\
Aut(\mu^{(p)}_{E(p)}) \arrow[r, "\simeq"'] & Aut(\mu_{E_w(p)})
\end{tikzcd}$$

We will finish the proof based on this assumption. Indeed, let $F' := Ew((\Gamma_{\tilde{v}_0}))$ be the power series field over $\Gamma_{\tilde{v}_0}$, and denote by v' the power series valuation: it is well known that v' is henselian. The ramification subgroup $R_{v'}$ of $G_{F'}(p)$ has a complement H by the work of Kuhlmann, Pank and Roquette ([15]). Let F be the fixed field of H, with valuation v_F prolonging v'. Clearly $char(F) = p$. Also,

$$R_{\tilde{v_0}} = 1$$
$$R_{v_F} = 1$$

The former holds since the residue characteristic of $\tilde{v}_0$ is 0, and the latter since $G_F(p)$ intersects trivially with $R_{v'}$. By Hilbert ramification theory, it follows that

$$I_{v_F} = I_{\tilde{v_0}}$$

By the commutative diagram assumed above, the action[3] of $G_{Ew}(p)$ on I_{v_F} coincides with the action of $G_E(p)$ on $I_{\tilde{v_0}}$. Therefore we get isomorphisms

$$G_F(p) \simeq I_{v_F} \rtimes G_{Ew}(p) \simeq I_{\tilde{v_0}} \rtimes G_E(p) \simeq G_{\widetilde{K}}(p) \simeq G_K(p)$$

where the isomorphism $G_K(p) \simeq G_{\widetilde{K}}(p)$ follows from the fact that $K \equiv \widetilde{K}$ and that $G_K(p)$ is finitely generated.

It remains to prove the existence of the commutative diagram above. The idea is to show that for any extension E'/E of degree p^n, that $[E' : E] = e(E'/E)$, and that $E'w/Ew$ is Galois. This immediately implies $G_E(p) \simeq G_{Ew}(p)$.

We will show first that $\Gamma_w = \mathbb{R}$: this is where the saturatedness of $\widetilde{K}$ is essential. First observe that $\Gamma_v = p\Gamma_v$ implies the same is true for $\tilde{v}$, and the exact sequence

$$1 \to \Gamma_{\tilde{v}_0} \to \Gamma_{\tilde{v}_p} \to \Gamma_w \to 1$$

therefore shows $\Gamma_w = p\Gamma_w$. Since w has rank 1, it embeds as a subgroup of $\mathbb{R}$: this subgroup is *dense* by p-divisibility [4]. Now let $\lambda \in \mathbb{R}$, and consider the type

$$p(x) = \{\phi_{q_1,q_2}(x) : q_1, q_2 \in \mathbb{Q} \wedge q_1 < \frac{\lambda}{w(p)} < q_2\}$$

where $\phi_{q_1,q_2}(x)$ is the formula

$$q_1\tilde{v}(p) < \tilde{v}(x) < q_2\tilde{v}(p).$$

[3] Note that because $\Gamma_{\tilde{v}_0} = p\Gamma_{\tilde{v}_0}$, the action of $G_E(p)$ on $T_{\tilde{v}_0}$ is determined by the image of G_E in $Aut(\mu_{E(p)}^{(p)})$ alone.

[4] For example, since additive subgroups of $\mathbb{R}$ are either dense or of the form $a\mathbb{Z}$ for some $a \in \mathbb{R}$.

By density of Γ_w, we can find an $x \in \widetilde{K}$ such that $q_1 w(p) < w(x) < q_2 w(p)$, whence also $q_1 \tilde{v}(p) < \tilde{v}(x) < q_2 \tilde{v}(p)$. Similarly, any finite combination of the $\phi_{q_1,q_2}(x)$ is realizable. Thus there is an $a \in \widetilde{K}$ realizing $p(x)$. Note that $\tilde{v}_0(a) > 0$ since $\tilde{v}(p) > 0$ by virtue of the residue characteristic being p. Hence if we let $\gamma_0 : \widetilde{K} \to E$ be the place corresponding to $\tilde{v}_0$, we have $\gamma_0(a) = a \bmod M_{\tilde{v}_0}$. Since $q_1 \tilde{v}(p) < \tilde{v}(a) < q_w \tilde{v}(p)$ for any consistent choice of q_1, q_2, we have

$$q_1 w(p) < w(\gamma_0(a)) < q_2 w(p)$$

for any consistent q_1, q_2. Thus clearly $w(\gamma_0(a)) = \lambda$. In other words,

$$\Gamma_w = \mathbb{R}.$$

Next we argue that for any Galois extension E'/E of degree p^n, E' has no immediate algebraic extensions. It will suffice to show that E'/E is not immediate, for the same argument can be applied to any extension of E', using that the value group of the extension of w to E' is still $\mathbb{R}$, its rank also being 1. So let α be a primitive element of E'/E with minimal polynomial $m(x)$. Now Lemma 1.2.5 implies that $w(m(E)) \subset \mathbb{R} = \Gamma_w$ is bounded, say with supremum λ. If $f \in \mathcal{O}_{\tilde{v}_0}[x]$ is any lift of $m(x)$, and $y \in \mathcal{O}_{\tilde{v}_0}$ satisfies $w(\gamma_0(y)) = \lambda$, then consider as before the type

$$p'(x) = \{\psi_{q_1,q_2}(x) : q_1, q_2 \in \mathbb{Q} \wedge q_1 < \frac{\tilde{v}(y)}{\tilde{v}(p)} < q_2\}$$

where ψ_{q_1,q_2} is the formula

$$q_1 \tilde{v}(p) < \tilde{v}(g(x)) < q_2 \tilde{v}(p)$$

Arguing as before, we can find $b \in E$ such that $w(f(b)) = \lambda$. Now assume for a contradiction that E'/E is immediate. Then we can find $c \in E$ which agrees with $b - \alpha$ in the residue field. In other words, $w(c-(b-\alpha)) > w(b-\alpha)$. If $H := \mathrm{Gal(E'/E)}$, then by p-henselianity, $w(c - (b - \sigma(\alpha)) = w(b - \sigma(\alpha))$ for every $\sigma \in H$, whence

$$w(f(b-c)) = w(\prod_{\sigma \in H}(b - c - \sigma(\alpha))) > w(\prod_{\sigma \in H}(b - \sigma(\alpha)) = w(f(b)).$$

This gives the desired contradiction.

In fact this already implies E is defectless wrt. subextensions of $K(p)$. Indeed, let N/E be an extension of degree $p^n, n \geq 1$, such that the defect $d(N/E) > 1$, with $[N : E]$ minimal with respect to this property. By Cauchy's Theorem, we can always find a subextension N'/E with $[N : N'] = p$. Since $d(N/E) = d(N'/N)d(N/E)$, we must have $d(N'/N) > 1$ by minimality. But since the defect is necessarily a power of p, this means $d(N'/N) = [N' : N]$ and so N'/N is an immediate extension, contradicting the above.

Finally, since $\Gamma_w = \mathbb{R}$, the value group can't increase in algebraic extensions, whence it follows that for any E'/E of degree p^n, $[E' : E] = [E'w : Ew]$. That $E'w/Ew$ is Galois follows because by Proposition 2.6.1, Ew is perfect: indeed, G_E is a quotient of $G_{\widetilde{K}}$ and hence $Ew^\times/(Ew^\times)^p$ is finite. Thus we have $G_E(p) \simeq G_{Ew}(p)$. The isomorphism is evidently compatible with the action of the cyclotomic character, and so the proof of the claim is complete. □

The following corollary is immediate, since any field of characteristic p has p-cohomological dimension at most 1:

Corollary 2.6.4. *Let (K, v) be a p-henselian valued field of mixed characteristic $(0, p)$ containing ζ_p, such that $\mathcal{O}_v[1/p] = K$ and $G_K(p)$ is finitely generated. Then*

$$\Gamma_v = p\Gamma_v \implies cd(G_K(p)) \leq 1.$$

The last result we need is a strengthening of a lemma by Pop (Satz 4 of [23]). We simply optimize his original proof.

Lemma 2.6.5. *Let $G := \mathrm{Gal}(\mathrm{F^{pq}/F}) = \mathrm{G_F^{pq}}$ where F is a finite extension of $\mathbb{Q}_p$ and F^{pq} is as in Definition 2.5.8. Then there is a p-subgroup R of G such that if $H \trianglelefteq G$ is non-trivial, then $H \cap R \neq \{1\}$.*

Proof. Let I_F and R_F denote the inertia and ramification subgroup of G with respect to the p-adic valuation on F. We claim that R_F satisfies the desired property.

Indeed, suppose H is any normal subgroup, and let L be the fixed field of H in F^{pq}. Then note that $R_F \cap H = R_L$, the ramification subgroup of the p-adic valuation on L. So we need to show that this ramification group is non-trivial. We will show that the p-Sylow subgroups of G_L^{pq} are non-cyclic. Assuming this, note that if $R_L = 1$, then $I_L \simeq (\mathbb{Z}/q)^r$ for some r. Also, $G_L^{pq}/I_L \simeq G_{Lv}^{pq}$. The Sylow subgroups of G_L^{pq}/I are of the form PI/I where P is a Sylow subgroup of G_L^c. Since I_L is not pro-p (and has no pro-p quotients) it commutes with any Sylow subgroup P as both are normal. Thus PI/I is cyclic if and only if P is cyclic. But $G_{Lv}^{pq} \simeq \mathbb{Z}/p \times \mathbb{Z}/q$ clearly has a cyclic p-Sylow subgroup, which gives us our desired contradiction.

Let F_1/F be any Galois sub-extension of F^{pq} not contained in L, and put $k = F_1 \cap L$, $L_1 = F_1' \cap L$, where F_1' is the maximal elementary abelian $\mathbb{Z}/p$-extension of F_1. Since L_1 and F_1 are linearly disjoint,

$$\mathrm{Gal(L_1/L)^c} \simeq \mathrm{Gal(L_1F_1/F_1)^c}$$

and $\mathrm{Gal(L_1F_1/F_1)}$ is a quotient of $\mathrm{Gal(F_1'/F_1)}$. Therefore L_1'/k is a $\mathbb{Z}/p\mathbb{Z}$-extension. Now

$$[F_1' : L_1F_1] = \frac{[F_1' : F_1]}{[L_1 : k]} \geqslant p^{a-b}$$

where $a = [F_1 : \mathbb{Q}_p], b = [k : \mathbb{Q}_p]$. By taking an element α in F^{pq} of degree p^2q over F but not contained in L, we may choose $F_1 = F(\alpha)$. Since L/F is of degree at most p^2q, $[F_1 : k]$ is at least degree p or q, and in either case is at least 2. Then $a - b \geqslant 2$ by the Tower Law, and so $p^2 \mid [F_1' : L_1F_1]$. It follows that $\mathrm{Gal(F_1'/L_1F_1)^c}$ is at least $(\mathbb{Z}/p\mathbb{Z})^2$ and so is not cyclic.

Now, any p-Sylow subgroup of $\mathrm{Gal(F_1'/L_1)^{pq}}$ must contain $\mathrm{Gal(F_1'/L_1F_1)^{pq}}$, as it's a subgroup of the p-group $\mathrm{Gal(F_1'/F_1)^c}$. Because any subgroup of a cyclic group is cyclic, it follows that $\mathrm{Gal(F_1'/L_1)^{pq}}$ has no cyclic p-Sylow subgroups. Since $\mathrm{Gal(F_1'/L_1)^c} \simeq \mathrm{Gal(LF_1'/L)^{pq}}$, neither does $\mathrm{Gal(LF_1'/L)^{pq}}$. But as this is a quotient of G_L^{pq}, it follows that G_L^{pq} also cannot have any cyclic p-Sylow subgroups. □

Armed with the above technicalities, we are ready to prove the second main result of the chapter.

Theorem 2.6.6. *Let F a finite extension of $\mathbb{Q}_p$ containing ζ_p and ζ_q with p-adic valuation v_p. Choose $\mathcal{C}$ to be any canonical class containing $\mathcal{C}_{p,q}$, where q is any* *prime different from p. Suppose L is any field with*

$$G_L^c \simeq G_F^c,$$

where, if $L(\zeta_n) \notin \mathcal{C}(L)$, $n \in \{p, q\}$, we additionally assume that $\zeta_n \in L$. Then L has characteristic 0 and there is a c-henselian valuation v on L with Lv a finite field of characteristic p and $\Gamma_v \simeq \mathbb{Z}$. Furthermore, there is a finite extension F' of $\mathbb{Q}_p$ with p-adic valuation v_p, such that $G_{F'}^c \simeq G_F^c$, $[F' : \mathbb{Q}_p] = [F : \mathbb{Q}_p]$, and $Lv \simeq F'v_p$. If we take $\mathcal{C} = \mathcal{C}_{solv}$ then F' can be taken to be F.[5]

Proof. Let v be the finest non-trivial c-henselian valuation on L, which exists by Theorem 2.5.6. Let us first show that the residue characteristic of v is p.

Suppose, for a contradiction, that the residue characteristic is not p. If $\Gamma_v \neq p\Gamma_v$ then L contains strongly p-rigid elements: indeed, it is not hard to see that any a with $v(a) \notin p\Gamma_v$ is strongly p-rigid. By the main result of [12], L therefore admits a p-henselian valuation tamely branching at p, which by Proposition 2.5.3 is encoded in $G_L(p)$. The isomorphism $G_L^c \simeq G_F^c$ forces their maximal pro-p quotients to be isomorphic, and since we are assuming $\mathcal{C}$ contains $\mathcal{C}_{p,q}$, these coincide naturally with the maximal pro-p quotients of the full absolute Galois group. It follows, again by Proposition 2.5.3, that F also admits a p-henselian valuation tamely branching at p, contradicting Lemma 2.5.2.

Hence it must be that $\Gamma_v = p\Gamma_v$. Because $char(Lv) \neq p$, the inertia subgroup I_v of G_L^c is normal and contains no non-trivial pro-p subgroups. By Lemma 2.6.5, this forces I_v to be trivial. Hence

$$G_{Lv}^c \simeq G_L^c / I_v \simeq G_F^c.$$

Again by Theorem 2.5.6, Lv admits a non-trivial c-henselian valuation, from which we may obtain a proper refinement of the original valuation on L, contradicting the fact that we choose v to be the finest such. Thus it must have been the case that $\mathrm{char}(Lv) = p$.

[5] And in this case, the statement is also true even if F does not contains ζ_p or ζ_q.

Now, since $G_L(p) \simeq G_F(p)$ as remarked above, and $cd(G_F(p)) = 2$, Proposition 2.6.4 implies that $\Gamma_v \neq p\Gamma_v$. Since a p-adic field has small absolute Galois group, having only finitely many extensions of a given degree, we may apply Proposition 2.6.1 to deduce that $\Gamma_v \simeq \mathbb{Z}$, and that Lv is a finite field of characteristic p.

Put $L' := L \cap \overline{\mathbb{Q}}$ and let F' be the henselization of L' with respect to v', the restriction of v to L'. The induced valuation on L^h still has value group $\mathbb{Z}$ and residue field finite of characteristic p: therefore it is a finite extension of F and v' coincides with the p-adic valuation v_p. By construction,

$$G^c_{F'} \simeq G^c_L \simeq G^c_F$$

and $F'v_p \simeq Lv$. Since $G^c_{F'} \simeq G^c_F$, we have $G_{F'}(p) \simeq G_F(p)$. By Chapter 3, Fact 3.2.3, we must have that $[F' : \mathbb{Q}_p] = [F : \mathbb{Q}_p]$.

Suppose next that $\mathcal{C} = \mathcal{C}_{solv}$. Then by work of Jarden, Ritter and Jenkner ([8], [30], [9]), it follows that

$$F' \cap \mathbb{Q}_p^{ab} = F \cap \mathbb{Q}_p^{ab},$$

which forces $Lv = Fv_p$. □

Note that as before, if we take $\mathcal{C} = \mathcal{C}_{solv}$, then we do not need any extra assumptions on L containing roots of unity. For the readers benefit, let us make this special case entirely clear:

Theorem 2.6.7. *Let F be a finite extension of $\mathbb{Q}_p$ with p-adic valuation v_p. Suppose L is any field with*

$$G^{solv}_L \simeq G^{solv}_F.$$

Then L has characteristic 0, and there is a solv-henselian valuation v on L with $Lv \simeq Fv_p$, $\Gamma_v \simeq \mathbb{Z}$.

Corollary 2.6.8. *Let F be a finite extension of $\mathbb{Q}_p$ containing ζ_p and ζ_q. If L is any field also containing ζ_p and ζ_q, and if* $\mathrm{Gal}(\mathrm{L}^{\mathrm{pq}}/\mathrm{L}) \simeq \mathrm{Gal}(\mathrm{F}^{\mathrm{pq}}/\mathrm{F})$, *then L admits a non-trivial (p,q)-henselian valuation v with $\Gamma_v \simeq \mathbb{Z}$. Furthermore, there is a finite extension F' of $\mathbb{Q}_p$ containing ζ_p and ζ_q such that $G^{pq}_{F'} \simeq G^{pq}_F$, $[F' : \mathbb{Q}_p] = [F : \mathbb{Q}_p]$ and $Lv \simeq F'v_p$.*

Proof. The proof is identical to the above, simply using Corollary 2.5.8. □

Chapter 3

Demushkin Fields

3.1 General Conjectures

Let F be a finite extension of $\mathbb{Q}_p$. In chapter 2 we showed that, assuming F contains the relevant roots of unity, the p-adic valuation on F could be recovered already from $G_F(p, q)$, where q is a prime different from p. Indeed, we saw that a tiny quotient of this sufficed. The fundamental result used was a way of detecting valuations from the structure of $G_F(q)$, and we pushed this to its limits. Further progress would require a totally new way of detecting valuations from $G_F(p)$ alone. This is what we will look at in this chapter.

Suppose now F contains ζ_p. The quotient $G_F(q)$ for $q \neq p$ lives in the 'tamely ramified' part of the Galois group while $G_F(p)$ lives in the 'wild' part. Its structure is known by work of Demushkin, Labute and Serre (cf. [33], 5.6). It is an example of a pro-p Demushkin group given by generators and relations which can be specified (see section 3.1): these fields are therefore canonical examples of what we will call *Demushkin fields*. Notice that $G_F(q) \simeq \mathbb{Z}_q \rtimes \mathbb{Z}_q$ is also Demushkin, but with a less rich structure than $G_F(p)$, which retains information on the prime p. Taking into account that different extensions of $\mathbb{Q}_p$ can have the same pro-p Galois group[1], we have the following conjecture:

[1] See Remark 2.5.5

Conjecture 1. Let $F/\mathbb{Q}_p$ be a finite extension, K an arbitrary field, where both F and K contain ζ_p. Suppose $G_F(p) \simeq G_K(p)$. Then there exists a non-trivial valuation v on K such that for some finite extension $F'/\mathbb{Q}_p$ with $G_{F'}(p) \simeq G_F(p)$ and p-adic valuation w, the following holds:

- v is *p-henselian*
- $F'w = Kv$
- $[\Gamma_v : p\Gamma_v] = p$
- There is a uniformizer π of (F', w) such that $\pi \in K \cap \overline{\mathbb{Q}}$ and $v(\pi)$ is a minimal positive element in Γ_v (in particular, the valuation is discrete).[2]

Thus conjecturally, the 'wild' part of G_K sees a lot more of the structure of the field than the 'tame' part. In fact, in accordance with the Elementary Type Conjecture (see e.g. the introduction of [7] as well as [2]), it is expected that the following conjecture holds:

Conjecture 2. Suppose $G_K(p)$ is a finitely generated pro-p Demushkin group of rank ≥ 3. Then there is a finite extension $F/\mathbb{Q}_p$ containing ζ_p such that $G_K(p) \simeq G_F(p)$.

That is, one expects that essentially the only examples of finitely generated pro-p Galois groups which are Demushkin are the ones coming from finite extensions of $\mathbb{Q}_p(\zeta_p)$, and that the structure implied by being Demushkin is already enough to force the existence of a valuation which is as close to being p-adic as one could reasonably hope. This would be a major step in the programme of classifying all finitely generated pro-p Galois groups.

[2] Here Kv and Γ_v denote the residue field and value group of the valuation respectively.

Remark 3.1.1. Observe that in Conjecture 1, one should not expect the valuation to be rank 1, since e.g. $\mathbb{Q}_p((\mathbb{Q}))$ has absolute Galois group isomorphic to that of $\mathbb{Q}_p$, and the associated valuation has higher rank.

In this chapter we aim to justify Conjecture 1 by proving the following result, which constitutes the first positive result on these conjectures:

Theorem 1. Conjecture 1 is true in the case $F = \mathbb{Q}_2$. That is, if K is any field with $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$, then there exists a non-trivial 2-henselian valuation v on K such that the residue field Kv is $\mathbb{F}_2$, the value group Γ_v is discrete with $v(2)$ a minimal positive element and $[\Gamma_v : 2\Gamma_v] = 2$.

The proof hinges on the fact that any field K for which $G_K(p)$ is Demushkin satisfies a 'local reciprocity' law induced by the norm map (see Proposition 3.2.6), established in Section 2. As noted in Remark 2.5.5, this was the crucial input in Proposition 2.5.3; the same is true here. The proof then proceeds in three steps. First, one uses the explicit structure of $G_{\mathbb{Q}_2}(2)$ to make some preliminary observations about $K^\times/(K^\times)^2$, which in turn imply that $char(K) = 0$. Secondly, putting $k = K \cap \overline{\mathbb{Q}}$, we show using class field theory that except in one exceptional case, k embeds into $\mathbb{Q}_2 \cap \overline{\mathbb{Q}}$ and hence that $K^\times/(K^\times)^2$ is generated as an $\mathbb{F}_2$-vector space by $-1, 2$ and 5. Assuming that we are not in the exceptional case, a consequence of this and 'local reciprocity' is that the 'lattice' of norm subgroups $Norm(K(\sqrt{a})^\times) \leqslant K^\times$ for $a \in K \setminus K^2$ is identical to that of $\mathbb{Q}_2$. Thirdly, we use an adaptation of the rigid element method to construct a valuation ring which satisfies all the desired properties. The fact that our construction yields a valuation ring depends on checking that certain elements in K are elements of certain norm subgroups. It turns out that this depends purely on the 'combinatorics' of the lattice of norm subgroups. Therefore, the existence of the desired valuation ring is lifted from k to K. This part is still quite mysterious: we cannot yet provide a good argument for why it works other than by direct calculations. Many of these calculations are relegated to the appendices to aid exposition. Finally, we show that the exceptional case simply cannot occur. This is done by showing that in this case,

k admits a p-adic valuation for $p \neq 2$. Another application of the technique of norm-combinatorics allows us to lift this to a p-adic valuation on K, which is encoded in $G_K(2)$ by one of the main results from [12]. The fact that $\mathbb{Q}_2$ doesn't admit such a valuation allows us thereby to obtain the desired contradiction.

We do not currently have any ideas for how to prove Conjecture 2, though see [3] for connections between Conjecture 1 and 2.

Let us remark that there is no *conceptual* obstruction to carrying out a similar proof in cases where $p > 2$. However, in its current state, the method of proof relies heavily on explicit computations, which quickly become intractable for fields like $\mathbb{Q}_p(\zeta_p)$ with $p > 2$.

In fact, by more closely analysing the proof of the main theorem, we show that one can get away with an even smaller quotient of the Galois group, the so-called maximal $\mathbb{Z}/p$ elementary meta-abelian quotient.

3.2 Demushkin Fields and the 'Local Reciprocity Law'

We start by recalling some basic facts about Demushkin groups and the connection with Brauer groups.

Definition 3.2.1. Let G be a finitely generated pro-p group for some prime p. We say G is **Demushkin** if

(i) $dim_{\mathbb{F}_p}(H^1(G, \mathbb{Z}/p\mathbb{Z})) = n < \infty$

(ii) $dim_{\mathbb{F}_p}(H^2(G, \mathbb{Z}/p\mathbb{Z})) = 1$

(iii) The cup product $H^1(G, \mathbb{Z}/p\mathbb{Z}) \times H^1(G, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z}$ is a *non-degenerate* bilinear pairing.

Definition 3.2.2. Let K be a field containing ζ_p. We say that K is a **Demushkin field** whenever $G_K(p)$ is a Demushkin group.

Examples of Demushkin fields are finite extensions K of $\mathbb{Q}_p$ containing ζ_p ([33], 5.6). In this case, the structure of $G_K(p)$ is known: it is generated by $N+2$ elements subject to a single relation r. Here $N = [K : \mathbb{Q}_p]$ and the relation r can be specified (see below). Also, if K is a finite extension of $\mathbb{Q}_l$ containing ζ_l, where $l \neq p$, then $G_F(p)$ is also Demushkin of rank 2, being isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_p$.

From Chapter 1, Section 1, the Demushkin property of $G_K(p)$ translates into the following field-theoretic statements:

- $K^\times/(K^\times)^p$ is finite;
- ${}_pBr(K) \simeq \mathbb{Z}/p\mathbb{Z}$;
- Given any $a \in K^\times$, there exists $b \in K^\times$ such that $(a,b)_K \neq 1$.

If we denote by p^s the maximal power of p such that $\zeta_{p^s} \in K$, then one can pick generators $x_1, \dots, x_{N+2}$ of $G_K(p)$ such that

$$r = x_1^{p^s}[x_1, x_2]...[x_{N+1}, x_{N+2}]$$

if $p^s \neq 2$ and N is even[3], where $x_1^{p^s}$ is defined to be 1 if $s = \infty$. If $p^s = 2$ and N is odd,

$$r = x_1^2 x_2^4 [x_2, x_3][x_4, x_5] \dots [x_{N+1}, x_{N+2}]$$

where $[a,b]$ denotes the commutator. Passing to the abelianization it is not hard to see the following:

Fact 3.2.3. *Let F be a finite extension of $\mathbb{Q}_p$ containing ζ_p, with N and s as above. If $p^s \neq 2$, or $p^s = 2, N = 1$ (i.e., $F = \mathbb{Q}_2$), then*

$$G_F(p)^{ab} \simeq \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}_p^{N+1}$$

and the isomorphism type of $G_F(p)$ is entirely determined by the integers s and N.

[3] Note that $p^s \neq 2$ implies that $[K : \mathbb{Q}_p]$ is even and so N is even, since $\zeta_p \in K$ and $[\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p] = p - 1$ is even.

Proof. If $r = x_1^{p^s}[x_1, x_2]...[x_{N+1}, x_{N+2}]$ this is clear. If

$$r = x_1^2 x_2^4 [x_2, x_3][x_4, x_5] \dots [x_{N+1}, x_{N+2}],$$

then after taking the abelianization, we get $G_K(p) \simeq \langle x_1, \dots x_{N+2} : x_1^2 x_2^4 = 1 \rangle$. Putting $z = x_1 x_2^2$, we see that this is the same as the group generated by $z, x_2, \dots, x_{N+2}$, modulo the single relation $z^2 = 1$, from whence we get the required isomorphism. □

Remark 3.2.4. Since the isomorphism type of $G_K(p)$ is determined entirely by N and s, we see that for example $\mathbb{Q}_2(\sqrt{2})$ and $\mathbb{Q}_2(\sqrt{5})$ have the same pro-2 Galois groups, as neither extension adds any new 2^k-th roots of unity.

Remark 3.2.5. Note that the fields $\mathbb{Q}_p(\zeta_p)$ are the only finite extensions of $\mathbb{Q}_p$ containing ζ_p with $s = 1$ and $N + 2 = p + 1$. Therefore for these fields, in Conjecture 1 F' may be taken to be F itself.

The crucial fact about Demushkin fields which we use is that they satisfy the following form of 'local reciprocity law'. The statement and proof here are due to Frohn and can be found in her thesis [5]. For the convenience of the reader we reproduce the proof here.

Proposition 3.2.6. *('Local Reciprocity') Let K be a Demushkin field with respect to p. Then for each $a \in K^\times \setminus (K^\times)^p$, $N(a)$ is a subgroup of $K^\times$ of index p, and the map*

$$\phi : \{K(\sqrt[p]{a}) : a \in K^\times \setminus (K^\times)^p\} \to \{H \leq K^\times/(K^\times)^p : H \text{ has index } p\}$$

given by $K(\sqrt[p]{a}) \mapsto N(a)$ is a bijection between Galois extensions of degree p and subgroups of $K^\times/(K^\times)^p$ of index p. Conversely, any field K containing ζ_p for which ϕ is a bijection is necessarily Demushkin.

Proof. Let us first prove that if K is Demushkin, then ϕ is a bijection.

Fix $a \in K^\times \setminus (K^\times)^p$. The induced map

$$\begin{aligned} K^\times/(K^\times)^p &\to \mathbb{Z}/p\mathbb{Z} \\ b &\mapsto (a, b) \end{aligned}$$

is surjective by virtue of the pairing being non-degenerate. Its kernel $N(a)$ is thus a subgroup of index p.

For any finite dimensional vector space, the number of subspaces of dimension 1 equals the number of subspaces of codimension 1. Since $K^\times/(K^\times)^p$ has finite $\mathbb{F}_p$-dimension by virtue of K being Demushkin, and one-dimensional subspaces of $K^\times/(K^\times)^p$ correspond to extensions of K of degree p, we have

$$|\{K(\sqrt[p]{a}) : a \in K^\times \setminus (K^\times)^p\}| = |\{H \leq K^\times/(K^\times)^p : \text{H has index p}\}| < \infty$$

Thus it suffices to show ϕ is injective. So let $a, b \in K^\times \setminus (K^\times)^p$ and suppose $N(a) = N(b)$. Since the pairing is non-degenerate, we may pick $x \in K^\times/(K^\times)^p$ such that (a, x) is non-trivial, and therefore generates $(\mathbb{Z}/p\mathbb{Z})^\times$. So $(a^n, x) = (b, x)$ for some n coprime to p. Now let $y \in K^\times/(K^\times)^p$ be arbitrary, with $(a, x)^m = (a, y)$. Then

$$(a, x^m y^{-1}) = 1$$

which implies $x^m = sy$ with $s \in N(a) = N(b)$. A simple calculation using bilinearity of the Hilbert symbol shows that $(a^n b^{-1}, y) = 1$. Since this is true for every y, non-degeneracy again implies that $a^n = b$ in $K^\times/(K^\times)^p$, whence they generate the same extension of K, as desired.

For the converse, suppose $\zeta_p \in K$ and that ϕ is a bijection. In particular, the norm groups $N(a)$ have index p in $K^\times/(K^\times)^p$ and are therefore all *proper* subgroups. Thus the pairing is non-degenerate. Since $G_K(p)$ is assumed finitely generated, $\dim_{\mathbb{F}_p} H^1(G_K(p), \mathbb{Z}/p\mathbb{Z}) < \infty$. It remains therefore only to show that $H^2(G_K(p), \mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$: by Merkurjev-Suslin, this is equivalent to showing ${}_pBr(K) \simeq \mathbb{Z}/p\mathbb{Z}$. Let $(a, b) \in {}_pBr(K)$ be non-trivial. It suffices to show that $(x, b) = (a, b)^k$ for some k, for any x such that $(x, b) \neq 1$. For then if $(c, d) \in {}_pBr(K)$ is arbitrary, we simply pick $x \in K^\times \setminus (N(b) \cup N(c))$: then (x, b) and (x, c) are non-trivial, and $(c, d) = (c, x)^i = (b, x)^{ij} = (a, b)^{ijk}$ for some i, j, k, whence (a, b) is a generator of order p. But if (a, b) is non-trivial and $x \notin N(b)$, then $x \in b^k N(a)$ for some k, since $1, b, \ldots, b^{p-1}$ are coset representatives for $K^\times/N(a)$. But then it is easy to see that $(a, b)^k = (a, b^k) = (a, x)$, so we are done. □

Remark 3.2.7. In the case $p = 2$, we get from this that $N(a) = N(b)$ if and only if a and b are *equal* modulo squares. This will be crucially exploited in what follows.

3.3 The structure of $K^\times/(K^\times)^2$

For the rest of this chapter we now fix once and for all a field K with

$$G_K(2) \simeq G_{\mathbb{Q}_2}(2).$$

Definition 3.3.1. For any field L, and a prime p, let

$$q_p(L) := dim_{\mathbb{F}_p} L^\times/(L^\times)^p.$$

For $x, y \in L^\times$, we write $x \sim y$ if the classes of x and y in $L^\times/(L^\times)^p$ are the same, i.e., if $x/y \in (L^\times)^p$. If $x_1, \ldots, x_n \in L^\times$, we write

$$\langle x_1, \ldots, x_n \rangle$$

for the subspace of $L^\times/(L^\times)^p$ generated by $x_1(L^\times)^p, \ldots, x_n(L^\times)^p$. So as a multiplicative group, $\langle x_1, \ldots, x_n \rangle$ is generated by the various products $x_{i_1} \ldots x_{i_k}$ and their powers.

In this section we aim to prove that the structure of $K^\times/(K^\times)^2$ is essentially the same as that of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. Let us first recall the structure of the latter group.

Proposition 3.3.2. *The group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ has dimension $q_2(\mathbb{Q}_2) = 3$. A basis is given by the square classes of $-1, 2$ and 5. Hence $\mathbb{Q}_2^\times = \{\pm 1, \pm 2, \pm 5, \pm 10\}$ modulo squares.*

Proof. See e.g. [32] Chapter 2. □

We will show that the same is true for $K^\times/(K^\times)^2$. Indeed, we will show the stronger statement that any relation between square classes of *algebraic* elements in $\mathbb{Q}_2$ also holds in K. For example, in $\mathbb{Q}_2$, it is true that $3 = -5$ modulo squares, so the same will also hold in K. This will be made precise in Proposition 3.3.11 below.

First observe that by Kummer Theory, we have isomorphisms of $\mathbb{F}_2$-vector spaces

$$K^\times/(K^\times)^2 \simeq Hom(G_K(2), \mathbb{Z}/2\mathbb{Z}) \simeq Hom(G_{\mathbb{Q}_2}(2), \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$$

and hence $q_2(K) = q_2(\mathbb{Q}_2) = 3$.

Let us now show that -1 and 2 are independent, non-trivial square classes in $K^\times/(K^\times)^2$.

Lemma 3.3.3. *(i) There is a quadratic extension of $\mathbb{Q}_2$ which does not embed into a $\mathbb{Z}/4\mathbb{Z}$-extension of $\mathbb{Q}_2$, i.e., a Galois extension $L/\mathbb{Q}_2$ with Galois group $\mathrm{Gal(L/\mathbb{Q}_2)} \simeq \mathbb{Z}/4\mathbb{Z}$.*

(ii) There is no open subgroup H of $G^{ab}_{\mathbb{Q}_2}(2)$ of index 2 such that

$$H \simeq \mathbb{Z}/2^s\mathbb{Z} \times \mathbb{Z}_2^3$$

with $s \geq 3$.

Proof. By Fact 3.2.3,

$$G_{\mathbb{Q}_2}(2)^{ab} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2$$

from which one may readily deduce the first claim.

For (ii), note any such subgroup would correspond to a quadratic extension of $\mathbb{Q}_2$ which would have to contain ζ_8, since for a Demushkin field, the cyclotomic height is encoded by the torsion part of the abelianization of its Galois group (see the discussion preceding Fact 3.2.3). But since $\zeta_8 = 1/\sqrt{2} + i/\sqrt{2}$, and $\sqrt{2} \notin \mathbb{Q}_2(i)$, any such extension would have to have degree at least 4, giving a contradiction. □

Lemma 3.3.4. *(i) The characteristic of K is not 2, and $-1 \notin K^2$. In particular, $2 \in K^\times$.*

(ii) $2 \notin K(\sqrt{-1})^2$

(iii) -1 is not the sum of two squares, and char(K)=0.

Proof. The property (i) in the previous lemma is evidently equivalent to a statement about $G_{\mathbb{Q}_2}(2)$, and hence the statement is also true of K. But if char(K)=2, or $\sqrt{-1} \in K$, then every (separable) quadratic extension embeds into a $\mathbb{Z}/4\mathbb{Z}$-extension. In particular 2 is non-zero in K.

For (ii), note that if $\sqrt{2} \in K(i)$, then $K(i)$ contains ζ_8, and hence, by Fact 3.2.3, $K(i)$ induces an open subgroup of $G_K^{ab}(2)$ of index 2 with torsion part $\mathbb{Z}/2^s\mathbb{Z}$, $s \geq 3$. This being a statement about $G_K(2)$, the same would be true for $G_{\mathbb{Q}_2}(2)$, contradicting the previous lemma.

For (iii), note that by (ii), it follows that -1 and 2 are independent and non-trivial square classes in $K^\times/(K^\times)^2$. If -1 were a sum of two squares, that is, if $-1 \in N(-1)$, then since $2 \in N(-1)$ also, $N(-1) = \langle -1, 2\rangle$. So $-2 \in N(-1)$ whence $-1 \in N(-2)$, and so $N(-2) = \langle -1, 2\rangle = N(-1)$. By Proposition 3.2.6 and Remark 2.8, 2 is a square: contradiction.

In particular, since in any finite field, -1 is a sum of two squares, the characteristic of K must be 0. □

By the above lemma, we may now define the field $k := K \cap \overline{\mathbb{Q}}$. That is, k is the relative algebraic closure of $\mathbb{Q}$ in K. Our next goal is to elucidate the structure of k, and show that except for one 'bad case', k admits a '2-adic' valuation, i.e., a valuation such that the henselization k^h of k is isomorphic to $\mathbb{Q}_2 \cap \overline{\mathbb{Q}}$. Note that this latter field can be identified with the henselization $\mathbb{Q}^h$ of $\mathbb{Q}$ with respect to the 2-adic valuation, and is elementarily equivalent to $\mathbb{Q}_2$ (c.f. e.g [28]). In particular, k is a subfield of $\mathbb{Q}_2 \cap \overline{\mathbb{Q}}$.

Before proceeding with the next proposition, let us recall some results about extensions of p-adic fields.

Lemma 3.3.5. *Let $L/\mathbb{Q}_p$ be an extension containing a primitive p-th root of unity ζ_p.*

(i) If the extension is finite, then $q_p(L) = [L : \mathbb{Q}_p] + 2$

(ii) If p^∞ divides $[L : \mathbb{Q}_p]$, then ${}_pBr(L) = 0$.

Both statements are also true if we replace $\mathbb{Q}_p$ with $\mathbb{Q}^h$, the henselization of $\mathbb{Q}$ with respect to the p-adic valuation.[4]

Proof. See e.g. [33], 5.6, Lemma 3 and Theorem 4, for proofs of (i) and (ii).

Now let us consider both statements with completions replaced by henselizations. First consider (i), so $L/\mathbb{Q}^h$ is a finite extension and L contains ζ_p. Then, by virtue of being henselian, $[L : \mathbb{Q}^h] = [\hat{L} : \mathbb{Q}_p]$, where $\hat{L}$ denotes the completion (this follows e.g. from [22] Chapter 2, Corollary 8.4). But we also have $q_p(L) = q_p(\hat{L})$. Indeed, L (resp. $\mathbb{Q}^h$) is elementarily equivalent to $\hat{L}$ (resp. $\mathbb{Q}_p$), by virtue of being p-adically closed (see e.g. [28]). Hence the two fields satisfy all the same algebraic identities. In particular they must have the same number of inequivalent square classes. This implies the formula (i) for $L/\mathbb{Q}^h$.

For (ii), again, if $p^\infty \mid [L : \mathbb{Q}^h]$, then for every n we can find a finite subextension $F/\mathbb{Q}^h$ of L with $p^n \mid [F : \mathbb{Q}^h]$. Then $p^n \mid [F\mathbb{Q}_p : \mathbb{Q}_p]$ with $F\mathbb{Q}_p$ a finite subextension of $\tilde{L} := L\mathbb{Q}_p$. Hence ${}_pBr(\tilde{L}) = 0$. We want to show that also ${}_pBr(L) = 0$.

By the Merkurjev-Suslin Theorem ([17]), ${}_pBr(L)$ is generated by the cyclic algebras $(a, b)_L$. Therefore it suffices to show that $(a, b)_L = 1$ for any $a, b \in L$. We know that $(a, b)_{\tilde{L}} = 1$. Let $\tilde{F}$ be the extension of $\mathbb{Q}_p$ generated by a, b and the coefficients of a solution in $\tilde{L}$ to the equation $b = Norm_{\tilde{L}(\sqrt[p]{a})}(x)$, where $x \in \tilde{L}(\sqrt[p]{a})$. Then $(a, b)_{\tilde{F}} = 1$ by construction. But now $\tilde{F}$ is a *finite* extension of $\mathbb{Q}_p$, and hence is elementarily equivalent to $F := \tilde{F} \cap \overline{\mathbb{Q}} \subset L$. Since the statement $(a, b) = 1$ is equivalent to an existential sentence expressing b as a norm depending only on the parameter a, it follows that $(a, b)_F = 1$. Therefore ${}_pBr(L) = 1$. □

We will also require the following well known result of class field theory (see [22] Chapter 6, Corollary 4.5):

Theorem 3.3.6. *(Hasse Norm Theorem) Let L/F be a cyclic extension of number fields. Then for any $x \in F$, $x \in N(L)$ if and only if $x \in N(L_v)$ for every completion L_v/F_v.*

[4] This is an example of the well known slogan that as far as algebra is concerned, henselizations are as good as completions.

Remark 3.3.7. As with the above lemma, the statement is still true if we consider henselizations and real closures rather than completions, by similar reasoning.

We are now ready to characterize the structure of k. Let us begin with a basic observation.

Lemma 3.3.8. *Let $k = K \cap \overline{\mathbb{Q}}$. Then $q_2(k) = 3$.*

Proof. We have $q_2(k) \leq q_2(K) = 3$. Since -1 and 2 are independent in $k^\times/(k^\times)^2$, $q_2(k) = 2$ or 3. Suppose, for a contradiction, that $q_2(k) = 2$. Since $2 \in N_k(-1)$ is non-square, k is not Pythagorean. By [16] II. Proposition 5.1, this implies that the Witt ring $W(k) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. By Table 5.2 in [7], we find that $G_k(2) \simeq \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$. Similarly one sees that $G_{k(i)}(2) \simeq \mathbb{Z}_2$, and so $q_2(k(i)) = 1$.

However, a simple calculation shows that since 2 is not a square in $k(i)$, neither is i. Further, $1 + i$ and $i(1 + i)$ both have norm 2, so i and $1 + i$ are independent non-squares in $k(i)$, contradicting $q_2(k(i)) = 1$. □

We are now ready for the crucial lemma. Before stating the result, recall that a valuation v is called **tamely branching** at a prime p if the residue characteristic is not p, the value group Γ_v is not p-divisible, and if $[\Gamma_v : p\Gamma_v] = p$, then the residue field is not p-closed.

Lemma 3.3.9. *Given $k = K \cap \overline{\mathbb{Q}}$, one of the following cases holds:*

(A) The restriction map $G_K(2) \to G_k(2)$ is an isomorphism, and $k^h = \overline{\mathbb{Q}} \cap \mathbb{Q}_2$;

(B) $G_k(2)$ is the free pro-2 product $\mathbb{Z}/2\mathbb{Z} *_2 (\mathbb{Z}_2 \rtimes \mathbb{Z}_2)$, and k admits both an ordering and a p-adic valuation tamely branching at 2 with $p \equiv 5\,(8)$.

Proof. Choose any chain of number fields $k_0 = \mathbb{Q} \subseteq k_1 \subseteq \ldots \subset k$ such that $k = \bigcup_{i=0}^{\infty} k_i$. By Lemma 3.3.4, $-1 \notin N_K(-1)$, so also $-1 \notin N_k(-1)$ and $-1 \notin N_{k_i}(-1)$ for any i. If we let Σ_i denote the set of orderings and valuations v of k_i for which $-1 \notin N_{k_i^v}(-1)$, where k_i^v is a real-closure, resp. a henselization, of k_i with respect to v, then by the Hasse Norm Theorem every Σ_i is non-empty. For $i < j$, each valuation in

Σ_j lies above a valuation in Σ_i. Now, it is easy to see that Σ_0 contains the archimedean valuation of $\mathbb{Q}$. Since it is only for $p = 2$ that the Hilbert symbol $(-1,-1)_p = -1$, we see that Σ_0 consists of exactly these two valuations, and hence every valuation in Σ_i lies above one of these. Since the Σ_i are finite (hence compact) and non-empty, their inverse limit Σ_∞ is non-empty by Tychonoff's Theorem, and every valuation $v \in \Sigma_\infty$ is either archimedean (corresponding to an ordering) or duadic. We now distinguish between two cases.

Case A: Suppose that Σ_∞ contains a duadic valuation v. If we let k^h denote the henselization of k with respect to v, then $-1 \notin N_{k^h}(-1)$. If we denote by $\mathbb{Q}^h$ a henselization of $\mathbb{Q}$ with respect to the 2-adic valuation (which we may without loss of generality take to be $\mathbb{Q}_2 \cap \overline{\mathbb{Q}}$) then there is a natural embedding $\mathbb{Q}^h \hookrightarrow k^h$. Let $F := k^h$. We claim that the extension $F/\mathbb{Q}^h$ is finite.

Indeed, first notice that if 2^∞ divides $[F : \mathbb{Q}^h]$, then ${}_2Br(F) = 0$ by Lemma 3.6. But the Brauer group of F contains the non-trivial degree-two element $(-1,-1)$, so this cannot be the case. Therefore there is a finite extension $L/\mathbb{Q}^h$ such that F/L has odd, possibly infinite, degree. Since F/L is of odd degree, the canonical map

$$L^\times/(L^\times)^2 \to F^\times/(F^\times)^2 \tag{3.1}$$

is injective, and indeed the same is true if we replace L by any finite subextension L'/L of F. Hence for any such L', $q_2(F) \geq q_2(L')$. But now, by Artin approximation, the canonical map

$$k^\times/(k^\times)^2 \to F^\times/(F^\times)^2$$

is *surjective*[5]. Putting this together, we therefore get

$$3 \geq q_2(k) \geq q_2(F) \geq q_2(L').$$

for any finite subextension L'/L of F. But by Lemma 3.6. (i),

$$q_2(L') = [L' : \mathbb{Q}^h] + 2 \geq 3 \tag{3.2}$$

[5] Another way of seeing this is that the map $Q_2(k) \to Q_2(\hat{k})$, where $\hat{k}$ is the completion, is surjective, since k is dense in its completion. But then $\hat{k}$ is also the completion of k^h.

and so $[L' : \mathbb{Q}^h] = 1$, whence we immediately deduce that $F = \mathbb{Q}^h$. Thus $k \hookrightarrow k^h = \mathbb{Q}^h = \mathbb{Q}_2 \cap \overline{\mathbb{Q}}$.

Since $q_2(k) = 3$ (Lemma 3.3.8), and $-1, 2$ and 5 form a basis for ${\mathbb{Q}^h}^\times/({\mathbb{Q}^h}^\times)^2$, it follows that $-1, 2$ and 5 also form a basis for $k^\times/(k^\times)^2$. We also know that $-3/5$ is a square in k, since this is true in k^h; it follows that $-5 \in N(-2)$. Since $G_{k^h}(2)$ is Demushkin of rank 3, the norm groups of k are generated by exactly 2 elements. From this it is easy to work out all the norm groups $N_k(a)$ for $a \in \{-1, \pm 2, \pm 5, \pm 10\}$. They are as follows:

- $N_k(-1) = \langle 2, 5\rangle$
- $N_k(2) = \langle -1, 2\rangle$
- $N_k(5) = \langle -1, 5\rangle$
- $N_k(10) = \langle -1, 10\rangle$
- $N_k(-2) = \langle 2, -5\rangle$
- $N_k(-5) = \langle -2, 5\rangle$
- $N_k(-10) = \langle -2, -5\rangle$

It follows by Proposition 3.2.6 that k is Demushkin of rank 3. Hence $G_K(2)$ and $G_k(2)$ are Demushkin with the same invariants, and so are isomorphic finitely generated pro-2 groups. Thus the epimorphism $G_K(2) \to G_k(2)$ is an isomorphism, by the profinite pidgeon-hole principle (see [29] Proposition 2.5.2).

Case B: Suppose Σ_∞ does not contain a duadic valuation. Then k is formally real, and $k^\times/(k^\times)^2 = \langle -1, 2, c\rangle$ for some $c \in k^\times$. We know as before that the norm groups are generated by at most 2 elements. In particular, either $N_k(-1) = \langle 2\rangle$ or we can choose c such that $N_k(-1) = \langle 2, c\rangle$. Suppose, for a contradiction, that $N_k(-1) = \langle 2\rangle$. Since $N_k(-1) = \cap P$, where the intersection is over all positive cones P of distinct orderings of k, and $N_k(-1)$ has index 4 in $k^\times$, k must admit two distinct orderings. Each of these will prolong in two distinct ways to $k(\sqrt{2})$, which therefore admits 4 distinct orderings. Notice next that $1 + \frac{1}{\sqrt{2}}$ has norm $1/2$, hence is not a square, but is positive with respect to any ordering on $k(\sqrt{2})$. Hence $k(\sqrt{2})$ is not Pythagorean. It follows that $q_2(k(\sqrt{2})) \geq 5$. But one also has $q_2(K(\sqrt{2})) = q_2(\mathbb{Q}_2(\sqrt{2})) = 4$, by a simple rank computation using Exercise 6, Chapter 4 of [33]. This gives a contradiction, since $k(\sqrt{2})$ is relatively algebraically closed in $K(\sqrt{2})$.

We conclude that $N_k(-1) = \langle 2, c\rangle$, and k admits a unique ordering with positive cone $N_k(-1)$. Note that since $N_k(2) = \langle -1, 2\rangle$, $c \notin N_k(2)$. However, being positive, $c \in N_{k^r}(2)$, where k^r is the real closure of k. A similar argument as before therefore shows that the set of valuations Σ^*_∞ for which $c \notin N_{k^h}(2)$ is non-empty, but does not contain a real place.

If Σ^*_∞ contains a duadic valuation, we end up back in Case A and we are done. So suppose it does not. Then it must contain a p-adic valuation v for which $v(c)$ is not 2-divisible, and by choosing c such that $c = 1 + a^2$ for some $a \in k$, $v(c)$ is odd and positive. Furthermore, -1 is a square in the residue field, while 2 is not, and hence $p \equiv 5\,(8)$. It follows, for example by another computation of the Witt ring of k, that $G_k(2) \simeq \mathbb{Z}/2\mathbb{Z} *_2 (\mathbb{Z}_2 \rtimes \mathbb{Z}_2)$ with presentation $\langle a, b, c : a^2 = b^4[b, c] = 1\rangle$. Here $\mathbb{Z}/2\mathbb{Z} = G_{k^r}(2)$, and $\mathbb{Z}_2 \rtimes \mathbb{Z}_2 \simeq G_{k^h}(2)$, where k^r (resp. k^h) is the real closure (resp. henselization) of k. □

We will ultimately show that Case B above does not occur. However, we have as of yet not found a way to rule this out other than by applying the norm-combinatorics machinery developed in Section 4. A major source of difficulty is that as remarked in the proof of Lemma 3.3.9, $G_k(2) \simeq \langle a, b, c : a^2 = b^4[b, c] = 1\rangle$ in Case B, and as an abstract group, this *does* in fact occur as a quotient of $G_K(2) \simeq \langle x, y, z : x^2y^4[y, z] = 1\rangle$. Therefore, Case B cannot be ruled out by purely group-theoretic reasons. As will be seen, our proof for ruling it out involves the arithmetic of the field in a subtle way. In Section 3.5 we will discuss how a new local-global principle for Brauer groups could be used to rule out Case B more easily. However, as we do not know how to prove such a principle, this approach remains speculative.

Remark 3.3.10. Let us also observe that there do exist algebraic extensions $k/\mathbb{Q}$ with $G_k(2) \simeq \mathbb{Z}/2\mathbb{Z} *_2 (\mathbb{Z}_2 \rtimes \mathbb{Z}_2)$. Indeed, consider $\mathbb{Q}$ with 5-adic valuation v_5, and let $\mathbb{Q}^h$

denote the 2-henselization of $\mathbb{Q}$ with respect to v_5. Then if we put $k = \mathbb{Q}(2) \cap \mathbb{R} \cap \mathbb{Q}^h$, we see that k admits both an ordering and a p-adic valuation tamely branching at 2. It follows, by the results of [2], that $G_k(2)$ is as desired. Therefore Case B can only be ruled out by the subtle interplay of the arithmetic of k and K.

Proposition 3.3.11. *Assume we are in Case A, that is, $k \subset \mathbb{Q}_2 \cap \overline{\mathbb{Q}}$. Then an $\mathbb{F}_2$-basis for $K^\times/(K^\times)^2$ is given by the classes of $-1, 2$ and 5. For any $q \in k$, $q \sim 1$ in K if and only if $q \sim 1$ in $\mathbb{Q}_2$. The quadratic norm groups $N(a)$ of K are all as follows:*

- $N_K(-1) = \langle 2, 5\rangle$
- $N_K(2) = \langle -1, 2\rangle$
- $N_K(5) = \langle -1, 5\rangle$
- $N_K(10) = \langle -1, 10\rangle$
- $N_K(-2) = \langle 2, -5\rangle$
- $N_K(-5) = \langle -2, 5\rangle$
- $N_K(-10) = \langle -2, -5\rangle$

Proof. Since $-1, 2$ and 5 form a basis for $k^\times/(k^\times)^2$, they are independent modulo squares, and since $K^\times/(K^\times)^2$ has dimension 3, these also form a basis of $K^\times/(K^\times)^2$. The structure of the norm groups for K must be the same as that of k, since $K^\times/(K^\times)^2$ has the same basis as k and the norm groups have the same size. These were calculated in the proof of the above lemma, resulting in the above list. For the last part, note that $q \sim 1$ in K iff $q \sim 1$ in k, since if q were a non-square in k, it could only become a square in K if one of $\pm 1, \pm 2, \pm 5, \pm 10$ become square in k, which we know can't happen. Since k embeds into $\mathbb{Q}_2$, the same argument shows that $q \sim 1$ in k iff $q \sim 1$ in $\mathbb{Q}_2$. □

3.4 Construction of the Valuation: Norm Combinatorics

In $\mathbb{Q}_2$, we can detect the valuation ring via norms by the equality

$$Norm(\mathbb{Q}_2(\sqrt{5})^\times) = \mathbb{Z}_2^\times \cdot (\mathbb{Q}_2^\times)^2$$

which follows from the fact that $\mathbb{Q}_2(\sqrt{5})$ is the (unique) unramified quadratic extension of $\mathbb{Q}_2$. We will use this observation along with the rigid element construction from Chapter 2 to construct the valuation of Theorem 1. We recall the general setup.

Let p be a rational prime, F a field, $T \leqslant F^\times$ a subgroup containing $(F^\times)^p$. Define the sets

$$\begin{aligned} \mathcal{O}_1(T) &:= \{x \in F \setminus T : 1 + x \in T\} && (3.3) \\ \mathcal{O}_2(T) &:= \{x \in T : x\mathcal{O}_1(T) \subseteq \mathcal{O}_1(T)\} && (3.4) \end{aligned}$$

and

$$\mathcal{O}(T) := \mathcal{O}_1(T) \cup \mathcal{O}_2(T).$$

One may be tempted to use directly the statement in Proposition 2.4.2 for $p = 2$. However, there appears to be no obvious way to exclude the possibility that the subgroup T' of $K^\times$ obtained for which $\mathcal{O}(T')$ is a valuation ring, is in fact the whole of $K^\times$. That is, there is no way of telling if the valuation obtained is trivial or not. To show that T' may be taken to be $N(5)$ (i.e., to show), we will need to examine the construction more closely. The next Lemma identifies the arithmetic condition needed to avoid triviality.

Lemma 3.4.1. *Suppose that for any $x, y \in \mathcal{O}_1(T)$, one has $1 - xy \in T$. Then $\mathcal{O}$ is a (non-trivial) valuation ring of F with $\mathcal{O}^\times \subset T$ and $\mathcal{O}_1 \cdot \mathcal{O}_1 \subset \mathcal{O}_2$.*

Proof. This is a straightforward adaptation of Theorem 2.2.7 and its proof in [4]. □

Thus it is the condition that for $x, y \in \mathcal{O}_1(T)$, $1 - xy \in T$, that we will need to check, rather than the existence of rigid elements. In fact, the existence of rigid elements will be trivial in the cases we consider, and so can hardly be expected to offer much information.

Case A

In this section we will always be working with a field K such that $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$ and $k \subset \mathbb{Q}_2 \cap \overline{\mathbb{Q}}$. That is, we are in Case A of Lemma 3.3.9.

Consider the above construction with $p = 2$, $F = K$ and $T = N(5)$. In this case we write $\mathcal{O}_1$ instead of $\mathcal{O}_1(T)$ etc. Notice that for $K = \mathbb{Q}_2$, the elements in $\mathcal{O}_1$ (other than 0) are those with positive, odd valuation, by the ultrametric inequality, and so $\mathcal{O}_2$ consists of the 2-adic integers with even valuation. Therefore in this case $\mathcal{O}$ is indeed just $\mathbb{Z}_2$. We will show that the condition of the lemma holds for our abstract K as well, and then deduce that the valuation ring $\mathcal{O}(N(5))$ satisfies the additional properties desired.

The idea of the proof is to decompose the term $1 - xy$ in several ways, all of which are visibly in certain norm groups $N(a)$. Working on a case by case basis, depending on the square classes of $x, y, 1 + x$ and $1 + y$, this places $1 - xy$ in the intersection of several norm groups, which are known by Proposition 3.3.11. In all cases, the possible square classes of $1 - xy$ thus obtained are always in $N(5)$. As an intermediate step, we need to establish that $\pm 1, \pm 5$ and $\pm 1/5 \in \mathcal{O}_2$, i.e., that these numbers are 'units' in $\mathcal{O}$; of course we expect this to be true since these numbers are units in $\mathbb{Z}_2$. Doing this amounts to computing the square class of expressions $1 + ax$ when $x \in \mathcal{O}_1$ and $a \in \{\pm 1, \pm 5, \pm 1/5\}$. This is again done by writing $1 + ax$ as a norm in several different ways, thereby severely restricting its possible square class.

The proof shows that the square class of expressions like $1 + ax$, for $a \in k$, $x \in K$, is determined entirely by the square class of $x, 1 + x$ and the 'lattice' of norm-groups. If such a statement could be made rigorous and then proved, one could deduce that $\mathcal{O}(N(5))$ is a valuation ring simply because it is one for k. Unfortunately, such a structural proof still eludes us, and we instead resort to direct computations.

Remark 3.4.2. Notice that $0 \in \mathcal{O}_1(T)$ for any T. In the calculations and lemmas established in the following, we always ignore this case, as it can easily be seen that

0 will satisfy all the claims made, or that the resulting computation gives 0, which we know to be in $\mathcal{O}_1$.

Before we begin, let us for ease of exposition introduce some notation. For $a_i \in K^\times$, we write

$$\{a_1, a_2, \ldots, a_n\}$$

as shorthand for the subset

$$a_1(K^\times)^2 \cup a_2(K^\times)^2 \cup \ldots \cup a_n(K^\times)^2$$

of $K^\times$. We will also write $x \sim y$ to mean that x and y are equal modulo squares.

Our first lemma should be thought of as proving that $v(2) > 0$.

Lemma 3.4.3. *Let $x \in \mathcal{O}_1$. Then $1 + 2x$ and $1 + 4x$ are in $N(5)$.*

Proof. See Appendix A. The proof uses explicit calculations on a case by case basis, as explained above. □

Exploiting that $N(5)$ is closed under multiplication, the above lemma can be used to prove the crucial

Corollary 3.4.4. *$-1, 5$ and $1/5 \in \mathcal{O}_2$, and consequently so is -5 and $-1/5$.*

Proof. We need to show that if $x \in \mathcal{O}_1$, then also $-x, 5x$ and $x/5$ are in $\mathcal{O}_1$. That then also -5 and $-1/5$ are in $\mathcal{O}_2$ follows since $\mathcal{O}_2$ is clearly closed under multiplication.

If $x \in \mathcal{O}_1$, then[6] so is $-x/(1+x)$, and hence, by Lemma 3.4.3, $1-2x/(1+x) \in N(5)$, whence $(1 + x)(1 - 2x/(1 + x)) = 1 - x \in N(5)$. So $-x \in \mathcal{O}_1$.

Next, for any $x \in \mathcal{O}_1, -x/(1 + x) \in \mathcal{O}_1$ and consequently so is $x/(1 + x)$ by the above. Thus, by Lemma 3.4.3, $1+4x/(1+x) \in N(5)$, whence $(1+x)(1+4x/(1+x)) = 1 + 5x \in N(5)$. Hence $5x \in \mathcal{O}_1$.

Finally, if $x \in \mathcal{O}_1$, then $1-2/(1+x) = -(1-x)/(1+x) \in N(5)$ so $-2/(1+x) \in \mathcal{O}_1$. Since we know already that $-1 \in \mathcal{O}_2$, we get $2/(1 + x) \in \mathcal{O}_1$ and so $1 + 4/(1 + x) \in$

[6] Observe that $-x/(1 + x)$ is not in $N(5)$ and $1 - x/(1 + x) = 1/(1 + x) \in N(5)$.

$N(5)$, whence $(1+4/(1+x))(1+x) = 5+x \in N(5)$, and so $1+(1/5)x \in N(5)$. Hence $1/5 \in \mathcal{O}_2$. □

We are now ready to prove the critical

Proposition 3.4.5. *For any $x, y \in \mathcal{O}_1$, $1 - xy \in N(5)$.*

Proof. The key point is to note the following decompositions:

$$\begin{aligned} 1 - xy &= (1+y)\left(1 + (1+x)\frac{-y}{1+y}\right) \\ &= (1-y)\left(1 + (1-x)\frac{y}{1-y}\right) \\ &= (1+5y)\left(1 + (1+5^{-1}x)\frac{-5y}{1+5y}\right) \\ &= (1-5y)\left(1 + (1-5^{-1}x)\frac{5y}{1-5y}\right) \end{aligned}$$

Therefore, thanks to Corollary 3.4.4, it suffices to show for example that $1+(1+x)y' \in N(5)$, where $y' = -y/(1+y)$. Now one notes that $1 + (1+x)y' = (1+x) + xy' = (1+x)(1+y') - y'$. Therefore if we know the square classes of $x, y, 1+x$ and $1+y$, this gives three different expressions of $1 + (1+x)y'$ as a norm, severely limiting the possible square class of $1 - xy$. By doing the same procedure for different choices of a decomposition of $1-xy$, one can show, case by case, that one always has $1-xy \in N(5)$. Since it is known that the expressions $1 + ax$, $a \in \{\pm 1, \pm 5, \pm 5^{-1}\}$, are all in $N(5)$, it is straightforward to pin down their exact square class in many cases (see Appendix A), and this is used throughout.

This is all elementary, but tedious. The calculations may be found in Appendix A. We include one case here to exemplify the above remarks.

Suppose $x \sim -2, 1+x \sim 1, y \sim -2, 1+y \sim 1$. Then

$$1 - xy \sim 1 + (1+x)\frac{-y}{1+y} \in N(-2)$$

Also, one can quickly check that $1 + 5^{-1}x \sim 1, 1 + 5y \sim 1$. Indeed, $1 + 5^{-1}x \in N(10)$ so $5 + x \in 5N(10)$. Also $5 + x = (1 + x) + 4 \in N(-1)$, and since we also know $5 + x \in N(5)$ by Corollary 3.4.4, we must have $5 + x \sim 5$, so $1 + 5^{-1}x \sim 1$ as claimed. Similarly, $5(1+5^{-1}y) = (1+y)+4$. The first expression is visibly in $5N(10)$ while the second is visible in $N(-1)$. But also $5+y \in N(5)$ since $5 \in \mathcal{O}_2$. Hence $5+y \in N(5) \cap 5N(10) \cap N(-1) = \{5\}$. Hence $1+5^{-1}y \sim 1$.

It follows that

$$1 - xy \sim 1 + (1+5^{-1}x)\frac{-5y}{1+5y} \in N(-10)$$

Thus $1 - xy \in N(-2) \cap N(-10) = \{1, -5\} \subset N(5)$ as desired. □

Corollary 3.4.6. *The set $\mathcal{O}$ is a non-trivial valuation ring of K with residue characteristic* 2.

Proof. Non-triviality is clear since $\mathcal{O}^\times \subset N(5)$. Also, since $2 \notin N(5)$, the value of 2 is strictly positive, whence 2 becomes trivial in the residue field.

□

Remark 3.4.7. *We will now choose a valuation v with $\mathcal{O}_v = \mathcal{O}$, and denote the value group, maximal ideal and residue field of v as Γ, $\mathcal{M}$ and Kv respectively.*

We now elucidate the structure of $\mathcal{O}_2$ further. Put

$$A := \{x \in N(5) : 1 + 2x \in N(5)\} \tag{3.5}$$

In $\mathbb{Q}_2$, this set coincides, by the ultrametric inequality, with the 2-adic integers with even valuation. Hence we expect the following

Lemma 3.4.8. $\mathcal{O}_2 = A$.

Proof. One direction is trivial: if $x \in \mathcal{O}_2$ then as $2 \in \mathcal{O}_1$, we have $2x \in \mathcal{O}_1$ so that $1 + 2x \in N(5)$. That is, $x \in A$.

For the other direction, note that if $x \in A$ then $2x \in \mathcal{O}_1$. Hence A is invariant under multiplication by $\pm 1, \pm 5$ and $\pm 5^{-1}$. Suppose therefore that we can prove that for any $x \in A$ with $x \sim 1$, that $x \in \mathcal{O}_2$. Then as $\mathcal{O}_2$ is also invariant under multiplication by those numbers, it easily follows that $x \in \mathcal{O}_2$ also when $x \sim -1$ or

± 5. Because $\mathcal{O}_2 \subset N(5) = \{\pm 1, \pm 5\}$, these are the only possible square classes of x. If $x \sim 1$, then in addition we know $1 + 2x \in N(5) \cap N(-2) = \{1, -5\}$. Thus we need only consider the following two cases:

- $\boxed{1 + 2x \sim 1}$ We need to show that for any $y \in \mathcal{O}_1$, $xy \in \mathcal{O}_1$. Since $\mathcal{O}_1$ is invariant under $\pm 1, \pm 5, \pm 5^{-1}$, as before, we can assume that $y \sim 2$, whence $1 - y \in N(5) \cap N(2) = \{\pm 1\}$.

  Suppose first $1 - y \sim 1$. Then if $1 + 2x = a^2$, we get $1 + 2xy = (1 - y) + a^2 y \in N(-1) \cap N(-2)$. But it's also in $N(5)$ since $-2x, y \in \mathcal{O}_1$ whence $1 - (-2x)y \in N(5)$ by Proposition 3.4.5. So $1 + 2xy \sim 1$. Hence $1 + 5xy = (1 + 2xy) + 3xy \in N(-10) \cap N(10) = \{1, 10\}$, using that $3 \sim -5$. If $1 + 5xy \sim 10$, we get $1 + 4xy = (1 + 5xy) - xy \in 2N(5)$. But since $\mathcal{O}$ is a ring, $2xy \in \mathcal{O}_2$ and so $4xy \in \mathcal{O}_1$, whence $1 + 4xy \in N(5)$, contradiction. So $1 + 5xy \in N(5)$, whence it follows that $5xy \in \mathcal{O}_1$ and hence so is xy.

  Suppose now that $1 - y \sim -1$. Then $1 + 2xy \in N(2) \cap N(5) \cap N(-1) = \{1\}$. Arguing as above, $1 + 5xy \in N(5)$ and we're done also in this case.

- $\boxed{1 + 2x \sim -5}$ First suppose $y \sim 2, 1 - y \sim 1$. Then $1 + 2x = -5a^2$ for some a, whence $1 + 2xy = (1 - y) - 5a^2 y$. Since $2x \in \mathcal{O}_1, 1 + 2xy \in N(5)$ as well. Consequently $1 + 2xy \in N(5) \cap N(-1) \cap N(10) = \{1\}$.

  It follows that $1 + xy = (1 + 2xy) - xy \in N(-2) \cap N(2) = \{1, 2\}$. If $1 + xy \sim 2$, then $1 + 4xy = (1 + xy) + 3xy \in 2N(5)$. But as $4xy \in \mathcal{O}_1$, $1 + 4xy \in N(5)$ as well, giving a contradiction. Hence $1 + xy \sim 1$ and we're done.

  Next suppose $y \sim 2, 1 - y \sim -1$. Then as above, we get $1 + 2xy = (1 - y) - 5a^2 y$ for some a, and so $1 + 2xy \in N(5) \cap -N(-10) \cap N(-1) = \{5\}$. Now $1 + 5xy = (1 + 2xy) + 3xy \in 5N(2) \cap N(-10) = \{-5, 10\}$. If $1 + 5xy \sim 10$, then $1 + 4xy = (1 + 5xy) - xy \in -2N(5) \cap N(5)$ which is empty. Hence we must have $1 + 5xy \sim -5$. That is, $5xy \in \mathcal{O}_1$, so $xy \in \mathcal{O}_1$ as well.

□

Since $\mathcal{O}^\times \subset \mathcal{O}_2$, we have

Corollary 3.4.9. *The units are*

$$\mathcal{O}^\times = \{x \in N(5) : 1 + 2x \in N(5) \text{ and } 2 + x \in N(5)\} \tag{3.6}$$

and the maximal ideal is the disjoint union $\mathcal{M} = \mathcal{O}_1 \sqcup B$ *where*

$$B := \{x \in N(5) : 1 + 2x \in N(5) \text{ and } 2 + x \notin N(5)\} \tag{3.7}$$

Proposition 3.4.10. $B = 2\mathcal{O}_1$.

Proof. If $x \in B$, then as $2+x \notin N(5)$, $1+x/2 \in N(5)$, so $x/2 \in \mathcal{O}_1$, whence $x \in 2\mathcal{O}_1$. The other direction follows easily from the previous Lemma in a similar fashion. □

Proposition 3.4.11. $v(2)$ *is a minimal positive element in* Γ.

Proof. Since $\mathcal{O}_1 \subset \mathcal{M}$, $v(2) > 0$. Now suppose we have $x \in \mathcal{M}$ with $v(x) < v(2)$, i.e., $2/x \in \mathcal{M} = \mathcal{O}_1 \cup 2\mathcal{O}_1$. If $2/x \in 2\mathcal{O}_1$, then $x^{-1} \in \mathcal{O}_1$, contradicting $v(x) > 0$. If $2/x \in \mathcal{O}_1$, then it cannot be the case that $x \in \mathcal{O}_1$, or else $2 \in \mathcal{O}_1 \cdot \mathcal{O}_1 \subset \mathcal{O}_2$. Hence $x \in 2\mathcal{O}_1$, so $x = 2y, y \in \mathcal{O}_1$. Then $v(2) > v(x) = v(2y) > v(2)$, which is absurd. □

Since $v(2) > 0$, it is clear that Kv has characteristic 2. In fact, more detailed calculations show that the residue field is exactly $\mathbb{F}_2$.

Proposition 3.4.12. *If* $x \in \mathcal{O}^\times$, *then* $1+x \in \mathcal{M}$. *In particular,* $\mathcal{O}/\mathcal{M}$ *contains only two elements, so is* $\mathbb{F}_2$.

Proof. As usual, one proceeds on a case by case basis.

Suppose $x \in \mathcal{O}^\times$ with $x \sim 1$. Then we aim to show $1 + x \notin N(5)$ and so in particular is not a unit. Indeed, $1 + 2x \in N(5) \cap N(-2) = \{1, -5\}$ and $2 + x \in N(5) \cap N(-2)$ as well. Suppose $1+2x \sim 1$, equalling a^2 say. Then $2+x = a^2/2+3/2$, and since $3 \sim -5$, this is in $2N(5)$, a contradiction.

So $1 + 2x \sim -5$, and a similar calculation shows $2 + x \in N(-1)$, so $2 + x \sim -5$.

Now $1 + x \in N(-1)$, so if it were also in $N(5)$, it would be equivalent to 1 or 5. But it is easy to check that both of these possibilities contradict $2 + x \sim -5$.

The other cases are similar. One shows either that $1 + x \notin N(5)$, or that $3 + x \notin N(5)$; the former implies $1 + x \in \mathcal{O}_1$, while the latter implies $1 + x \in 2\mathcal{O}_1$. The remaining cases may be found in Appendix B. □

Next, we would like to show 2-henselianity. We shall see that in our case, this property is inherited from the 2-henselianity of $k = K \cap \overline{\mathbb{Q}}$.

Proposition 3.4.13. *The valuation $\mathcal{O}$ is 2-henselian.*

Proof. It suffices to show that $\mathcal{O}$ extends uniquely to every quadratic extension of K. Recall that k^h can be identified with the henselization of $\mathbb{Q}$ with respect to the 2-adic valuation. Hence k^h is henselian, and the ramification indices and degrees with respect to the different quadratic extensions are known: we have $e = 1, f = 2$ for the extension $k^h(\sqrt{5})$, and $e = 2, f = 1$ for all the other extensions. Furthermore, note that both K and k^h have residue fields $\mathbb{F}_2$.

Hence if we let $\mathcal{O}'$ be any extension of $\mathcal{O}$ to $K(\sqrt{5})$, and let f' be the residue degree of the induced extension with respect to $k^h(\sqrt{5})/k^h$, we get, by multiplicativity of residue degrees, that $2 \geq f(\mathcal{O}'/\mathcal{O}) = 2f' \geq 2$, and hence $f(\mathcal{O}'/\mathcal{O}) = 2$.

For all the other quadratic extensions $L = K(\sqrt{a})$, we know that since $e(\mathcal{O}_L/\mathcal{O}) \leq 2$, we have that the index is either 2 or the value groups Γ_K and Γ_L are isomorphic. Let $k' = L \cap \overline{\mathbb{Q}} = k(\sqrt{a})$. Then since $\Gamma_{k^h} = \Gamma_K \cap \Gamma_{\overline{\mathbb{Q}}}$ and $\Gamma_{(k')^h} = \Gamma_L \cap \Gamma_{\overline{\mathbb{Q}}}$, it follows that if $\Gamma_K = \Gamma_L$, then $\Gamma_{k^h} = \Gamma_{(k')^h}$. Since for $a \not\sim 5$, the ramification index with respect to $(k')^h/k^h$ is always 2, it follows that it must also be 2 for L/K.

We have shown that for any quadratic extension of K, $ef = 2$ always holds, which implies by the fundamental inequality for valuations ([4] Theorem 3.3.4) that there is always at most one extension of $\mathcal{O}$ to any such field. Hence the valuation is 2-henselian. □

In the next section we will show that Case B of Lemma 3.3.9 does not occur. Therefore upon combining the above results we obtain at last our main result.

Theorem 3.4.14. *Suppose $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$. Then there is a valuation v on K which is 2-henselian, has discrete value group with $v(2)$ as a minimal positive element, residue field $\mathbb{F}_2$ and $[\Gamma : 2\Gamma] = 2$.*

Proof. The only thing remaining to prove is that $[\Gamma : 2\Gamma] = 2$. Note that $\Gamma \simeq K^\times/\mathcal{O}^\times$, and $\mathcal{O}^\times(K^\times)^2 = N(5)$. Since $v(\mathcal{O}^\times(K^\times)^2) = 2\Gamma$, and $N(5)$ has index 2 in $K^\times$, this implies that

$$\Gamma/2\Gamma \simeq \frac{K^\times}{\mathcal{O}^\times (K^\times)^2}$$

has order 2. □

In fact, upon reviewing the proof, we see that we didn't need all of $G_K(2)$, only the significantly smaller quotient $\mathrm{Gal(K''/K)}$, where K'' is the so-called maximal $\mathbb{Z}/2\mathbb{Z}$ elementary meta-abelian extension of K. Indeed, Lemma 3.3.3 and 3.3.4 clearly only need this quotient, and we saw in Chapter 1 that the Galois cohomology used is already seen by $\mathrm{Gal(K''/K)}$. Therefore we get the much stronger

Corollary 3.4.15. *Suppose* $\mathrm{Gal(K''/K)} \simeq \mathrm{Gal}(\mathbb{Q}_2''/\mathbb{Q}_2)$*. Then the conclusion of Theorem 3.4.14 holds.*

Case B

Suppose in this section that $G_K(2) \simeq G_{\mathbb{Q}_2}(2)$ and $k = K \cap \overline{\mathbb{Q}}$ satisfies the conditions of Case B in Lemma 3.3.9. Then k admits an ordering as well as a p-adic valuation v_p where $p \equiv 5\,(8)$. Furthermore, $k^\times/(k^\times)^2$ admits an $\mathbb{F}_2$-basis $\langle -1, 2, c\rangle$, where $v_p(c) > 0$ is odd. It is also straightforward now to work out the structure of the norm groups. Indeed, since we know that $N_k(-1) = \langle 2, c\rangle$, reciprocity quickly gives us $N_k(2), N_k(c)$ and $N_k(2c)$. Note that $G_k(2)$ is not Demushkin, so we cannot have $-c \in N_k(-2)$. Indeed, otherwise $N_k(-2) = \langle 2, c\rangle$, from which we quickly obtain $N_k(-c) = \langle -2, c\rangle$ and $N_k(-2c) = \langle -c, 2c\rangle$. Since all the norm groups then have index 2, Proposition 3.2.6 implies that $G_k(2)$ would be Demushkin.

In conclusion we get the following 'lattice':

- $N_k(-1) = \langle 2, c\rangle$
- $N_k(2) = \langle -1, 2\rangle$
- $N_k(c) = \langle -1, c\rangle$
- $N_k(2c) = \langle -1, 2c\rangle$
- $N_k(-2) = \langle 2\rangle$

- $N_k(-c) = \langle c \rangle$
- $N_k(-2c) = \langle 2c \rangle$

The 'lattice' for K is the same except $N_K(-2) = \langle 2, -c \rangle$, $N_K(-c) = \langle c, -2 \rangle$ and $N_K(-2c) = \langle 2c, -2 \rangle$

Since 2 is a square in the real closure of k but not in k, we must have that $2 \notin (k^h)^2$ and so, by henselianity, $2 \notin (k^h v_p)^2$. Thus $k^h(\sqrt{2})$ is the unique unramified extension of k^h, and so $\mathcal{O}(N_k(2))$ defines the p-adic valuation ring in k^h, and hence also in k. The goal now is to derive a contradiction from the following

Proposition 3.4.16. *If k is as described above, then $\mathcal{O}(N_K(2))$ defines a (non-trivial) valuation v on K with Kv not 2-closed.*

Indeed, taking this as given for the present, this valuation on K will not have 2-divisible value group, by virtue of the fact that $c \notin N(2)$. Hence the same is true for K^h, the 2-henselization of K, and the residue field is again not 2-closed. In other words, K^h admits a 2-henselian valuation tamely branching at 2. Then $G_{K^h}(2) \simeq \mathbb{Z}_l \rtimes \mathbb{Z}_l$ where l is the residue characteristic. By [12] Theorem 2.15, it follows that $\mathbb{Q}_2$ admits a (non-2-henselian) valuation w tamely branching at 2: in particular w has non-2-closed residue field. The henselization $\mathbb{Q}_2^w$ with respect to w therefore admits two henselian valuations, namely w and the duadic valuation. Since these have different residue characteristic they are incomparable. By F.K. Schmidt's Theorem (Theorem 4.4.1 in [4]) $\mathbb{Q}_2^w$ is algebraically closed, contradicting the fact that $\mathbb{Q}_2^w w$ is not 2-closed.

All that remains is to prove Proposition 3.4.16. We will do so using the same techniques as in Case A. The fact that we are working with an undetermined 'c' rather than the simple integer 5 might appear to make this a gruelling task. However, a closer inspection of the calculations in Case A show that the crucial information needed was the square values of $3, c-1, c-2, c-3$ and $c-4$. In Case A these were all easy to determine, and it turns out that any c such that $c-1 \sim 1, c-2 \sim -c, c-3 \sim 2, c-4 \sim 1$ would do in place of 5. In our present case, once we fix the value of 3, we can work out the rest of the values. Since $3 \in N_k(-2) = \langle 2 \rangle$, we have $3 \sim 1$ or $3 \sim 2$. It would be desirable to have a proof as in Lemma 3.3.3 which shows 3 is not a square, but while we suspect it may be possible to do so by considering dihedral extensions of $\mathbb{Q}_2$ of order 8, we have been unable to find such an argument. Instead both cases are considered separately.

The computations proceed the same way in both cases. First one shows by direct computation that whether $3 \sim 1$ or 2, we always have $\pm 1, \pm 2, \pm 1/2 \in \mathcal{O}_2$. This allows us to compile a list of the possible square classes of expressions $1 + ax$, where $a \in \{\pm 1, \pm 2, \pm 1/2\}$, $x \in \mathcal{O}_1$. This list turns out to be independent of the square class of 3. Finally, one uses this list to check that $1 - xy \in N(2)$ for any $x, y \in \mathcal{O}_1$, thereby completing the proof by Lemma 3.4.1. The details can all be found in Appendix C.

3.5 Model theoretic consequences

In a classic unpublished paper, Cherlin, van den Dries and Macintyre introduce a model theoretic formalism for studying profinite groups, and show that the elementary theory of G_F (in the profinite group language) is determined by the elementary theory of F (in the language of rings), provided G_F is finitely generated (see [5] for much more on this). That is, with respect to the languages specified, if F_1, F_2 are fields, then

$$F_1 \equiv F_2 \Rightarrow G_{F_1} \simeq G_{F_2},$$

where '$\equiv$' denotes elementary equivalence. As mentioned before, the main result of [10] can be seen as converse statement in the p-adic context: it showed that when F is p-adic, then the *isomorphism type* of G_F determines the elementary theory of F. That is, if F' is any other field, then

$$G_{F'} \simeq G_F \Rightarrow F' \equiv F.$$

It is not hard to show that any field with the same elementary theory as F has the same absolute Galois group, using that the Galois groups are finitely generated in this case. It is natural therefore to ask what model theory can be extracted from $G_F(p)$ based on Conjecture 1. The next result partially answers this question.

Theorem 3.5.1. *Suppose Conjecture 1 is true. Let F be a finite extension of $\mathbb{Q}_p$ containing ζ_p, and let K/F be a field extension such that*

$$G_F(p) \simeq G_K(p).$$

Then

$$K \models \sigma \iff F \models \sigma$$

where σ is any existential or universal sentence (in the language of rings) with parameters in F.

Proof. By Conjecture 1, K admits a p-adic valuation. By Lemma 1.3.4, there is a p-adic closure $\tilde{K}$ of K, which must be an elementary extension of F by Lemma 1.3.5:

$$\begin{tikzcd}
 & \tilde{K} \\
K \arrow[ur, hook] & F \arrow[l, hook'] \arrow[u, hook, "\preccurlyeq"']
\end{tikzcd}$$

Let σ be an existential sentence with parameters in F. Then it is immediate that if $F \models \sigma$, also $K \models \sigma$ since $F \subset K$. Conversely, if $K \models \sigma$, then also $\tilde{K} \models \sigma$, and so $F \models \sigma$ since $\tilde{K}$ is an elementary extension of F. Proceed similarly if σ is universal. □

As we will see in Chapter 4, the preservation of existential sentences in this context is in fact equivalent to a weak version of the Birational Section Conjecture for varieties over F.

Question: The above Theorem shows that for F p-adic, $G_F(p)$ encodes the existential and universal theory of F. It is unlikely that the converse is true. Is it nevertheless possible to find a set of sentences S, necessarily containing all existential and universal sentences, such that

$$G_K(p) \simeq G_F(p) \iff Th_S(K) = Th_S(F)?$$

where $Th_S(K)$, resp. $Th_S(F)$, denotes the subset of S of sentences true in K, resp. F? That is, can one isolate the 'p-part' of the theory of a field?

3.6 Local-global principles and Case B

We explore a potential alternative method for ruling out Case B. Having such methods would be preferable when looking to generalize the norm-combinatorics to larger primes, as the computations become cumbersome.

In [23], Pop derived a local-global principle for Brauer groups, which says that if K is finitely generated of transcendence degree 1 over k, where k is p-adically closed with p-adic valuation v, then

$$Br(K) \hookrightarrow \prod_w K^{h,w}$$

where the product ranges over all prolongations of v to w, and $K^{h,w}$ is the henselization of K with respect to w. This is used to great effect to recover p-adic valuations from an isomorphism $G_K \simeq G_k$ when K is finitely generated of transcendence degree 1 over k.

Now, in the context and notation of Case B, observe that it suffices to obtain a contradiction under the additional assumption that K is finitely generated of transcendence degree 1 over k, since if we pick a transcendental element in K over k and take the relative algebraic closure of $k(t)$ in K, we obtain a new field with the same pro-p Galois group as K and with algebraic part exactly k. However, k is not p-adically closed, so we cannot make use of Pop's local-global principle. What we know however is that since $G_k(2) \simeq G_{k^r}(2) *_2 G_{k^h}(2)$, where k^r (resp. k^h) is the real closure (resp. henselization) of k with respect to the ordering (resp. p-adic valuation), we have

$$_2Br(k) \simeq {_2Br(k^r)} \times {_2Br(k^h)}. \tag{3.8}$$

by general Galois cohomology. It is therefore perhaps not unreasonable to propose the following local-global principle, assuming that K is of transcendence degree 1 over

k:

$$_2Br(K) \hookrightarrow \prod_i {}_2Br(K^{r_i}) \times \prod_w {}_2Br(K^{h,w}) \tag{3.9}$$

where the r_i are all the extensions of the ordering from k to K, and w ranges over all extensions of the p-adic valuation to K. We have no idea how to prove a statement like this, but the following proposition demonstrates its potential power towards fully settling Conjecture 1.

Proposition 3.6.1. *Assume the local-global principle of (3.9) holds. Then Case B cannot occur.*

Proof. We know that $(-1,-1)_K = -1$. Since $G_K(2)$ does not admit any involutions, K does not admit any orderings, and so by (3.9) there must be a prolongation w of the p-adic valuation v on k to K, such that $(-1,-1)_{K^h} = -1$.

Let H be the 2-part of K^h/K, i.e. the maximal subextension such that 2 does not divide $[K^h : K]$. Then w', the restriction of w to H is 2-henselian and has residue characteristic $p > 2$. Since $(-1,-1)_{K^h} = -1$, also $(-1,-1)_H = -1$, and so ${}_2Br(H) \neq \{0\}$. Therefore $cd(G_H(2)) > 1$. As $G_K(2)$ is Demushkin, any closed subgroup of infinite index is free (see the exercises at the end of chapter 4, [33]). Therefore $G_H(2)$ is a closed subgroup of finite index, and so H is a *finite* extension of K. We thus know that $G_H(2)$ is finitely generated, with a 2-henselian valuation v with residue characteristic $p > 2$. Denote the valuation ring by $\mathcal{O}_v$.

If $\mathcal{O}_v[1/p] \neq H$, then $G_H(2)$ admits a non-trivial, normal abelian subgroup, namely the inertia subgroup of the corresponding valuation (with valuation ring $\mathcal{O}_v[1/p]$), which is abelian since its residue characteristic is 0. Hence there is a finite extension L of $\mathbb{Q}_2$ such that $G_L(2)$ has a non-trivial normal abelian subgroup. By Theorem 2.5.6, L admits a 2-henselian valuation tamely branching at 2, a contradiction.

Hence $\mathcal{O}_v[1/p] = K$. By Lemma 2.6.4, it follows that $\Gamma_{w'} \neq 2\Gamma_{w'}$. So it is still the case that H admits a non-trivial 2-henselian valuation tamely branching at 2, which gives a contradiction as above. □

3.7 The case $p > 2$

We discuss two possible, speculative, methods for proving Conjecture 1 for the cases $F = \mathbb{Q}_p(\zeta_p)$. The proof in the case $\mathbb{Q}_2$ suggests that the following assumption is not entirely unreasonable:

Assumption: If $G_K(p) \simeq G_F(p)$, then K is of characteristic 0 and $k := K \cap \overline{\mathbb{Q}}$ admits a p-adic valuation with henselization equal to $\mathbb{Q}_p(\zeta_p) \cap \overline{\mathbb{Q}}$, and $G_K(p) \simeq G_k(p)$ via the canonical restriction map.

Method 1: The same argument as in Proposition 3.3.11 shows that with the above assumption, K has the same basis for $K^\times/(K^\times)^p$ as F and the same norm groups as F. Therefore if $F(\sqrt[p]{a})$ is the unique unramified extension of F of degree p, then we put $T = N_K(a)$ and hope to show that this defines the desired valuation.

For $p > 2$, it is easier to use the rigid element construction. Indeed, by the main result of [10], it suffices now to show that there exists a single T-rigid element. That is, we need to find an x satisfying

$$1 + xN(a) \subseteq N(a) \cup xN(a). \tag{3.10}$$

In F, we can find such elements by taking any x with $v_p(x)$ not p-divisible. The proof in the case of $\mathbb{Q}_2$ suggests that the fact that such elements are indeed T-rigid should be witnessed by a finite number of equations with algebraic coefficients, each of the form

$$1 + xn = b(1 + c),$$

where $n \in N(a)$ and the p-th power classes of b and c depend entirely on the p-th power classes of $x, 1 + x$ and n. Each such equation pins down more precisely the possible class of x, and the collection of all the conditions imposed by these equations should show that for each choice of n, (3.10) is satisfied. It might be possible to demonstrate this for cases like e.g. $\mathbb{Q}_3(\zeta_3)$ by computing a basis for the cubes and using a computer to check for such witnessing equations. If such witnessing equations could indeed be found, then the fact that the norm groups of K and F are the same, the existence of a T-rigid element would be demonstrated for K as well, and hence a non-trivial valuation.

Method 2: Section 3.6 shows the power of a suitably generalized local-global principle. Indeed, Theorem B from [26] shows, using the local-global principle for p-adically closed fields, that if k is p-adically closed ($p > 2$) and K is any field extension with $G_K(p) \simeq G_k(p)$, then K admits a non-trivial p-adic valuation, thereby already going a long way towards proving Conjecture 1 in this special case. However, as per our Assumption, we cannot expect $k = K \cap \overline{\mathbb{Q}}$ to be p-adically closed. A generalized local-global principle as in Section 3.6 seems like it might be powerful enough to at least reproduce Pops result in this more general case.

Chapter 4

The Birational Section Conjecture

In this Chapter we use the results of the previous chapters to prove some minimalistic versions of the BSC, including some results for higher dimensional varieties.

We will only discuss the Birational version, and not the original conjecture phrased using étale fundamental groups. For an excellent exposition of all things related to the Section Conjecture, we refer the reader to [36].

4.1 The conjecture

Recall that given a smooth, complete curve X over a field K, there is a canonical exact sequence of Galois groups

$$1 \to G_{\overline{K}(X)} \to G_{K(X)} \to G_K \to 1 \tag{4.1}$$

where $K(X)$ is the function field of X and $\overline{K}(X) = \overline{K} \otimes_K K(X)$.

Given any $a \in X(K)$, we can assign to it a 'bouquet' of group-theoretic sections $s_a : G_K \to G_{K(X)}$. Indeed, let v_a be the valuation on $K(X)$ corresponding to a, and w the valuation on $\overline{K}(X)$ corresponding to a preimage of a in $\overline{X} := X \otimes_K \overline{K}$ (so w extends v). If we let I_w and D_w denote the inertia and decomposition group of w/v inside $G_{K(X)}$, then we get by Hilbert Decomposition Theory a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & G_{\overline{K}(X)} \arrow[r] & G_{K(X)} \arrow[r] & G_K \arrow[r] & 1 \\
1 \arrow[r] & I_w \arrow[r] \arrow[u] & D_w \arrow[r] \arrow[u] & G_w \arrow[r] \arrow[u, "\simeq"'] & 1
\end{tikzcd}$$

with exact rows. Here G_w denotes the Galois group of the residue field extension. It is known that the bottom row admits sections (see e.g. [15]). Any choice of such induces a section s_w of (4.1) such that $s(G_K) \subset D_w$, which is unique up to conjugation by an element of $G_{\overline{K}(X)}$. Any member of the 'bouquet' of sections obtained in this manner is said to lie over a. In a similar manner, if v is a valuation which is trivial on K and has residue field K, the same discussion shows that v induces a 'bouquet' of sections which are said to lie over v. We call such valuations **K-valuations**.

Remark 4.1.1. If we fix a canonical class $\mathcal{C}$, and suppose our fields contain the relevant roots of unity, then the above discussion also holds if we replace the absolute Galois groups in (4.1) with their maximal pro-c-quotients.

The *birational anabelian section conjecture* of Grothendieck says that *every* section of (8) lies over a unique $a \in X(K)$. This was proved in [13] in the case where K is a finite extension of $\mathbb{Q}_p$. Pop later showed in [25] that one could obtain a bijection already by considering a much smaller quotient of (8), the maximal $\mathbb{Z}/p\mathbb{Z}$ elementary meta-abelian quotient. Conjecture 1 implies that if the groundfield contains ζ_p, then one obtains a bijection when considering the maximal pro-p quotient. This already follows from Pop's Theorem, but the proof we give is independent.

We also note that the generality of the results from Chapter 2 and 3 mean we can prove a statement for varieties, not just curves. The pendant for the birational section conjecture in higher dimensions was proven by Stix in [35]: here one finds that every section lies over a unique K-valuation. When X is a curve, it is well known that such valuations correspond exactly to points. For higher dimensions, such valuations always imply the *existence* of a point, but the valuation itself need not be induced by this point. That is, non-geometric sections exist. In [26], Pop generalized this again to the meta-abelian setting, but only in the case when $p > 2$. Our main result allows us to partially fill this gap.

Example 4.1.2. Let $F = K(x, y)$ be the function field of any smooth, projective 2-dimensional variety over the field K. Define the valuation v on F by specifying $v(x) = 1, v(y) = \pi$ and making v trivial on K. Then v defines a K-valuation on F with value group $\mathbb{Z} \oplus \pi\mathbb{Z}$ (with lexicographic ordering), and hence does not equal the valuation associated to any K-rational point.

4.2 The p-adic BSC for p=2

Proposition 4.2.1. *Assume Conjecture 1 holds, and suppose X is a smooth, projective variety over F of dimension n, where F is a finite extension of $\mathbb{Q}_p$ containing ζ_p. Then given any section s of*

$$1 \to G_{\overline{F(X)}}(p) \to G_{F(X)}(p) \to G_F(p) \to 1 \tag{4.2}$$

there is a finite extension F' of $\mathbb{Q}_p$ containing ζ_p such that $G_{F'}(p) \simeq G_F(p)$ and $s'(G_{F'}(p)) \subset D_{w'}$ for a unique F'-valuation w'. Here $s' : G_{F'}(p) \to G_{F'(X)}(p)$ is the section induced by s.

Proof. Let $s : G_F(p) \to G_{F(X)}(p)$ be a section, and let K be the fixed field in $F(X)(p)$ of $s(G_F(p))$. Then $G_K(p) \simeq s(G_F(p)) \simeq G_F(p)$. By Conjecture 1, there is a finite extension $F'/\mathbb{Q}_p$ and a valuation v on K satisfying the properties of the Conjecture. In particular, the residue field is finite and $v(\pi)$ is a minimal positive element in Γ_v, where π is a uniformizer in F'. Then the restriction w of v to $F'(X)$ still has residue field $F'v$ and $w(\pi)$ is a minimal positive element.

Consider the subgroup H of Γ_w generated by $w(\pi)$. It is a convex subgroup isomorphic to $\mathbb{Z}$. Since F' is complete, it admits no immediate extensions of transcendence degree n. Therefore $H \neq \Gamma_w$. Let w' be the valuation obtained from w with value group Γ_w/H. By construction, w' is trivial on F' and has residue field F', since $w'(\pi) = 0$. Since w' is a coarsening of a p-henselian valuation, it is itself p-henselian. Hence w' is an F'-valuation with $s(G_F(p)) \subset D_{w'}$.

To show uniqueness, suppose w'' is another valuation such that $s(G_{F'}(p)) \subset D_{w''}$. Then as both are p-henselian with residue field not p-closed, they are comparable, by Proposition 2.2.3 applied to the class $\mathcal{C}_p$. If w' is a coarsening of w'', then the quotient valuation w''/w' is a p-henselian valuation on an algebraic extension of F' with residue field F', and hence must be trivial. That is, $w'' = w'$. The argument is identical if w'' is a coarsening of w'. □

Remark 4.2.2. By Remark 3.2.5, if $F = \mathbb{Q}_p(\zeta_p)$, then $F' = F$ in the statement of the above.

Corollary 4.2.3. *Assume Conjecture 1 holds, and suppose X is a smooth, projective variety over F, where F is a finite extension of $\mathbb{Q}_p$ containing ζ_p. Then there is a section of (4.2) if and only if $X(F) \neq \emptyset$.*

Proof. Note that the valuation w' of Proposition 4.2.1 defines an F'-rational place of $F(X)$, and hence gives rise to a point in $X(F')$. Indeed, we may always choose a generic point in $F(X)$ with positive value. Its image under the place gives a rational point $a \in X(F')$. Since the restriction map $G_K(p) \to G_F(p)$ is an isomorphism, F is relatively algebraically closed in K, and because X is defined over F, in fact $a \in X(F)$, as desired. □

Remark 4.2.4. Notice that in actuality we didn't need the smoothness of X in the above proof. Indeed, a section always gives rise to a valuation and hence a point. Conversely, every *smooth point* of X gives rise to a section. This slightly stronger version will be useful later.

Corollary 4.2.5. *Assume Conjecture 1 holds, and suppose X is a smooth, projective* curve *over F, where F is a finite extension of $\mathbb{Q}_p$ containing ζ_p. Then every section of (4.2) lies over a unique F-rational point $a \in X(F)$.*

Proof. This follows from the above corollary at once using Lemma 1.7 from [13]. Alternatively, it is a classical result that for curves, all K-valuations come from K-rational points. □

Theorem 3.4.14 therefore yields the following unconditional result:

Theorem 4.2.6. *Suppose X is a smooth, complete variety over $\mathbb{Q}_2$. Then any group-theoretic section of the exact sequence*

$$1 \to G_{\overline{\mathbb{Q}_2}(X)}(2) \to G_{\mathbb{Q}_2(X)}(2) \to G_{\mathbb{Q}_2}(2) \to 1$$

lies above a unique $\mathbb{Q}_2$-valuation v, which corresponds to a $\mathbb{Q}_2$-rational point if X is a curve. In both cases, the existence of a section implies that $X(\mathbb{Q}_2) \neq \emptyset$.

Using Corollary 3.4.15, we even obtain the same conclusion using just the maximal $\mathbb{Z}/2\mathbb{Z}$ elementary meta-abelian quotients.

4.3 The case $p > 2$

Theorem 4.3.1. *Let X be a smooth, projective variety of dimension n, where F is a finite extension of $\mathbb{Q}_p$, where $p > 2$ and F contains ζ_p and ζ_q. Then given any section s of*

$$1 \to G_{\overline{F}(X)}(p, q) \to G_{F(X)}(p, q) \to G_F(p, q) \to 1$$

there exists a unique F-valuation v of $F(X)$ such that s lies above v. In particular, the existence of a section implies the existence of a point. When X is a curve, the F-valuation is induced by a unique point $a \in X(F)$ and therefore the section lies over a.

Proof. The argument is the same as in Proposition 4.2.1, using Theorem 2.6.6. □

Remark 4.3.2. If we were to use the maximal solvable quotients, then we would not require the presence of any extra roots of unity.

As before, using Corollary 2.6.8, we obtain the same conclusion using just the maximal (p, q)-meta-abelian quotients.

4.4 Model-theoretic interpretation

Given a canonical class $\mathcal{C}$, let $B_c(F)$ denote the so-called weak birational section conjecture for varieties over F. That is, $B_c(F)$ holds if and only if for every projective variety X/F, if there is a section of the canonical exact sequence

$$1 \to G^c_{\overline{F}(X)} \to G^c_{F(X)} \to G^c_F \to 1$$

then there exists a point in $X(F)$.[1] The next proposition gives a model-theoretic interpretation of this statement.

Proposition 4.4.1. *For any field F, $B_c(F)$ holds if and only if for any field extension K/F with $G^c_K \simeq G^c_F$, and any existential sentence σ in the language of rings with parameters in F,*

$$K \models \sigma \iff F \models \sigma.$$

Proof. Suppose first that $B_c(F)$ holds, and let F be any field extension of K with $G^c_K \simeq G^c_F$. Then we have the following commutative diagram:

$$\begin{tikzcd}
G^c_{K(X)} \arrow[r] \arrow[d] & G^c_K \arrow[d, "\simeq"] \\
G^c_{F(X)} \arrow[r] & G^c_F
\end{tikzcd}$$

Any existential sentence in the language of rings with parameters in F is equivalent to a conjunction of statements each stating that a certain F-variety does or does not have a rational point. So it suffices to prove the statement when σ is the sentence stating that the F-variety X has a rational point. Clearly if it has a F-rational point, it also has a K-rational point. For the converse, suppose first that X has a singular K-rational point $a \in X(K)$; that is, $K \models \sigma$. Since the singular locus of X is defined over F, by the Jacobian criterion, we must have in fact $a \in X(F)$. If $X(K)$ admits

[1] Note that Stix gives in [35] an example of a normal variety which admits a rational, necessarily non-singular, point, which does not give rise to a section. That is, for varieties that are not smooth, rational points do not always give rise to sections.

a non-singular point, then (by Remark 4.2.4) this induces a section $s : G^c_K \to G^c_{K(X)}$ and hence, by the above diagram, a section $s : G^c_F \to G^c_{F(X)}$. Therefore, by $B_c(F)$, X admits an F-rational point, i.e., $F \models \sigma$.

For the other direction, let $s : G^c_F \to G^c_{F(X)}$ be a section of the canonical exact sequence. Then if K is the fixed field of the image of s inside $F(X)^c$, we have

$$G^c_K \simeq G^c_F.$$

Since $F(X) \subset K$, X admits a K-rational point, namely the generic one. But as this is an existential statement with parameters in F, it follows that X also admits an F-rational point, and so $B_c(F)$ holds. □

Therefore, using Theorem 3.5.1, we obtain a model-theoretic interpretation of the proofs of the statements in this chapter.

Chapter 5

Model theory of schemes

5.1 Motivation and General Discussion

The history of the interaction of model theory with classical algebraic geometry has been rich and fruitful. From the perspective of model theory, the study of algebraic geometry is interpreted as the study of $\text{Th}(ACF)$, the theory of algebraically closed fields in the ring language. By quantifier elimination, this amounts to thinking of algebraic varieties as sets whose points are zeros of certain polynomial equations, always working over an algebraically closed field. While this perspective is still extremely powerful and useful, it fails to interact meaningfully with the modern perspective on algebraic geometry brought about by the school of Grothendieck, namely the language of *schemes*. For this reason alone it seems desirable to examine the possible interactions of model theory with schemes. In particular though, the scheme-theoretic perspective has been particularly powerful in applications to number theory, and this is where we draw our main motivation.

The original proof of the birational section conjecture for a p-adic curve $X/\mathbb{Q}_p$ (see Chapter 4) proceeds as follows: given a section $s : G_{\mathbb{Q}_p} \to G_{\mathbb{Q}_p(X)}$, let K denote the fixed field of the image of s in $G_{\mathbb{Q}_p(X)}$. Then $G_K \simeq G_{\mathbb{Q}_p}$ and from this one deduces, via model theory of p-adically closed fields, that K is an elementary extension of $\mathbb{Q}_p$, which yields the desired result. If we were to try mimicking this argument in the setting of fundamental groups, we would obtain, from a section $s : G_{\mathbb{Q}_p} \to \pi_1^{et}(X)$, a pro-étale cover $Y \to X$ such that

$$\pi_1^{et}(Y) \simeq G_{\mathbb{Q}_p} \simeq \pi_1^{et}(Spec(\mathbb{Q}_p)).$$

It is tempting to ask if one can, from such an isomorphism, make sense of the idea that Y is an elementary extension of $Spec(\mathbb{Q}_p)$. Since both Y and $Spec(\mathbb{Q}_p)$ are only sensible geometric objects in the language of schemes, this would seem to require a model theory of schemes to answer fully.

Since $Spec(\mathbb{Q}_p)$ is, as a topological space, just a point, it is clear that to have a full picture one would need the model-theory to see both the topological space and the underlying structure sheaf, and their interaction. In this chapter we have made some first tentative steps towards treating general schemes as model-theoretic objects, taking our inspiration from the theory of Zariski geometries ([39], [38]). There, one considers a variety X defined over an algebraically closed field K, and forms a structure as follows: the underlying set is $X(K)$, and the n-ary relation symbols are all the irreducible closed subsets of $X(K)^n$ for every n. Together with the associated dimension function, this becomes the canonical example of what Zilber and Hrushovski call a Zariski structure. This approach works well when K is algebraically closed, because then the K-rational points of X are precisely the closed points, by the Nullstellensatz. Furthermore, the cartesian products X^n are all varieties over K as well. This is one reason why the classical model-theoretic approach to algebraic geometry has been so successful.

This fails dramatically when K is not algebraically closed. Indeed, given a scheme X, the cartesian product X^2 rarely carries the structure of a scheme in a natural way. One of the main lessons in scheme theory is to treat as fundamental, not single objects, but a morphism of objects. For a scheme $X \to S$ over the base S, one can form the fiber products $X \times_S X \to S$, and these are the correct 'powers' of X to consider.

With these considerations in mind, we believe that a more general, category theoretic approach to models will be needed. The main observation to make here is that a model in the classical sense, is essentially nothing more than a *functor* $\mathcal{M} : \mathcal{L} \to Set$, where $\mathcal{L}$ is a category formally constructed in a straightforward way from the choice of a language, and *Set* is the usual category of sets. Now it is a simple step to consider models valued in other categories, such as the category of schemes, and considerations of what a formula should be in such categories are quite straightforward. Using this, we mimic the classical approach to varieties, and examine the model-theoretic properties in this context.

The results of this approach are at present very incomplete, but we hope they may form the first steps towards a more complete theory.

Note: It did not seem sensible to attempt to include a brief introduction to the language of schemes in this thesis, especially as there are so many excellent texts available already. Any basic introduction to scheme-theoretic algebraic geometry will be sufficient to read this section, and we will assume the reader is familiar with the basic ideas and definitions. Anything used in this chapter can be found in the Stacks Project ([34]).

5.2 Basic categorial model theory

We begin by setting up the basic framework within which we will study schemes. While we could strictly speaking have just introduced this in an ad-hoc manner for schemes alone, we felt it would offer more clarity to set things up in more generality before specializing.

Remark 5.2.1. Note that this setup is not, on the face of it, the same as that of *categorical logic*, developed by Lawvere et. al., or the notion of *geometric theories* as developed by Johnstone et. al. It would however be interesting to explore the connections.

Definition 5.2.2. A 'first-order language' $\mathcal{L}$ consists of the following data:

- A category $\mathcal{C}$ with finite limits;
- A final object $*$;

- A distinguished arrow $\star \to *$ where $\star$ is some fixed object;
- A distinguished class C of arrows with source $\star$;
- A distinguished class of arrows R.

We may sometimes write $\mathcal{L}(\mathcal{C})$ to denote the category of the language in question.

The point is that the elements in a member X of the category are to be interpreted as the elements in the *set* $Hom_*(\star, X)$, the morphisms $\star \to X$ which respect the structure map to the final object $*$. In other words, we are looking at morphisms $X \to *$ and considering its '$\star$-points' as the points under consideration. The class C is to be thought of as constants, and R as the relation and function-symbols.

The next example will show how, given a classical first-order language, one can obtain a category as above.

Example 5.2.3. Consider a classical, multisorted first-order language $\mathcal{L}$. Build the category $\mathcal{C}_{\mathcal{L}}$ in steps as follows.

- Add an object $*$ and let $\star = *$.
- For each sort in $\mathcal{L}$, add a corresponding object X.
- For each X, add objects $X^{\otimes n}$ for each n, defined formally as an object which satisfies the universal property of the n-fold fiber product over $*$.
- Similarly add fiber products of any two objects in the category.
- Add arrows for all the function symbols based on the specified domain and range of the symbol.
- For each relation symbol, add an object U and arrow from U to $X^{\otimes n}$ for the object X corresponding to the symbol; these objects will form the class R above.
- Finally, for each constant symbol of a given sort X, add an arrow $* \to X$; these correspond to the class C above.

It is clear the category formed in this way is equivalent to the language, and that similarly any language as defined above can be converted to a many-sorted classical language, giving an equivalence between the two notions. We will from now on pass freely between the two.

A $\mathcal{L}$-structure is simply a coherent way to give concrete meaning to the abstract language.

Definition 5.2.4. An $\mathcal{L}$-structure is a covariant (resp. contravariant) functor $\mathcal{F} : \mathcal{L} \to \mathcal{C}$ where $\mathcal{C}$ is any category with a final object and with finite limits (resp. colimits). If $\mathcal{F}(*) = S$, $\mathcal{F}(\star) = T$, then we call the set $Hom_S(T, X)$ the *elements of* X, or the T-points of $X \to S$, abbreviated $X(T)$.

Classical model theory is thus concerned with particular (covariant) structures where $\mathcal{C} = Set$ and $\star = *$. Indeed, there $* = \star$ may be taken to be any point-set, whence fiber products become the usual cartesian products. If one specifies that the arrows corresponding to relation symbols be monic, then such arrows can be identified with subsets of various direct products. The elements $Hom_*(*, X)$, for a sort X, are naturally identified with the actual elements of the *set* X.

Notice that relation symbols are not required in general to be monic. That is, relations are not necessarily subsets of the structure. This essentially amounts to embedding the many-sorted setting into structures from the outset. A classical relation-symbol picks out a subset, and one could alternatively simply add another sort corresponding to that subset, with the function symbol connecting this new sort to the 'main' sort given by the inclusion. In this way one simply considers any morphism as a relation-symbol.

In general, we consider multi-categorial structures, i.e. collections of functors $\mathcal{F}_i : \mathcal{L}_i \to \mathcal{C}_i$ over some indexing set I, along with natural transformations $\mathcal{G}_{ij} : \mathcal{C}_i \to \mathcal{C}_j$. Call such a collection a *multifunctor*.

We now define formulas in this context.

Definition 5.2.5. Let a language $\mathcal{L}$ be given. Formulas are defined recursively in the usual manner:

- Any constant symbols c_i and variable symbols x_i, attached to the sorts indexed by $i \in I$, are terms. If t is a term and f is a function symbol, $f(t)$ is a term, where this is to be understood as an abbreviation of $f \circ t$, provided the term and symbol are compatible in terms of their associated sorts.

- Atomic formulas consist of formulas of the form $t_1 = t_2$ and $U(t_1, \ldots, t_n)$ where the t_i are terms, U is a relation symbol compatible with the sorts of the terms.

- Close the class of formulas under the usual logical operations, noting that quantification ranges over elements as defined in the special sense of this note.

Definition 5.2.6. Given languages $\mathcal{L}_i$, a theory T is a collection of sentences T_i. A model of T is a multifunctor $\langle \mathcal{M}_i : \mathcal{L}_i \to \mathcal{C}_i \rangle$ such that the sentences of T_i hold in $\mathcal{C}_i$ and such that truth is preserved via the connecting natural transformations. Notice that the choice of the $\mathcal{C}_i$'s form part of the defining data.

A morphism of $(\mathcal{L}_i)$-structures is a collection of natural transformations commuting with the connection transformations.

A morphism of $(\mathcal{L}_i)$-structures $(\mathcal{F}_i) \to (\mathcal{G}_i)$ is *elementary* if each $\mathcal{F}_i(\mathcal{L}_i) \to \mathcal{G}_i(\mathcal{L}_i)$ is elementary in the usual sense.

5.3 Affine scheme structures

We specialize the above to the study of the first-order structure of an *affine* scheme[1]. Our schemes/morphisms will always be assumed to be **separated**.

Notation: Given a morphism $X \to S$, let $X^{\otimes n}$ denote the n-fold fiber product of X over S.

[1] It is in fact clear how to define a general scheme structure, but it is not at this point clear that compactness is valid for such structures; checking this requires one to check that gluing data is definable on the ring level.

Definition 5.3.1. Let $\mathcal{L}_{sch}$ be the category with one sort corresponding to X, some number of relation arrows to $X^{\otimes n}$ for each n, and no non-trivial function or constant arrows. Let $\mathcal{L}_{alg}$ be the two-sorted language for algebras over a ring. That is, we have two sorts, both with the usual ring-language, and a homomorphism connecting the two. Given a choice of base-scheme $S = Spec(A)$ and a morphism $T \to S$, we define an *affine scheme structure* to be a structure

$$\begin{tikzcd}
\mathcal{L}_{sch} \arrow[d, "\mathcal{F}_1"'] & \mathcal{L}_{alg} \arrow[d, "\mathcal{F}_2"] \\
\text{AffSch} \arrow[r, bend left, "\Gamma"] & \text{Alg} \arrow[l, bend left, "Spec"]
\end{tikzcd}$$

Here, $\mathcal{F}_1$ takes the arrow $X \to *$ to a morphism *of schemes* $Spec(B) \to Spec(A)$, and $\mathcal{F}_1(\star) = T$. The relation symbols of $\mathcal{L}_{sch}$ are to be interpreted as the open subschemes[2] of $X := Spec(B)$. Similarly, $\mathcal{F}_2$ produces a ring-homomorphism $A \to B$ which induces the structure of an A-algebra on B. We let $\mathcal{F}_2(*) = \mathcal{F}_2(\star)$ be the trivial ring (so elements are taken to be actual elements of the rings). Note that here *Spec* is the functor taking an algebra A to the affine scheme A, and Γ is the global sections functor taking an affine scheme $Spec(A)$ to the ring of global sections A.

So in our definition, the underlying set of the structure is just $X(T) = Hom_S(T, X)$. Note that for a given choice of T, this set might be finite, or even empty! In these cases, most of the results that follow will be trivial.

Remark 5.3.2. If we add in a constant symbol and some non-trivial function symbols, we can axiomatize e.g. group schemes over some base scheme S as scheme structures satisfying some extra axioms given by various commutative diagrams.

Remark 5.3.3. By Yonedas Lemma, knowing $X(T)$ for every $T \to S$ is equivalent to knowing $X \to S$, which is equivalent again to knowing $A \to B$. Therefore it is not entirely unreasonable to suggest that the first-order theory of $X \to S$ is the same as the first-order theory of all the $X(T)$'s combined.

[2] Note that all the open subsets of the scheme carry a canonical scheme structure.

A simple observation now is a characterization of the quantifier-free definable sets.

Proposition 5.3.4. *The quantifier-free definable subsets of $\mathcal{F}_1(\mathcal{L}_{sch})$ are exactly the T-points of constructible subsets of the scheme.*

Proof. (Sketch) Recall that the constructible subsets of a scheme coincide exactly with finite, disjoint unions of locally closed subsets, where a locally closed subset is the intersection of an open and closed subset. It is clear that these are all defined by formulas in the language, and conversely that any formula defined using only the predicate symbols as basic atomics defines such a subset. Since the morphism is separated[3], the diagonal embedding defined by a formula $x = y$ will have a closed image, and its negation will thus be open. In more detail, there is a commutative diagram

$$\begin{tikzcd}
Hom_S(T, X \times_S X) \arrow[r, "\sim"] & Hom_S(T, X) \times Hom_S(T, X) \\
& Hom_S(T, X) \arrow[u, "diag"'] \arrow[ul, "d^*"]
\end{tikzcd}$$

where *diag* is the diagonal embedding, and d^* is the map induced by the diagonal embedding of schemes $X \to X \times_S X$. Hence if we add these formulas in as atomics as well, the subsets generated will still be constructible. □

At this point we may begin to suppress the mentioning of the language, and informally just refer to a morphism of affine schemes as an affine scheme structure. In other words, an affine scheme structure simply *is* a morphism of schemes together with the particular choice of language specified above.

5.4 Chevalleys Theorem and Quantifier Elimination

We now restrict further.

[3] Recall we always assume our morphisms to be separated.

Definition 5.4.1. An *affine K-scheme structure* is an affine scheme structure $Spec(B) \to Spec(A)$ where the morphism is separated and of finite type, with B Noetherian. In addition, we will assume that $T = Spec(K)$ where K is a field.

The significance of letting T be the spectrum of a field is that a morphism $T \to X$ actually gives us a point in X. This will greatly simplify the exposition of the following results, which we believe will still be true in more general settings.

Quantifier elimination for algebraically closed fields can be thought of as a consequence of (and is in fact equivalent to) a restricted form of Chevalley's Theorem, which in full generality says the following:

Theorem 5.4.2 (Chevalley's Theorem)**.** *Let $Y \to X$ be a morphism of finite type between Noetherian schemes. Then the image of any constructible subset of Y is constructible.*

We now wish to show that Chevalleys Theorem can be interpreted as a certain form of quantifier elimination for schemes. This needs some clarification in order to be a precise statement.

Definition 5.4.3. Let $X \to S$ be a morphism of affine schemes. We say X admits **elimination of quantifiers** if, for every $T \to S$, and every formula ϕ in the scheme-language, there is a quantifier-free formula ψ such that

$$X(T) \models \phi \iff X(T) \models \psi.$$

Morally, this is akin to thinking of X as being a syntactic object, with $X(T)$ its semantic models. Therefore Yonedas lemma could be interpreted as the equivalence between syntax and semantics in this context.

Proposition 5.4.4. *If $X \to S$ is an affine K-scheme structure, then X admits elimination of quantifiers, provided we adjoin a constant $c : Spec(K) \to X$ to the language which is to be interpreted in the structure as a* closed *point.*

Proof. First notice that the only new atomic formula added is $x = c$. As c is closed, the subset defined by this formula is constructible, and hence we still have that the quantifier-free formulas are all constructible.

We will now show that any formula of the form $\exists x \phi$, where ϕ is a quantifier-free formula in one or two variables, is equivalent to a quantifier-free formula. By general model-theory, quantifier elimination in full generality will follow.

Assume first that $\phi = \phi(x, y)$ is a quantifier-free formula in two variables. Therefore ϕ defines a constructible subset C of $X \times_S X$. Now observe that we have a commutative diagram

$$\begin{tikzcd}
Hom(S, X \times_S X) \arrow[r, "\sim"] \arrow[dr, "f^*"'] & Hom(S, X) \times Hom(S, X) \arrow[d, "pr"] \\
& Hom(S, X)
\end{tikzcd}$$

where f^* is induced by the canonical morphism $f : X \times_S X \to X$, and pr is the projection onto one of the coordinates. Now since $X \to S$ is finite, so is $f : X \times_S X \to X$, and both are again Noetherian. By Chevalley's Theorem, the image under this map of a constructible subset is constructible. In particular, $f(C)$ is a constructible subset of X. Now

$$\{y : \exists x \phi(x, y)\} = \{y : \exists x C(x, y)\} = \{y : y \in f(C)\}$$

since the fiber $f^{-1}(y)$ is non-empty precisely when y is in $f(C)$. Therefore $\exists x \phi(x, y)$ is equivalent to the quantifier-free formula $f(C)(y)$.

The only remaining case we need to consider are formulas of the form $\exists x \phi(x)$, where $\phi(x)$ has just one free variable. The only possibilities for atomic ϕ are $U(x)$ for some open set U and $x = c$. In either case the formula $\exists x \phi(x)$ is trivially true and thus equivalent to the quantifier-free formula $c = c$. $\square$

It is important to observe that this statement does *not* say that the image of a constructible subset of $X(T) \times X(T)$ is a constructible subset of $X(T)$, which is not true in general. Rather, the image of a constructible subset lands inside the T-points of a constructible subset of X itself.

Note: From now on we will always assume we have a constant symbol in our scheme language.

Question: Does the converse to the above statement hold? In other words, is the most general form of Chevalleys Theorem equivalent to quantifier-elimination for affine K-scheme structures?

5.5 A Compactness Theorem

The following result shows that affine K-scheme structures satisfy an analogue of the usual Compactness Theorem.

Theorem 5.5.1 (Compactness for Affine K-Scheme Structures)**.** *Suppose Γ is a theory for affine scheme structures which is finitely satisfiable, in the sense that given any finite subset Γ' of $T(\mathcal{L}_{sch})$ and $T(\mathcal{L}_{alg})$, there is an affine scheme structure modelling Γ'. Then Γ itself is satisfiable by an affine scheme structure.* [4]

Proof. Expand the language $\mathcal{L}_{alg}$ to include a predicate for all the prime ideals of B valued over k, and a constant symbol for every element of the ring. We first show that for any sentence $\phi \in Sent(\mathcal{L}_{sch})$, there is a $S_\phi \subset Sent(\mathcal{L}_{alg})$ such that

$$\mathcal{F}_1(\mathcal{L}_{sch}) \models \phi \iff \mathcal{F}_2(\mathcal{L}_{alg}) \models S_\phi.$$

By quantifier-elimination, we only need to consider quantifier-free sentences. The only atomic quantifier-free sentences are those of the form $U(c)$ for some open subset U. Now the open subsets of the form $D(f) = \{\mathfrak{p} \in Spec(A) : f \notin \mathfrak{p}\}$ where $f \in A$, form a basis for the topology. So we can find a collection $f_i^U \in A$ such that $U(c) \iff D(f_i^U)(c)$ for some i. Therefore it suffices to assume that $U = D(f)$ for some f and show that $U(x)$ is equivalent to a formula on the ring-side. But clearly

$$U(x) \iff \neg(f \in \mathfrak{p})$$

[4] Note that the claim the model of Γ is an actual affine scheme is the crucial point. One could always look at the underlying sets involved and apply the usual compactness theorem to get a new *set* satisfying Γ, but there's no way of knowing that this set is still an affine scheme.

and the right-hand side is defined by a formula in the extended language.

So without loss of generality, Γ only contains sentences in the ring-sort. Now if we adjoin to Γ the usual axioms for a ring, any finite subset Γ' containing these will still be satisfied by a ring[5]. The forgetful functor *Ring* → *Set* now transports any such Γ' to a set of formulas which is still satisfiable. Applying the classical Compactness Theorem for the category *Set*, we deduce that there is a set $\tilde{A}$ which satisfies Γ, and hence, in particular, is a commutative ring. Since we adjoined constant symbols for the elements of A, there is a natural embedding $A \to \tilde{A}$ inducing a morphism $Spec(\tilde{A}) \to Spec(A)$ of schemes. Clearly then the affine scheme structure $Spec(\tilde{A})$ is a model of Γ by construction. □

Remark 5.5.2. It is clear that any category which admits an axiomatization in the category of sets will admit a compactness theorem by the above procedure, and similarly any category equivalent to such a category will work. Since the category of affine schemes is equivalent to the category of rings, and rings are axiomatizable in *Set*, the above result can be seen as just a special case of this principle.

Definition 5.5.3. One can define types in the usual way.

Corollary 5.5.4. *Let M be an affine scheme structure, p an n-type. Then there is an elementary extension M' of M which realizes p.*

Proof. Apply the compactness theorem for affine scheme structures to the set of formulas in p along with the full elementary diagram of M. □

Hence affine scheme structures behave nicely from a model theoretic perspective, despite the fact that they cannot be axiomatized in the category of sets in a satisfactory manner.

[5] Note that we did not need to include these axioms to begin with because the models were a priori assumed to exist in the category of rings, where these axioms necessarily hold.

5.6 Comparison with classical model theory

Consider the case where $S = T = Spec(K)$, where K is algebraically closed and of characteristic 0. We want to compare the logical structure of affine scheme structures and the classical model theoretic approach to algebraic geometry as the study of ACF_0. The following shows that the model theory of geometric closed points is essentially the same

Proposition 5.6.1. *Let $X \to Spec(K)$ be an affine, irreducible variety over K, an algebraically closed field of characteristic 0. There are maps*

$$\Psi : Form(\mathcal{L}_{sch}) \to Form(\mathcal{L}_{acf_0})$$

$$\Phi : Form(\mathcal{L}_{acf_0}) \to Form(\mathcal{L}_{alg})$$

such that for any $\phi \in Form(\mathcal{L}_{sch})$ and any closed point $x \in X(K)$, there is a $\bar{x} \in K^n$ for some n such that

$$X \models \phi(x) \iff K \models \Psi(\phi(\bar{x}))$$

and similarly for Φ. Furthermore, these maps are compatible with respect to the transfer map from $\mathcal{L}_{sch}$ to $\mathcal{L}_{alg}$ indicated in the proof of compactness.

Proof. The map Φ is induced by the natural map $K \to A$ coming from the structure map. To define Ψ, it suffices to determine where the formula $V(x)$ goes, where $V = V(I)$ is a standard closed set, and x is a closed, geometric point. Note firstly that X itself is defined by some polynomial equations with coefficients in k: by taking disjunctions, we can thus reduce to the case where X is affine k-space. By Noetherianity, there are $f_1, \ldots, f_n \in A$ such that $I = (f_1, \ldots, f_n)$. Let Ψ map the formula $V(x)$ to the formula $(f_1(x) = 0) \wedge \ldots \wedge (f_n(x) = 0)$. Using the Nullstellensatz, it is not hard to see that these maps satisfy the desired claims. □

Thus the benefit of the more general model theory of schemes is much the same as the benefit of scheme-theoretic algebraic geometry; you can work with non-closed points, and work over coefficients rings that are not algebraically closed (or even fields at all).

5.7 Zariski Geometries

One way of understanding the notion of a Zariski geometry is that it is a way of developing algebraic geometry for sets simply assumed to possess a topology and a good notion of a dimension. With this interpretation in mind, one can just as easily work with the notion of Zariski geometries in the category of schemes, as a means of developing scheme theoretic algebraic geometry based simply on the Zariski topology on a scheme $X \to S$ (and its fiber products $X^{\otimes n}$ for all n) along with a notion of dimension.

Definition 5.7.1. Let X be a scheme of finite type over a field k, and L a field extension of k. Define the closed subsets of $X(L)$ to be the subsets of the form $U(L)$ for U a closed subscheme of X. Then define for such a U, the dimension $dim(U(L)) := dim(U)$, where the latter is the usual Krull dimension.

A morphism $Spec(L) \to U$ is specified precisely by the data of a point $x \in U$ and a morphism $\kappa(x) \to L$ of fields. Since the residue field can be computed from any affine neighbourhood of x, it is easy to now see that $U(L) \cap V(L) = (U \cap V)(L), U(L) \cup V(L) = (U \cup V)(L)$ and $U(L) \setminus V(L) = (U \setminus V)(L)$. Therefore this gives the L-points of X the structure of a topological space. Since any constructible subset $Q \subset X$ has the form $\cup(S_i \setminus P_i)$ where S_i, P_i are closed and $P_i \subset S_i$ with S_i irreducible, we have $\bar{Q} = \cup S_i$. Consequently, we can extend the dimension to constructible subsets by putting $dim(Q) := max(dim\, S_i)$.

One defines the topology and dimension identically for each $X^{\otimes n}$.

We now state the modified dimension axioms of a Zariski structure in the category of schemes.

Definition 5.7.2. Let $X \to S$ be any morphism of schemes, and let dim be a map from closed subsets of X to $\mathbb{N}^{\geq}$. Then we say that dim makes X into a *Zariski scheme* if the following properties hold:

(DP) The dimension of a point is 0

(DU) $dim(S_1 \cup S_2) = max\{dimS_1, dimS_2\}$

(SI) For any irreducible $S \subset X^{\otimes n}$ and a closed subset $S_1 \subset S$, if $S_1 \neq S$, then $dimS_1 < dimS$.

(AF) For any closed irreducible subscheme $S \subseteq X^{\otimes n}$ and a projection map $p : X^{\otimes n} \to X^{\otimes m}$, we have

$$dim\, S \leq dim\, p(S) + dim\,(S_x) \tag{5.1}$$

for every closed point $x \in p(S)$, where the fiber is with respect to p.

(FC) For any closed irreducible subscheme $S \subseteq X^{\otimes n}$ and a projection $P : X^{\otimes n} \to X^{\otimes m}$, there exists V open in $p(S)$ such that

$$min_x\, dim(S_x) = dim(S_z) \tag{5.2}$$

for any $z \in V$, where the minimum runs over closed points $x \in p(S)$.

As in the classical case, we have the following basic example of Zariski schemes.

Proposition 5.7.3. *If $X \to Spec(k)$ is a reduced, quasicompact, Noetherian scheme of finite type over $Spec(k)$, then the Krull dimension of X satisfies the axioms listed.*

Proof. The first three axioms are easy. Let's consider first the (AF) axiom. Clearly it will suffice to assume in all cases that the projection map is $p : X^{\otimes 2} \to X$. The general case will follow analogously.

Firstly, note that since the structure morphism $X \to Spec(k)$ is universally open ([34, Tag 06DN]), the morphism p is *open*. As the property of being finite type is preserved by base change, it is also of finite type.

Secondly, note that since $X \to Spec(k)$ is reduced and of finite type, so is $X^{\otimes n}$. If $S \subset X^{\otimes 2}$ is irreducible, then it is in particular integral. The image of an irreducible set under a continuous map is irreducible, so $p(S)$ is also integral. Consider the restriction $p : S \to p(S)$ and compose it with the closed immersion $p(S) \to \overline{p(S)}$, where the image and closure of the image are endowed with their canonical scheme structure. We are left with a morphism $S \to \overline{p(S)}$; both of these schemes are closed subsets in their ambient space, hence of finite type over $Spec(k)$ (closed immersions are of finite type). Let $y \in S$ be any closed point [6], and let $x = f(y)$. Then we have

$$dim\, \mathcal{O}_{S,y} \leq dim\, \mathcal{O}_{p(S),x} + dim_x S_x \tag{5.3}$$

and by [34, Tag 02JT], $dim\, \mathcal{O}_{S,y} = dim(S)$. Let x' be any specialization of x which is closed (which exists by quasicompactness). Then it's easy to check that $dim\, \mathcal{O}_{p(S),x} \leq dim\, \mathcal{O}_{p(S),x'}$, and the latter equals $dim(p(S))$ as x' is closed. Putting this together we get

$$dim(S) \leq dim(p(S)) + dim\, S_x \tag{5.4}$$

for any closed point $x \in p(S)$. [7]

Next we consider the (FC) axiom. By [34, Tag 02FW] and the above facts, we find that

$$U := \{s \in S : dim\, S_{f(s)} \leq \min_{a \in p(S)} dim\, S_a\}$$

is open in S. Hence $p(U)$ is open in $p(S)$ and satisfies the (FC) condition. □

This allows us to obtain another proof of quantifier elimination in this more restricted setting.

Corollary 5.7.4. *Let X be as above. Then X admits elimination of quantifiers.*

Proof. The argument is formally the same as Theorem 3.2.1 in [38]. □

Question: Is it true that if $X \to S$ is any morphism of schemes for which the Krull dimension satisfies the Zariski structure axioms, is S necessarily the spectrum of a field and $X \to S$ is of finite type?

[6] Which exists since S is of finite type over a field.

[7] Indeed, for the 'converse', note that if $x \in p(S)$ is closed, if we take any y lying over x, any point in its closure still lies over x; picking a closed such y we get the same inequality as before.

Chapter 6

Appendix

We detail the missing calculations from Chapter 3.

6.1 Appendix A: Case A

Let us begin by proving Lemma 3.4.3. We want to show that for $x \in \mathcal{O}_1$, $1 + 2x$ and $1 + 4x$ are in $N(5)$.

Remark 6.1.1. Let us emphasize that in the calculations below, the *order* in which calculations are done is crucial.

Proof. We proceed by cases, based on the square classes of x and $1 + x$. We write $x \sim y$ to denote that x and y have the same square class, i.e., x/y is a square in K. Throughout we use freely Proposition 3.3.11 to determine intersections of various norm groups.

Note also that $x \in \mathcal{O}_1$ implies $x \sim \pm 2, \pm 10$. If $x \sim 2$, then $1+x \in N(5) \cap N(-2) = \{1, -5\}$, and similarly when $x \sim -2$ or ± 10. Therefore the cases considered below are indeed exhaustive.

- $\boxed{x \sim 2, 1 + x \sim 1}$ Note that $1+2x = (1+x)+x \in N(-1) \cap N(-2) = \{1, 2\}$. Also we have $1+5x = (1+x)+4x \in N(-10) \cap N(-2) = \{1, -5\}$. If $1+5x \sim -5$, with say $1+5x = -5a^2$, then one finds $1+2x = (1+5x)-3x \in -5N(2) = \{\pm 5, \pm 10\}$, contradiction.

Hence $1+5x \sim 1$ whence $1+2x = (1+5x) - 3x \in N(-10)$, so $1+2x \sim 1$. Now $1+4x = (1+x)+3x \in N(-2) \cap N(-10) = \{1, -5\} \subset N(5)$.

- $\boxed{x \sim 2, 1+x \sim -5}$ Then $1+2x \in N(-1)$, and, equalling $(1+x)+x$ can be written in the form $-5a^2+2b^2$ for some a and b, or equivalently $-5(A^2-10B^2)$ for some A, B. This expression is visibly in $-5N(10)$, and so $1+2x \in N(-1) \cap -5N(10) = \{2, 5\}$. Suppose for a contradiction that $1+2x \sim 2$. Then $1+3x = (1+x)+2x = (1+2x)+x \in N(10) \cap N(5) \cap N(-1) = \{1\}$, so $1+3x \sim 1$. Therefore $1+5x = (1+x)+4x = (1+3x)+2x \in N(-10) \cap 2N(10) \cap N(-1) = \varnothing$: contradiction. Hence $1+2x \sim 5$, and also $1+5x = (1+x)+4x = (1+2x)+3x \in N(-10) \cap 2N(10) \cap 5N(2) = \{-5\}$, so $1+5x \sim -5$.

  From this we get $1+4x = (1+2x)+2x = (1+5x)-x \in N(-2) \cap N(-5) \cap N(-10) = \{1\}$, so $1+4x \sim 1$.

- $\boxed{x \sim -2, 1+x \sim 1}$ We have $1-4x = (1+x)-5x \in N(-2) \cap N(-10) = \{1, -5\}$. Also $1-x = (1+x)-2x \in N(-2) \cap N(-1) = \{1, 2\}$. If $1-x \sim 2$ then we get $1-4x = (1-x)-3x \in 2N(5)$, giving a contradiction. So $1-x \sim 1$. Hence $1+4x = (1-x)+5x = (1+x)+3x \in N(2) \cap N(10) \cap N(-10) = \{1\}$.

  Next, $1+2x = (1+4x)-2x = (1+x)+x = (1-x)+3x \in N(-1) \cap N(2) \cap N(-10) = \{1\}$.

- $\boxed{x \sim -2, 1+x \sim -1}$ Then $1+4x = (1+x)+3x \in N(2) \cap N(10) = \{1, -1\}$.

  Now, $1-5x = (1+x)-6x \in N(-10) \cap -N(-5) = \{-5, 10\}$. If $1+4x \sim -1$, then also $1-5x = (1+4x)-9x \in N(2)$ as well, giving a contradiction as neither -5 or 10 are in $N(2)$. Thus $1+4x \sim 1$, whence $1+5x = (1+x)+4x = (1+4x)+x \in N(10) \cap -N(-2) \cap N(2) = \{-1\}$.

  From this we get that $1+2x = (1+x)+x = (1+4x)-2x = (1+5x)-3x \in -N(-2) \cap N(-1) \cap -N(-10) = \{5\}$.

- $\boxed{x \sim 10, 1+x \sim 1}$ First note $1-2x \in N(5) \cap N(-2) = \{1, -5\}$. Also, $1-x \in N(10) \cap N(5) = \{1, -1\}$. If $1-x \sim -1$, then $1-2x = (1-x)-x \in -N(-10)$, a contradiction. Therefore $1-x \sim 1$.

Now, $1 + 2x \in N(-5) \cap N(-10) = \{1, -2\}$. Suppose $1 + 2x \sim -2$. Then $1+3x = (1+x)+2x = (1+2x)+x \in N(2) \cap N(-5) \cap 2N(5)$ giving $1+3x \sim 2$. Then $1 + 4x \in N(-10) \cap N(2) \cap 2N(5)$ giving $1 + 4x \sim -2$. Finally, this gives $1 - x = (1 + 4x) - 5x \in -N(-1)$, a contradiction.

Hence $1 + 2x \sim 1$. The above also shows $1 + 4x$ is not equivalent to -2. But $1 + 4x \in N(-10) \cap N(2)$, so $1 + 4x \sim 1$.

- $\boxed{x \sim 10, 1 + x \sim -5}$ We have $1 + 2x \in N(-5) \cap 5N(2) = \{5, -10\}$. Assume, for a contradiction, that $1 + 2x \sim -10$.

  Then $1 - x = (1 + 2x) - 3x = (1 + x) - 2x \in 2N(5) \cap N(10) \cap -N(-1) = \{-10\}$. Now, $1 + 4x = (1 + 2x) + 2x \in 5N(2) \cap N(-10) = \{-5, 10\}$. Next, $1 - 4x = (1 + x) - 5x = (1 - x) - 3x \in N(10) \cap -5N(-10) \cap 2N(5) = \{10\}$. Thus $1+4x = (1-4x)+8x \in 5N(-2)$, whence $1+4x \sim 10$. This in turn forces $1+5x = (1+4x)+x \sim N(-1)$. But also $1+5x = (1+x)+4x \in N(-2)\cap 5N(2)$, which has empty intersection with $N(-1)$. So we get our required contradiction.

  Therefore $1 + 2x \sim 5$. We also showed above that $1 + 4x \sim -5$ or 1, so we're again done in this case.

- $\boxed{x \sim -10, 1 + x \sim 1}$: It is immediate that $1 + 2x \in N(5) \cap N(10) = \{1, -1\}$. Next, observe that $1 + 4x \in N(10) \cap N(-2) = \{1, -10\}$. But if $1 + 4x \sim -10$, we find $1 + 2x = (1 + 4x) - 2x \in 5N(2)$, a contradiction to the above. Hence $1 + 4x \sim 1$ and we are done.

- $\boxed{x \sim -10, 1 + x \sim -1}$ We have $1+2x \in N(5)$ at once, and $1+4x = (1+x)+3x \in N(2) \cap N(10) = \{1, -1\}$.

This completes the proof. □

Corollary 3.4.4 then shows that $\mathcal{O}_1$ is closed under multiplication by $\pm 1, \pm 5$ and $\pm 5^{-1}$. For the proof of the crucial Proposition 3.4.5, we will want to use more detailed knowledge of how multiplication of these numbers permutes the elements in $\mathcal{O}_1$. More specifically, given $x \in \mathcal{O}_1$, where we know the square class of x and $1 + x$, we want to know the square class of ax and $1+ax$, for $a \in \{\pm 1, \pm 5, \pm 5^{-1}\}$. We proceed in a similar manner as the proof of Lemma 4.4: the idea is essentially to express $1+ax$ as a norm in two or three different ways. For example, if $x \sim 2, 1+x \sim 1$, then $1-5x = (1+x) - 6x \in N(10) \cap N(-5) \cap N(5) = \{1\}$, so $1-5x$ is a square.

The other calculations are entirely similar and are left to the reader. We note also that the proof of Lemma 3.4.3 dealt already with a few cases. The results are summarized in Table 1 below.

Table 6.1: Stability of $\mathcal{O}_1$ under $N(5)$

x	$1+x$	$1-x$	$1+5x$	$1-5x$	$1+5^{-1}x$	$1-5^{-1}x$
2	1	1,-1	1	1	1	1
2	-5	-1	-5	±1	-1,5	±1
-2	1	1	±1	1,-5	1	-1, 5
-2	-1	1, -5	-1	1,-5	±5	-5
10	1	±1	1,-5	1	1	1
10	-5	-1	-5	±1	1,-5	1
-10	1	1,-5	±1	1	1	1,-5
-10	-1	1,-5	±1	1, -5	±1	-5

Note that given the explicit information provided by the proof of Lemma 3.4.3, it is possible to make every entry unique in this table, and indeed even to pin down the exact value of $1+ax$ for $a \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 5^{-1}, \pm 3^{-1}\}$. However, this will not be necessary to complete the remaining proofs; the table above will suffice.

Finally, we include all the remaining calculations of Proposition 3.4.5. That is, we systematically show that for all possible combinations of the square classes of $x, 1+x, y, 1+y$ with $x, y \in \mathcal{O}_1$, $1-xy \in N(5)$. Clearly if $x \sim 2, y \sim 10$ or $x \sim -2, y \sim -10$ then $1-xy \in N(5)$ is automatic. Next observe that any $x \in \mathcal{O}_1$ is of the form $2ab^2$ where $a \in \{\pm 1, \pm c\}$. Since for any such a and any other $y \in \mathcal{O}_1$, $ay \in \mathcal{O}_1$, we can without loss of generality always assume that $x \sim 2$. We also freely exploit symmetry in x and y to reduce the number of cases to those done below.

Let us recall that we have the decomposition

$$1-xy=(1+ay)\left(1+(1+ax)\frac{-ay}{1+ay}\right) \tag{6.1}$$

for $a=\pm1,\pm5$. We will refer to the decomposition with respect to a as the a-decomposition. So the -1-decomposition means

$$1-xy=(1-y)\left(1+(1-x)\frac{y}{1-y}\right)$$

We will use this freely in what follows. The calculations involved are trivial; the difficulty is in identifying which calculations will actually give the desired result. Therefore in the below, rather than include all the details of the arithmetic, we simply indicate how to proceed. Note we will also use without comment the result of Table 1 above.

Proof. (Proposition 3.4.5) By the above discussion, we only need to check the following cases:

- $\boxed{x\sim 2, 1+x\sim 1, y\sim 10, 1+y\sim 1}$ Immediate.

- $\boxed{x\sim 2, 1+x\sim 1, y\sim 10, 1+y\sim -5}$ Immediate.

- $\boxed{x\sim 2, 1+x\sim 1, y\sim -10, 1+y\sim 1}$ We immediately get $1-xy\in N(-5)$, and the $+1$-decomposition gives also $1-xy\in N(-10)$, so $1-xy\in\{1,-2\}$. Now $1+5^{-1}y\sim 1$. Also, $1+5x\sim 1$ or -5. But since $1-5x\sim 1$, we get $1+5x=(1-5x)+10x\in N(-5)$, so in fact $1+5x\sim 1$. Therefore the $+5$-decomposition gives $1-xy\in N(10)$, forcing $1-xy\sim 1$.

- $\boxed{x\sim 2, 1+x\sim 1, y\sim -10, 1+y\sim -1}$ We immediately get $1-xy\in N(-5)$, and the $+1$-decomposition also gives $1-xy\in N(-2)$. So $1-xy\in\{1,-10\}$. Also, $1-5^{-1}y\sim -5$ and $1-5x\sim 1$, whence the -5-decomposition gives $1-xy\in N(2)$, forcing $1-xy\sim 1$.

- $\boxed{x\sim 2, 1+x\sim -5, y\sim 10, 1+y\sim 1}$ Immediate.

- $\boxed{x\sim 2, 1+x\sim -5, y\sim 10, 1+y\sim -5}$ Immediate.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim -10, 1+y \sim 1}$ We immediately get $1-xy \in N(-5)$, and the $+1$-decomposition gives $1-xy \in N(2)$. We also see $1-5y \sim 1$. Since $1-x \sim -1$, we find $5-x \in -N(-1)$, and since $1-5^{-1}x \sim \pm 1$, we get $1-5^{-1}x \sim -1$. Using the -5-decomposition now gives $1-xy \in N(-2)$, forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim -10, 1+y \sim -1}$ We immediately get $1-xy \in N(-5)$, and $1-xy = (1+y)(1+(1+x)\frac{-y}{1+y})$ gives $1-xy \in \{-2, 5\}$. Now $1-5^{-1}y \sim -5$ forces $1-y \sim -5$. So using $1-xy = 1-xy = (1-y)(1+(1-x)\frac{y}{1-y})$ quickly gives $1-xy \sim 5$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim 2, 1+y \sim 1}$ The $+1$-decomposition yields $1-xy \in N(2)$. Now $1-x \sim 1, 1-y \sim 1$, so the -1-decomposition yields $1-xy \in N(-2)$. Hence $1-xy \in \{1,2\}$. Also, $1-5y \sim 1, 1-5^{-1}x \sim 1$, so the -5-decomposition gives $1-xy \in N(-10)$ forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim 2, 1+y \sim -5}$ The $+1$-decomposition gives $1-xy \in N(-10)$. Also, $1-xy \sim 1, 1-y \sim 1$ so the -1-decomposition yields $1-xy \sim 1, -5$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim -2, 1+y \sim 1}$ The $+1$-decomposition gives $1-xy \in N(-2) \cap N(2) = \{1,2\}$. Also, $1+5x \sim 1, 1+5^{-1}y \sim 1$, so the $+5$-decomposition gives $1-xy \in N(10)$ whence $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim 1, y \sim -2, 1+y \sim -1}$: We immediately get $1-xy \in N(-1)$, and the $+1$-decomposition gives $1-xy \in -N(2)$, so $1-xy \in \{1,2\}$. Also, $1+5y \sim -1, 1+5^{-1}x \sim 1$, so the $+5$-decomposition gives $1-xy \in N(10)$, forcing $1-xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim 2, 1+y \sim -5}$ The $+1$-decomposition gives $1-xy \in -5N(2)$. Also, $1-x \sim -1, 1-y \sim -1$, so the -1-decomposition gives $1-xy \in -N(-2)$, forcing $1-xy \in \{5, 10\}$. Finally, the -5-decomposition gives $1-xy \in -N(-10)$ which gives $1-xy \sim 5$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim -2, 1+y \sim 1}$ We immediately get $1 - xy \in N(-1)$. The $+1$-decomposition gives $1 - xy \in N(-10)$ so $1 - xy \in \{1, 10\}$. Also, $1 - xy \sim -1, 1 - y \sim 1$ so the $+1$-decomposition gives $1 - xy \in N(-2)$, forcing $1 - xy \sim 1$.

- $\boxed{x \sim 2, 1+x \sim -5, y \sim -2, 1+y \sim -1}$ We immediately get $1 - xy \in N(-1)$. The $+1$-decomposition gives $1 - xy \in N(-10) \cap -N(-1)$, so $1 - xy \in \{2, 5\}$. Also, $1 - 5x \sim -1$ and $1 - 5^{-1}y \sim -5$, whence the -5-decomposition gives $1 - xy \in -N(-2)$, forcing $1 - xy \sim 5$.

In all cases $1 - xy \in N(5)$, completing the proof. □

6.2 Appendix B: Calculation of the Residue Field in Case A

We complete the proof of Proposition 3.4.12. As remarked there, it suffices to show in all cases either that $1+x \notin N(5)$, or that $3+x \notin N(5)$; the former implies $1+x \in \mathcal{O}_1$, while the latter implies $1 + x \in 2\mathcal{O}_1$.

Lemma 6.2.1. *If $x \in \mathcal{O}^\times, x \sim -1$, then $3 + x \notin N(5)$.*

Proof. By assumption, and Corollary 3.4.9, $1 + 2x \in N(5)$. We have $1 + 2x \in N(5) \cap N(2) = \{\pm 1\}$. Suppose $1 + 2x \sim 1$, with $1 + 2x = a^2$ say. Then $2 + x = a^2/2 + 3/2 = 2A^2 - 10B^2$ for some A, B. Hence $1 + 2x \in 2N(5)$, a contradiction. Thus $1 + 2x \sim -1$.

Write $1+2x = -a^2$ for some a. Then $2+x \in N(-5)$ by a calculation identical to the above. Also $2 + x \in N(2)$ is immediate, while by Corollary 3.4.9, $2 + x \in N(5)$ as well, forcing $2 + x \sim 1$. Thus $3 + x \in -N(-5) \cap N(-1) = \{2, 10\}$. □

Lemma 6.2.2. *If $x \in \mathcal{O}^\times, x \sim 5$, then $1 + x \notin N(5)$.*

Proof. $1 + 2x \in N(5) \cap N(-10) = \{1, -5\}$. If $1 + 2x \sim 1$, say equalling a^2, then we find $2 + x \in 2N(5)$ as in the above lemma. Therefore we must have $1 + 2x \sim -5$.

Again using Corollary 3.4.9, $2+x \in -N(-1) \cap N(5) = \{-1, -5\}$. Also, $2+x = 2+5b^2$ for some b, which can't be -5 modulo squares, since $2 \notin -N(-1)$. Hence $2+x \sim -1$.

If $1+x \in N(5) \cap N(-5) = \{1, 5\}$, then $1+x \sim 1$ gives $2+x \in N(-1)$, contradiction. Similarly, $1+x \sim 5$ gives $2+x \in N(-5)$, contradiction.

Hence $1+x \notin N(5)$. □

Lemma 6.2.3. *If $x \in \mathcal{O}^\times, x \sim -5$, then $3+x \notin N(5)$.*

Proof. $1+2x \in N(5) \cap N(10) = \{\pm 1\}$. As in the proofs of the above cases, $1+2x$ is not a square, so $1+2x \sim -1$, giving $2+x \in N(-5) \cap N(5) = \{1, 5\}$. Also, $2+x = 2-5b^2$ for some b, which gives $2+x \sim 5$. Thus $3+x \in N(-5)$.

But in addition, $3+x \in -N(-1)$ is visible, so $3+x \in \{-2, -10\}$, as desired. □

This completes all the cases, and hence the proof that $Kv \simeq \mathbb{F}_2$.

6.3 Appendix C: Case B

As explained, the calculations depend on whether $3 \sim 1$ or $3 \sim 2$. Suppose that $3 \sim 2$. Let v_p denote the p-adic valuation on k. Then $v_p(c-2) = v_p(2) = 0$, since $v_p(c) > 0$. Hence $c-2 \in N_k(2)$. It's easy to rule out ± 1 as possibilities, using that $c \notin N(2) \cup N(-2)$. Hence $c-2 \sim \pm 2$. Since $(k, <)$ is archimedean, we can always multiply c by a^2 where $1 < a^2 < 2$, and still have $c-1 \sim 1$ (and so $c \in N_k(-1)$). By choosing a suitable such a^2, we can force a^2c-2 to be negative, and hence we may without loss of generality assume that $c-2 \sim -2$. From here it is easy to pin down the value of $c-3$ and $c-4$, and a similar argument deals with the case when $3 \sim 1$. The result is summarized in the following table:

Table 6.2:

3	$c-2$	$c-3$	$c-4$
2	-2	-2	-1
1	-2	-1	-1

Note that by our choice of c, we always have $c-1 \sim 1$.

Lemma 6.3.1. *Suppose* $3 \sim 2$*. Then* $-1, 2$ *and* $1/2 \in \mathcal{O}_2$*, and consequently so is* -2 *and* $-1/2$*.*

Proof. Pick $x \in \mathcal{O}_1$. We have to show that also $-x, 2x$ and $x/2 \in \mathcal{O}_1$. We proceed as always on a case by case basis. Our strategy is to do the calculations in full for the case when $x \sim c$, and then transfer most of the other cases back to this case.

- $\boxed{x \sim c, 1 + x \sim -2}$ We have $1 - x = (1 + x) - 2x \in N(c) \cap N(-2c) = \{1, -c\}$. Suppose, for a contradiction, that $1 - x \sim -c$. Then $1 + (c-1)x = (1-x) + cx \in N(-c) \cap N(c) = \{1, c\}$. Also, $1 - (c-1)x = (1 + x) - cx \in N(2c) \cap -N(-2) = \{-1, 2c\}$. If $1 - (c-1)x \sim 2$, then we get $1 + (c-1)x \in 2N(c) \cap \{1, c\} = \varnothing$. Hence $1 - (c-1)x \sim -1$, which quickly implies that $1 + (c-1)x \sim 1$, using that $1 + (c-1)x = (1 - (c-1)x) + 2(c-1)x$. From here we get that $1 + (c-2)x = (1 + (c-1)x) - x = (1 + x) + (c - 3)x \in N(c) \cap N(2c) \cap N(-c) = \{1\}$. It is easy to check that $1 + 2x \sim -c$, whence $1 - (c-2)x = (1 + 2x) - cx = (1 + x) - (c-1)x = (1 - (c-1)x) + x$ giving $1 - (c-2)x \sim -c$. Putting $1 - (c-2)x = -ca^2$ for some a, we get $2 + ca^2 = 1 + (c-2)x \sim 1$, whence $2 \in N(c)$: contradiction.

  Hence $1 - x \sim 1$, from which we quickly find $1 - 2x = (1 - x) - x = (1 + x) - 3x \in N(2c) \cap N(c) \cap N(-c) = \{1\}$. Finally, $1 + 2x = (1 + x) + x = (1 - 2x) + 4x \in N(-2c) \cap 2N(2c) \cap N(-c) = \{-2\}$. Checking that $2 + x \in N(2)$ is straightforward.

- $\boxed{x \sim c, 1 + x \sim 1}$ This case requires only the obvious calculations. For example, $1 - x = (1 + x) - 2x \in N(c) \cap N(2c) = \{1, -1\} \subset N(2)$.

- $\boxed{x \sim -c, 1 + x \sim 1}$ We have $1 - x = (1 + x) - 2x \in N(-c) \cap N(-2c) = \{1, -2\} \subset N(2)$. Thus $-x \in \mathcal{O}_1$, and $-x \sim c$. But we know then from the above cases that $-2x, -x/2 \in \mathcal{O}_1$ as well, which gives us what we want.

- $\boxed{x \sim -c, 1 + x \sim -1}$ We have $1 - x = (1 + x) - 2x \in N(-c) \cap N(2c) = \{1, -2c\}$. Suppose, for a contradiction, that $1 = x \sim -2c$. Then $1 + 2x \in N(2c) \cap -N(-c) \cap -N(-1) = \{-1\}$. Next, $1 - 2x = (1 + x) - 3x = (1 - x) - x \in N(-2c) \cap$

$N(2c) \cap -N(-c) = \{2c\}$. It follows that $1-(c-3)x = (1+2x)-(c-1)x = (1+x)-(c-2)x = (1-x)-(c-4)x \in N(2c) \cap N(c) \cap -N(-2c) \cap N(-2) = \varnothing$. Hence we must have $1-x \sim 1$. In other words, $-x \in \mathcal{O}_1$. The other identities to check now follow at once as in the above case.

- $\boxed{x \sim 2c, 1+x \sim 1}$ We have $1-x = (1+x)-2x \in \{1,-1\}$. Next, $1+2x = (1+x)+x \in N(-c) \cap N(-2c) = \{1,-2\} \subset N(2)$. Finally, $2+x = 1+(1+x) \in -N(-c) \cap N(-1) = \{2, 2c\}$. If $2+x = 2cb^2$ for some b, then $1-x = 3-2cb^2 \in 2N(c) \cap \{1,-1\} = \varnothing$: contradiction. Hence $2+x \sim 2$.

- $\boxed{x \sim 2c, 1+x \sim -2}$ It's easy to check that $2+x \in N(2)$, hence $x/2 \in \mathcal{O}_1$. Since $x/2 \sim c$, we immediately get the other calculations for free.

- $\boxed{x \sim -2c, 1+x \sim 1}$ We have $1-x = (1+x)-2x \in N(-2c) \cap N(-c) = \{1,-2\}$. Hence $-x \in \mathcal{O}_1$, and $-x \sim 2c$. Thus we immediately deduce the remaining calculations from the above cases.

- $\boxed{x \sim -2c, 1+x \sim -1}$ We have $1-x = (1+x)-2x \in N(-2c) \cap N(c) = \{1,-c\}$. Suppose $1-x \sim -c$. Then we find $1+2x = (1+x)+x = (1-x)+3x \in N(c) \cap -N(-2c) \cap -N(-1) = \{-1\}$. Also, $1-2x = (1+x)-3x = (1-x)-x = (1+2x)-4x \in N(-c) \cap N(c) \cap cN(2) \in N(2c) = \varnothing$: contradiction. Hence $1-x \sim 1$ and so $-x \in \mathcal{O}_1$. As before, the rest of the calculations now follow from the above cases.

This completes all the cases and thereby the proof. □

Lemma 6.3.2. *Suppose* $3 \sim 1$. *Then* $-1, 2$ *and* $1/2 \in \mathcal{O}_2$, *and consequently so are* -2 *and* $-1/2$.

Proof. We will only do the case where $x \sim c$. All the other cases are easy to do by way of reducing to this case, as in the above lemma.

- $\boxed{x \sim c, 1+x \sim 1}$ It's easy to check that $1-x \in \{1,-1\}$. Next, $1+2x = (1+x)+x \in N(-2c) \cap N(-c) = \{1,-2\} \subset N(2)$. Finally, checking that $2+x \in N(2)$ is also easy.

- $\boxed{x \sim c, 1+x \sim -2}$ We find at once $1-x \in \{1,-c\}$. Suppose, for a contradiction, that $1-x \sim -c$. Then one shows in order that $1-2x \sim -2c$ and so $1+2x \sim -c$. Hence $1-(c-4)x = (1+2x)-(c-2)x = (1+x)-(c-3)x \in \{c\}$, whence $1-(c-2)x = (1+2x)-cx = (1+x)-(c-1)x = (1-(c-4)x)-2x \in \{2c\}$. But $1-(c-1)x \in \{1,-2\}$, and $(1-(c-2)x)-x \in cN(2) = \{\pm c, \pm 2c\}$: contradiction. Hence $1-x \sim 1$. It's now easy to check that $1+2x$ and $2+x$ are in $N(2)$.

□

Using only the obvious decompositions, along with the above lemmas, we can now easily compile the following table summarizing the relevant square classes:

Table 6.3: Stability of $\mathcal{O}_1$ under $N(2)$

x	$1+x$	$1-x$	$1+2x$	$1-2x$	$2+x$	$2-x$
c	1	1,-1	1	1,-1	2	2,-2
c	-2	1	-2	1	-1,2	2
-c	1	1,-2	1,-1	1,-2	2	-1, 2
-c	-1	1	-1	1	2,-2	2
2c	1	1,-1	1,-2	1,-1	2	2,-2
2c	-2	1	-2	1	1,-2	2
-2c	1	1,-2	1,-1	1,-2	2	-1,2
-2c	-1	1	-1	1	2,-2	2

Note that this table *does not depend on the square class of 3*. Our proof that $1-xy \in N(2)$ for $x, y \in \mathcal{O}_1$ will depend only on this table, hence completing the proof irrespective of the square class of 3. We use for this the following decompositions:

$$\begin{aligned}1 - xy &= (1+y)\left(1 + (1+x)\frac{-y}{1+y}\right)\\ &= (1-y)\left(1 + (1-x)\frac{y}{1-y}\right)\\ &= (1+2y)\left(1 + (1+2^{-1}x)\frac{-2y}{1-2y}\right)\\ &= (1-2y)\left(1 + (1-2^{-1}x)\frac{2y}{1-2y}\right)\end{aligned}$$

which we refer to respectively as the $+1, -1, +2$ and -2 decomposition (with respect to y; by symmetry we get analogous identities wrt. x). The following proposition now shows that $\mathcal{O}(N(2))$ does define a valuation ring.

Proposition 6.3.3. *If* $x, y \in \mathcal{O}_1$*, then* $1 - xy \in N(2)$*.*

Proof. We once again can always assume that $x \sim c$. Thus we are left to check the following cases. We do the first case in full, and for the rest simply specify which decompositions to consider.

- $\boxed{x \sim c, 1+x \sim 1, y \sim c, 1+y \sim 1}$ We have $1 - xy = (1+y)(1+(1+x)y')$ where $y' = \frac{-y}{1+y} \sim -c, 1+y' \sim 1$. Hence $1 - xy \in N(c)$. Next, $1 - xy = (1+2y)(1+(1+2^{-1}x)y'')$, where $y'' = \frac{-2y}{1+2y} \sim -2c, 1+y'' \sim 1$. Also, $1+2y \sim 1$ and $1+2^{-1}x \sim 1$ by Table 3. Hence this decomposition yields $1 - xy \in N(2c)$, whence $1 - xy \in \{1, -1\} \subset N(2)$ as desired.

- $\boxed{x \sim c, 1+x \sim 1, y \sim c, 1+y \sim -2}$ The $+1$-decomposition wrt. y gives $1 - xy \in N(-2c)$, while the $+2$-decomposition wrt. y gives $1 - xy \in N(-c)$. Hence $1 - xy \in \{1, -2\} \subset N(2)$.

- $\boxed{x \sim c, 1+x \sim 1, y \sim -c, 1+y \sim 1}$ We immediately get $1 - xy \in N(-c)$. The $+1$-decomposition wrt. y gives $1 - xy \in N(-1)$, while the $+2$-decomposition wrt. x gives $1 - xy \in N(2c)$. In total therefore $1 - xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim 1, y \sim -c, 1+y \sim -1}$ We immediately get $1 - xy \in N(-c)$. The $+1$-decomposition wrt. x gives $1 - xy \in N(-1)$, while the $+2$-decomposition wrt. y gives $1 - xy \in N(2c)$. In total therefore $1 - xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim 1, y \sim 2c, 1+y \sim 1}$ This case is trivial.

- $\boxed{x \sim c, 1+x \sim 1, y \sim 2c, 1+y \sim -2}$ This case is trivial.

- $\boxed{x \sim c, 1+x \sim 1, y \sim -2c, 1+y \sim 1}$ We immediately get $1-xy \in N(-2)$. The $+1$-decomposition wrt. x gives $1-xy \in N(c)$, while the $+2$-decomposition wrt. x gives $1-xy \in N(2c)$. Hence $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim 1, y \sim -2c, 1+y \sim -1}$ Here the $+2$-decomposition wrt. x immediately gives $1-xy \in N(2)$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim c, 1+y \sim -2}$ The $+1$-decomposition wrt. y gives $1-xy \in 2N(c)$, while the -1-decomposition wrt. y gives $1-xy \in N(-c)$. Finally, the -2-decomposition wrt. y gives $1-xy \in N(-2c)$, which gives in total that $1-xy \sim -2$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim -c, 1+y \sim 1}$ We immediately get $1-xy \in N(-1)$. The $+1$-decomposition wrt. y gives $1-xy \in N(2c)$, while the $+2$-decomposition wrt. x gives $1-xy \in N(-c)$. In total therefore $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim -c, 1+y \sim -1}$ We immediately get $1-xy \in N(-1)$. The $+1$-decomposition wrt. y gives $1-xy \in N(2c)$, while the -1-decomposition wrt. y gives $1-xy \in N(c)$. In total therefore $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim -2c, 1+y \sim 1}$ We immediately get $1-xy \in N(-2)$. The $+1$-decomposition wrt. y gives $1-xy \in N(c)$, while the $+2$-decomposition wrt. x gives $1-xy \in N(-c)$. In total therefore $1-xy \sim 1$.

- $\boxed{x \sim c, 1+x \sim -2, y \sim -2c, 1+y \sim -1}$ The -1-decomposition wrt. y immediately gives $1-xy \in N(2)$.

For the last two cases, we have $x \sim c$ and $y \sim 2c$, whence $1-xy \in N(2)$ is immediate.

□

It remains to show that the residue field is not 2-closed. In fact, we show that 2 is not a square in Kv. Since $2 \notin K^2$, it suffices to show that there is no $a \in \mathcal{O}$ such that $a^2 - 2 \in \mathcal{M}$, the maximal ideal. Therefore the following proposition finishes the proof that Case B cannot occur:

Proposition 6.3.4. *For any $a \in K$, we have that $(a^2 - 2)^{-1} \in \mathcal{O}_2$. Therefore if $a \in \mathcal{O}$, $a^2 - 2 \in \mathcal{O}^\times$.*

Proof. We need to show that for all $x \in \mathcal{O}_1$, $x/(a^2 - 2) \in \mathcal{O}_1$, which amounts to showing $1 + \frac{x}{a^2-2} \in N(2)$, or equivalently, $a^2 - (2 - x) \in N(2)$. Since $\mathcal{O}_2$ is closed under multiplication by $\pm 1, \pm 2, \pm 1/2$, it suffices to check this when $x \sim c$. There are two cases to consider.

First suppose that $1 + x \sim -2$. Then by Table 3, we see that $2 - x \sim 2$, so clearly $a^2 - (2 - x) \in N(2)$.

Secondly suppose that $1 + x \sim 1$. Then by Table 3, $1 - x \sim \pm 1$. If $1 - x \sim 1$, then it follows easily that $2 - x \sim 2$ and we are done as above. Otherwise $1 - x \sim -1$. In this case let $x' := -x$. Then $x' \sim -c$ and $1 + x' \sim -1$. Again by Table 3 we find $2 - x' \sim 2$. Hence we get $x'/(a^2 - 2) \in \mathcal{O}_1$, whence also $-x'/(a^2 - 2) = x/(a^2 - 2) \in \mathcal{O}_1$. □

Bibliography

[1] C. Consani and M. Marcolli. *Noncommutative geometry and number theory: where arithmetic meets geometry and physics.* Vieweg Verlag, 2006.

[2] I. Efrat. Finitely generated pro-p Galois groups of p-Henselian fields. *Journal of Pure and Applied Algebra*, **138**:215–228, 1999.

[3] I. Efrat. Demushkin fields with valuations. *Math. Z.*, **243**:333–353, 2003.

[4] A.J. Engler and A. Prestel. *Valued Fields.* Springer-Verlag, 2005.

[5] N. Frohn. *The Model Theory of Absolute Galois Groups.* PhD thesis, Freiburg University, 2011.

[6] P. Gilles and T. Szamuely. *Central simple algebras and Galois cohomology.* Cambridge University Press, 2009.

[7] B. Jacob and R. Ware. A recursive description of the maximal pro-2 Galois group via Witt rings. *Math. Z.*, **200**:379–396, 1989.

[8] M. Jarden and J. Ritter. On the characterization of the local fields by their absolute Galois groups. *J. Number Th.*, **11**:1–13, 1979.

[9] W. Jenkner. Les corps p-adiques dont les groupes de Galois absolus sont isomorphes. *Asterisque*, **209**:221–226, 1992.

[10] J. Koenigsmann. From p-rigid elements to valuations (with a Galois-characterization of p-adic fields). *J. reine angew. Math*, **465**:165–182, 1995.

[11] J. Koenigsmann. Elementary characterization of fields by their absolute Galois groups. *Sib. Adv. Math*, **10**, 2000.

[12] J. Koenigsmann. Encoding valuations in absolute Galois groups. *Fields Institute Communications*, **33**:107–132, 2003.

[13] J. Koenigsmann. On the section conjecture in anabelian geometry. *J. reine angew. Math*, **588**:221–235, 2005.

[14] F.V. Kuhlmann. *Valuation Theory.* Unpublished: available on authors website, 2011.

[15] F.V. Kuhlmann, M. Pank, and P. Roquette. Immediate and purely wild extensions of valued fields. *Manuscr. Math.*, **55**:39–67, 1986.

[16] T.Y. Lam. *Introduction to Quadratic Forms over Fields.* American Mathematical Society, 2005.

[17] A.S. Merkurjev and A.A. Suslin. K-cohomology of Brauer-Severi varieties and the norm residue isomorphism. *Izv. Akad. Nauk SSSR, Ser. Mat.*, **46**:307–340, 1983.

[18] S. Mochizuki. The local pro-p anabelian geometry of curves. In *RIMS Preprint 1097*, 1996.

[19] S. Mochizuki. A version of the Grothendieck conjecture for p-adic local fields. *International Journal of Mathematics*, **6**:499–506, 1997.

[20] H. Nakamura, A. Tamagawa, and S. Mochizuki. The Grothendieck conjecture on the fundamental groups of algebraic curves. *Sugaku Expositions AMS*, **14**:31–53, 2001.

[21] J. Neukirch. Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkorper. *Invent. Math.*, **6**:296–314, 1969.

[22] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, 1999.

[23] F. Pop. Galoische Kennzeichnung p-adisch abgeschlossener Körper. *J. reine angew. Math.*, **392**:145–175, 1988.

[24] F. Pop. On Grothendiecks conjecture in birational anabelian geometry. *Ann. Math.*, **139**:145–182, 1994.

[25] F. Pop. On the birational p-adic section conjecture. *Compositio Math.*, 2010.

[26] F. Pop. $\mathbb{Z}/p$ metabelian birational p-adic section conjecture for varieties. *Unpublished: available on authors website*, 2015.

[27] F. Pop and J. Stix. Arithmetic in the fundamental group of a p-adic curve: on the p-adic section conjecture for curves. *Unpublished: available at arXiv:1111.1354*, 2011.

[28] A. Prestel and P. Roquette. *Formally p-adic fields.* Springer-Verlag, 1980.

[29] L. Ribes and P. Zalesskii. *Profinite Groups.* Springer-Verlag, 2010.

[30] J. Ritter. p-adic fields having the same type of algebraic extensions. *Ann. Math.*, **238**:281–288, 1978.

[31] L. Schneps and P. Lochak. *Geometric Galois Actions 1.* Cambridge, 1997.

[32] J.P. Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

[33] J.P. Serre. *Galois Cohomology.* Springer-Verlag, 2002.

[34] The Stacks Project Authors. Stacks Project. `http://stacks.math.columbia.edu`, *2015.*

[35] J. Stix. Birational p-adic Galois sections in higher dimensions. *Israel Journal of Mathematics*, **198**:49–61, 2013.

[36] J. Stix. *Rational points and arithmetic of fundamental groups: evidence for the section conjecture.* Springer-Verlag, 2013.

[37] A. Tamagawa. The Grothendieck conjecture for affine curves. *Compositio Mathematica*, **109**:135–194, 1997.

[38] B. Zilber. *Zariski geometries: Geometry from the logician's point of view.* Cambridge University Press, 2010.

[39] B. Zilber and E. Hrushovski. Zariski Geometries. *J. American Math Soc.*, **9**:1–56, 1996.