On the Decidability of $\mathbb{Q}_p^{\mathrm{ab}}$

Wang, Chenkai
MSc by Research in Mathematics

Mansfield College
University of Oxford

October 17, 2018

Abstract

In this project we investigate some approaches attacking the question of whether the theory of the maximal abelian extension of the p-adic numbers is decidable. A list of axioms is presented whose completeness we aim to show via quantifier elimination. We separated the quantifier elimination process into five embedding stages. We constructed four of the embeddings, up to the subextension field whose residue field is algebraically closed. For the last stage, some possible approaches are discussed.

Contents

1 Introduction **2**

2 Background **2**

3 Axiomatization of $\mathbb{Q}_p^{\mathrm{ab}}$ **11**

4 Proof Strategy **15**

5 Acknowledgement **20**

1 Introduction

Decidability has always been one of the central problems investigated in the intersection of model theory and number theory. A theory is decidable if there is a (deterministic) algorithm which can decide whether a given statement belongs to that theory (for a formal definition cf., e.g., Definition IV.1.1 in [Kun09]). The most practical way to show decidability is to show there exists a complete recursive axiomatization. Apart from proving some kind of categoricity (which will not be applicable in our case), there are other ways of showing completeness, e.g., through model-completeness and through quantifier elimination (although quantifier elimination implies model-completeness, we separate the two because the approach for proving these two could be a lot different), the former also requires the existence of a prime model and the latter requires the existence of a prime substructure. Certainly the stronger quantifier elimination is a more favorable way to prove decidability because a decidable theory together with quantifier elimination algorithm give us a concrete algorithm of reducing sentences to quantifier-free ones. It is well known that the field of real numbers $\mathbb{R}$ ([Tar51]) and the fields of p-adic numbers $\mathbb{Q}_p$ are decidable in the language of rings $\mathcal{L}_{\text{ring}} = \{+, -, \cdot, 0, 1\}$, the latter is a result due to three papers by Ax and Kochen [AK65a] [AK65b] [AK66] between 1965 to 1966, and independently Ersov [Erš67] (His original paper is in Russian, see [Dri14] for more information) in 1965. On the other hand, $\mathbb{Q}$ is undecidable because there is a way to interpret $\mathbb{Z}$ inside $\mathbb{Q}$ (in fact $\mathbb{Z}$ is definable in $\mathbb{Q}$ [Rob49]), hence the undecidability transfers from $\mathbb{Z}$ to $\mathbb{Q}$ ([Göd31],[Koe14]). In this paper, we shall discuss the possible steps to show the decidability of the maximal abelian extension of $\mathbb{Q}_p$.

2 Background

Hensel ([Hen97]) invented the p-adic numbers at the end of 19th century with the objective to transfer methods from analysis, especially the series expansion and approximation algorithms to the algebraic world of number theory [Bél11] [Rob00]. These all start with the comparison between two rings: $\mathbb{Z}$ and $\mathbb{C}[X]$ [Gou03]. We will see the prime elements play a central role of revealing local information about the elements of these rings. We present the connections in the following table:

$\mathbb{Z}$	$\mathbb{C}[X]$
prime numbers	linear polynomials
$m = \pm p_1 \cdots p_n$	$P(X) = a(X - r_1) \cdots (X - r_n)$
base-p expansion	Taylor expansion

The next natural thing to do is to extend these connections to their field of quotients. First on the $\mathbb{C}[X]$ side, we get the field of rational functions $\mathbb{C}(X)$, and the expansion for a particular rational function is a finite tailed Laurent series:

$$f(X) = \frac{P(X)}{Q(X)} = \sum_{i=k}^{\infty} a_i (X - r)^i, \text{ where } a_k \neq 0. \tag{1}$$

The integer k in the indices of a Laurent series actually carries local information about $f(X)$ around a particular point $r \in \mathbb{C}$: it indicates whether $f(X)$ has a root or a pole at $r \in \mathbb{C}$, and to what degree. If k is positive, then we have a root of multiplicity k. If k is negative, then we have a pole of order $-k$. Since such expansion is unique for each rational function, we obtain the inclusion $\mathbb{C}(X) \hookrightarrow \mathbb{C}((X - r))$, one for each r.

Hensel's idea is to mimic such construction on the $\mathbb{Z}$ side, this is precisely the very idea behind the p-adic numbers, i.e., every rational number can be "expanded" in base p:

$$\frac{n}{m} = \sum_{i=k}^{\infty} a_i p^i \tag{2}$$

where $0 \leq a_i < p$. Certainly a clear difference between expansion (equation 2) and the one for rational functions (equation 1) is carrying since p is an integer and these coefficients are also integers, so the sum of two such coefficients can be greater than p, whereas adding two complex numbers can never be a linear polynomial. Like rational functions, these expansions carry important information of a rational number around p, and similarly we have inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. The number k represents a kind of "multiplicity" or "order" of p. So we can write $\frac{n}{m} = p^k \frac{a}{b}$, where p divides neither a nor b. Of course, these discussions does not convey formal description, but the idea is still very clear: an analogy of Taylor/Laurent series expansion applied to the integers.

$\mathbb{Q}$	$\mathbb{C}(X)$
p-adic expansion	Laurent expansion

We now introduce the field of p-adic numbers $\mathbb{Q}_p$, which can be constructed in different ways. Analytically, it is the completion of $\mathbb{Q}$ with respect to the p-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, which can be obtained using the following steps:

1. We define $v_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ to be $v_p(n) = \max\{k \in \mathbb{N} \mid p^k \text{ divides } n\}$ and $v_p(0) = \infty$.

2. We extend $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ using the formula $v_p(m/n) = v_p(m) - v_p(n)$ and $v_p(0) = \infty$.

Then the p-adic absolute value can be defined to be $|r|_p = p^{-v_p(r)}$ so the structure of metric space and completion can be defined in the usual way. Intuitively, the p-adic absolute value of a number counts the prime factor p. In a 1916 paper written by one of Hensel's students, Ostrowski, using techniques from analysis, he showed that the only absolute values on $\mathbb{Q}$ are (more precisely, equivalent to, or induce the same topology) either the trivial absolute value, or the usual absolute value or one of the p-adic absolute values (Theorem 1 in [Kob77], Proposition 1.2.1 and Theorem 2.1.4 in [EP05]). In this paper we focus on the p-adic cases, they are also called non-archimedean absolute values because they satisfy the ultra-metric triangular inequality (although the trivial absolute value also satisfies it) $|x| + |y| \leq \max\{|x|, |y|\}$. It is called non-archimedean because there is an equivalence between the ultra-metric triangular inequality and the property that $\{|n| \mid n \in \mathbb{Z}\}$ is bounded (Proposition 1.1.1 in [EP05]). Using this p-adic absolute value, we can define the metric space structure in the usual way, and analyze the topological properties of $\mathbb{Q}_p$.

Algebraically speaking, $\mathbb{Q}_p$ is the quotient field of the p-adic integers $\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$, the inverse limit of the rings $\mathbb{Z}/p^k\mathbb{Z}$ (Example 2.1.6(2) in [RZ00]). This matches the previous analogy of expanding a number in a "p-adic" way, i.e., write an infinite expansion in base p. Thus we may view the field of p-adic numbers as a formal Laurent series (finitely many negative terms) in base p:

$$\mathbb{Q}_p = \left\{ \sum_{k=n}^{\infty} a_k p^k \middle| n \in \mathbb{Z}, 0 \leq a_k < p, a_n > 0 \right\} \tag{3}$$

with the arithmetic given by the usual base-p expansion of the real numbers, except the carrying needs to be done up to infinity. The extended p-adic valuation is the exponent of the first nonzero term:

$$v_p\left(\sum_{k=n}^{\infty} a_k p^k \right) = n \tag{4}$$

This "base-p" expansion is like our usual decimal expansion, but in the opposite direction, i.e., the "decimal part" is finite and the "integer part" is infinite.

Combining the two view points, we can give detail descriptions for the two important subsets of $\mathbb{Q}_p$:

1. The closed unit disk:

$$\begin{aligned}\mathcal{O} &= \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\} \\ &= \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\} \\ &= \left\{ \sum_{k=0}^{\infty} a_k p^k \middle| 0 \leq a_k < p \right\} \\ &= \mathbb{Z}_p \end{aligned} \tag{5}$$

2. The open unit disk:

$$\begin{aligned}\mathfrak{m} &= \{x \in \mathbb{Q}_p \mid |x|_p < 1\} \\ &= \{x \in \mathbb{Q}_p \mid v_p(x) > 0\} \\ &= \left\{ \sum_{k=1}^{\infty} a_k p^k \middle| 0 \leq a_k < p \right\} \\ &= p\,\mathbb{Z}_p \end{aligned} \tag{6}$$

From this, we see that the residue field $\mathcal{O}/\mathfrak{m} = \mathbb{Z}_p/p\,\mathbb{Z}_p \cong \mathbb{Z}/p\,\mathbb{Z} = \mathbb{F}_p$ (the middle isomorphism followed from Corollary 3.3.6 in [Gou03]) corresponds to the set $\{0, \cdots, p-1\}$ of "digits" used in the p-adic expansion.

An important application of the p-adic numbers is Hasse's local-global principle (Section 2.8 in [Neu99]), which states that certain types of equations have solutions in $\mathbb{Q}$ iff they have solutions in $\mathbb{R}$ and all $\mathbb{Q}_p$. This in general is not true, but we have the Hasse-Minkowski Theorem (Section 6.4 in [Neu99]), which states the local-global principle is true for quadratic forms. Thus, the question of whether a given rational number can be represented by a given quadratic form is a decidable problem, since $\mathbb{R}$ and $\mathbb{Q}_p$ are decidable and we only need to check finitely many p (Section 2.2 in [Koe14]).

The p-adic numbers also have deep connection with Hilbert's 10th problem. The generalized Hibert's 10th problem asks if there is an algorithm deciding whether a given polynomial has roots in a given ring (given a polynomial equation $f(x_1, \cdots, x_n) = 0$ with coefficients in a ring R, decide whether it has a solution with $x_1, \cdots, x_n \in R$), i.e., in model-theoretical terms, it asks if the existential positive theory of a given ring is decidable [Poo03]. The original Hilbert's 10th problem asks the question on the ring of integers. The key strategy (Matiyasevich–Robinson–Davis–Putnam (MRDP) Theorem [MF93]) for proving the original Hilbert's 10th problem is to establish the equivalence of the Diophantine sets and semi-decidable sets (or called recursively enumerable). And then code the halting problem as a semi-decidable but non-decidable set, thus showing a universal algorithm cannot exist (Section 3.2.5 in [Yan98]).

Now we give the general definition of a valuation, sometimes called a Krull valuation. This is a generalization of the concept of a real valuation into an

abstract one by relaxing the requirement of the set of values to be a mere ordered abelian group. It corresponds to non-archimedean absolute values.

Definition 2.1. A valuation v on a field K is a surjective function

$$v : K \to \Gamma \cup \{\infty\} \tag{7}$$

where Γ is an ordered abelian group (we extend $+$ by $\infty = \gamma + \infty = \infty + \gamma$ for all $\gamma \in \Gamma$), such that for all $x, y \in K$

1. $v(x) = \infty$ iff $x = 0$.
2. $v(xy) = v(x) + v(y)$.
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

Then we define the valuation ring and the residue field. It can be shown that $\mathcal{O}$ is a local ring (Section 2.1 in [EP05]), so $\mathfrak{m}$ is its only maximal ideal:

1. $\mathcal{O} = \{x \in K \mid v(x) \geq 0\}$.
2. $\mathfrak{m} = \{x \in K \mid v(x) > 0\}$.
3. $K_v = \mathcal{O} / \mathfrak{m}$.

Given a field K, the set of valuations and valuation rings on the field are in one-one correspondence (up to an order-preserving isomorphism between value groups) via the mappings (Proposition 2.1.3 in [EP05]):

1. $v \mapsto \mathcal{O}_v = \{x \in K \mid v(x) \geq 0\} \subseteq K$.
2. $\mathcal{O} \mapsto v_{\mathcal{O}} : K \to (K^\times / \mathcal{O}^\times) \cup \{\infty\}$, via the canonical projection.

Hence we can present a valued field model theoretically as either the structure (K, v) or $(K, \mathcal{O})$. Viewing the valued field as a structure in the model theory sense ($\mathcal{O}$ as unary predicate), we naturally have the substructure and extension relation with the condition $\mathcal{O}_1 = \mathcal{O}_2 \cap K_1$ for $(K_1, \mathcal{O}_1) \subseteq (K_2, \mathcal{O}_2)$. Hence we get the two canonical embeddings (Section 3.2 in [EP05]):

1. $\Gamma_1 \to \Gamma_2$.
2. $K_{v_1} \to K_{v_2}$.

The index between the two value groups is called the ramification index, denoted by e, and the degree between the two residue fields is called the residue degree, denoted by f. If $e = f = 1$ for a valued field extension pair, we call the extension immediate, which indicates that the value group and the residue

field stay unchanged. For finite extension L/K, the number of valuation ring extensions is bounded by the field extension degree, and furthermore we have the "fundamental inequality" (Theorem 3.3.4 in [EP05]):

$$\sum_i e_i f_i \leq [L : K] \tag{8}$$

where i enumerates the finitely many valuation ring extending $(K, \mathcal{O})$ to L.

Hensel's lemma (Theorem 1.3.1 in [EP05]) is one of the most powerful items in the toolkit that comes with the p-adic numbers, which is in the spirit of Newton's methods in the p-adic world. It is the key building block bridging together analytic methods with the algebraic settings. We present a slightly more general version here. Recall that the rank of a valuation is the rank of its value group, i.e., the order type of the chain of proper convex subgroups, linearly ordered by $\subseteq$. An ordered abelien group has rank 1 if and only if it can be embedded into the reals (Proposition 2.1.1 in [EP05]). Here we state and prove the Hensel's lemma using a mild reformulation of Theorem 1.3.1 from [EP05]:

Theorem 2.2 (Hensel)**.** Let (K, v) be a complete rank 1 valued field, then Hensel's property holds: Let $f \in \mathcal{O}[X]$ be a polynomial and let $a_0 \in \mathcal{O}$ such that $v(f(a_0)) > 2v(f'(a_0))$, then $f(a) = 0$ for some $a \in \mathcal{O}$ with $v(a - a_0) > v(f'(a_0))$.

Proof. Since our field is complete, it suffices to construct a Cauchy sequence. First we define the sequence just like the regular Newton's method:

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} \tag{9}$$

Next we need to show it satisfies the Cauchy property. For demonstration purpose, we begin by expanding $f(a_1)$, the rest is just a matter of induction.

$$\begin{aligned} f(a_1) &= f\left(a_0 - \frac{f(a_0)}{f'(a_0)}\right) \\ &= f(a_0) - \frac{f(a_0)}{f'(a_0)} f'(a_0) + \left(\frac{f(a_0)}{f'(a_0)}\right)^2 b_0 \\ &= f'(a_0)^2 \frac{f(a_0)^2}{f'(a_0)^4} b_0 \end{aligned} \tag{10}$$

where $b_0 \in \mathcal{O}$. From the assumption, we see $v(f(a_0)) \geq 2v(f'(a_0)) + \epsilon$ for some $\epsilon > 0$ (fix this ϵ throughout the proof). So the value of $f(a_1)$ is

$$v(f(a_1)) \geq 2v(f'(a_0)) + 2\epsilon \tag{11}$$

Similarly, we expand $f'(a_1)$:

$$\begin{aligned} f'(a_1) &= f'\left(a_0 - \frac{f(a_0)}{f'(a_0)}\right) \\ &= f'(a_0) - \frac{f(a_0)}{f'(a_0)}c_0 \\ &= f'(a_0)\left(1 - \frac{f(a_0)}{f'(a_0)^2}c_0\right) \end{aligned} \tag{12}$$

So the value of $f'(a_1)$ is

$$v(f'(a_1)) = v(f'(a_0)) + 0 = v(f'(a_0)) \tag{13}$$

By induction we have the following (in)equalities:

1. $v(f(a_{n+1})) \geq 2v(f'(a_n)) + 2^n\epsilon$.
2. $v(f'(a_{n+1})) = v(f'(a_n))$.

First, it is not hard to see the sequence a_n is Cauchy and the value of $v(f(a_n))$ goes to infinity (since we assume our value group has rank 1, i.e., the only convex subgroup is the trivial one) so the limit $a = \lim a_n$ is a zero of f. Second, the sequence $f'(a_n)$ is also Cauchy and the limit is $f'(a)$. From this, we deduce that for $\delta > v(f'(a_0))$,

$$v(f'(a) - f'(a_n)) > \delta > v(f'(a_0)) = v(f'(a_n)) \tag{14}$$

so $v(f'(a)) = v(f'(a_0))$.

Finally, from the Cauchy property, we see that $v(a_n - a_0) \geq v(f'(a_0)) + \epsilon$. So for large n, we have:

$$v(a - a_0) = v(a - a_n + a_n - a_0) > v(f'(a_0)) = v(f'(a)) \tag{15}$$

which finishes the proof. □

Note the rank 1 in the assumption of the above statement means the value group has only one convex proper subgroup, namely $\{0\}$, this condition can be shown to be equivalent to the property that the value group can be embedded into the ordered group of the real numbers. This condition is necessary because for a fixed $\epsilon > 0$, $\lim_n 2^n\epsilon = \infty$ holds only in rank 1 ordered abelian group.

It can also be shown that Hensel's property is equivalent to the following statement called Hensel's lifting principle (Corollary 1.3.2 in [EP05]). Notice the $\rightarrow$ direction is a direct application, the $\leftarrow$ proof will be presented below. Denote $\overline{a}$ and $\overline{f}$ for the corresponding element in the residue field K_v and the polynomial ring over the residue field $K_v[X]$:

Theorem 2.3. Hensel's property is equivalent to the following statement: Let $f \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ with $\overline{f}(\overline{a}) = 0$ but $\overline{f}'(\overline{a}) \neq 0$, i.e., f has a simple zero in the residue field. Then $f(b) = 0$ for some $b \in \mathcal{O}$ with $\overline{a} = \overline{b}$ in K_v.

Proof. ($\leftarrow$) First we expand $f(a_0 + X) = f(a_0) + f'(a_0)X + g(X)X^2$, where $g \in \mathcal{O}[X]$. Then we do a change of variable by putting $Y = \frac{X}{f'(a_0)}$. Let

$$\begin{aligned} f_1 &= \frac{f(a_0 + X)}{f'(a_0)^2} \\ &= \frac{f(a_0)}{f'(a_0)^2} + Y + g_1(Y)Y^2 \end{aligned} \tag{16}$$

where $g_1(Y) = g(X) = g(f'(a_0)Y)$. Clearly $f_1, g_1 \in \mathcal{O}[Y]$ and $\frac{f(a_0)}{f'(a_0)^2} \in \mathfrak{m}$ by assumption. By passing down to residue field, we see f_1 has a simple zero there, which is $\overline{0} = \mathfrak{m}$, so $f_1(b) = 0$ for some $b \in \mathfrak{m}$, which implies $f(a) = 0$, where we let $a = a_0 + f'(a_0)b$. To complete the proof, we have $v(a - a_0) = v(f'(a_0)) + v(b) > v(f'(a_0))$. □

There are many other properties which can be shown to be equivalent to Hensel's lemma, we list them here (Theorem 4.1.3 in [EP05]):

1. (K, v) extends uniquely to every algebraic extension.
2. (K, v) extends uniquely to K^{sep}, the separable closure.
3. For each irreducible $f \in \mathcal{O}[X]$ with $\overline{f} \notin K_v[X]$, there exists $g \in \mathcal{O}[X]$ such that $\overline{g} \in K_v[X]$ and it is irreducible and $\overline{f} = (\overline{g})^s$ for some $s \geq 1$.
4. For $f, g, h \in \mathcal{O}[X]$ with $\overline{g}, \overline{h}$ relatively prime in $K_v[X]$ and $\overline{f} = \overline{g}\overline{h}$, there exists $g_1, h_1 \in \mathcal{O}[X]$ such that $f = g_1 h_1$, $\overline{g} = \overline{g_1}$, $\overline{h} = \overline{h_1}$, and $\deg g_1 = \deg \overline{g}$.
5. Every polynomial of the form $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathcal{O}[X]$ with $a_{n-1} \notin \mathfrak{m}$ and $a_{n-2}, \cdots, a_0 \in \mathfrak{m}$ has a root in K.
6. Every polynomial of the form $X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1 X + a_0 \in \mathcal{O}[X]$ with $a_{n-2}, \cdots, a_0 \in \mathfrak{m}$ has a root in K.

Next we look into algebraic extensions of $\mathbb{Q}_p$. There has been much progress in this direction. The original idea of Ax and Kochen (pp.448-449 in [AK66], also surveyed by p.5 in [Bél11]) is also based on quantifier elimination, but instead of using valuation, they were using a cross-section map $\pi(x)$, which is a section of the valuation, from the value group to the multiplicative group as follows:

$$n \mapsto p^n : \mathbb{Z} \to \mathbb{Q}_p^\times \tag{17}$$

This is not definable in $\mathcal{L}_{\text{val}}$ ([Mac76]), but Macintyre introduced the power predicates $P_n(x) \leftrightarrow \exists y(x = y^n)$ as a tool to transfer semi-algebraic formulas between models, so that the quantifier elimination can be achieved. It is also worth mentioning that under these power predicates, the valuation ring $\mathcal{O}$ can be defined using an algebraic atomic formula for example $x \in \mathcal{O}$ iff $1+p^3x^4 = y^2$ for some y.

In this paper we look into the maximal abelian extension of the p-adic numbers. An abelian extension of a field is a Galois extension such that its Galois group is abelian. The maximal abelian extension is the compositum of all such abelian extensions. Studying abelian extensions is the subject of class field theory (see Chapter IV to VI in [Neu99]). One of its fundamental result is the following, it describes what an abelian extension looks like for simple cases like $\mathbb{Q}$ and $\mathbb{Q}_p$, we presents the local version (i.e., the version for $\mathbb{Q}_p$, Corollary V.1.9 in [Neu99]) here. We denote by μ_∞ the group of all roots of unity:

Theorem 2.4 (Kronecker-Weber)**.** Every abelian extension of $\mathbb{Q}_p$ is contained in some cyclotomic extension of $\mathbb{Q}_p$. Hence the maximal abelian extension is just $\mathbb{Q}_p$ adjoining all roots of unity $\mathbb{Q}_p^{\text{ab}} = \prod_n \mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\mu_\infty)$.

One application of the above theorem is to use the cyclotomic polynomials to describe the value group of $\mathbb{Q}_p^{\text{ab}}$. First, we list some facts about valued field extension:

Proposition 2.5. Let K be a finite extension $\mathbb{Q}_p \subseteq K$ of degree n.

1. There is a unique valuation on K extending v_p (also written v_p), which is given by the formula: $v_p(x) = \frac{1}{n} v_p(N(x))$, where $N : K \to \mathbb{Q}_p$ is the norm function. (Remark 3.2.17 in [EP05] and Theorem 5.3.5 in [Gou03])

2. Let e be the ramification index, then the value group of K is $\frac{1}{e}\mathbb{Z}$. (Proposition 5.4.2 in [Gou03]) We say an element π is a uniformizer if $v_p(\pi) = 1/e$, i.e., it generates the value group. In the case of $K = \mathbb{Q}_p(\zeta_{p^k})$, a uniformizer is $1 - \zeta_{p^k}$ (Section 5.6 in [Gou03]).

3. Let f be the residue degree, then the residue field is $\mathbb{F}_{p^f}$, the finite field with p^f elements. (Proposition 5.4.6 in [Gou03]) For each f, $\mathbb{Q}_p(\zeta_{p^f-1})$ is the unique unramified extension of $\mathbb{Q}_p$ of degree f. The compositum of all these extensions is called the maximal unramified extension of $\mathbb{Q}_p$, denoted by $\mathbb{Q}_p^{\text{uram}}$. It can be shown that $\mathbb{Q}_p^{\text{uram}} = \mathbb{Q}_p(\mu_{q\neq p})$, $\mathbb{Q}_p$ adjoined by all prime to p-th roots of unity. (Proposition 5.4.11 in [Gou03])

Using the fact that the group μ_∞ is generated by all prime powers q^k, we see it suffices to compute the value for all uniformizers of the form $1 - \zeta_{p^k}$. Let

$\Phi_{p^k}(X) = \prod_{i=1}^{\varphi(p^k)}(X - \zeta_{p^k,i})$ be the p^k-th cyclotomic polynomial, where $\varphi(n)$ is the Euler totient function, and $\zeta_{p^k,i}$ denote i-th primitive p^k-th root of unity (the order does not matter here, we can pick any one of these to be ζ_{p^k}). Evaluate at $X = 1$ we have $p = \prod_{i=1}^{\varphi(p^k)}(1 - \zeta_{p^k,i})$ and take valuation on both sides we have $1 = \varphi(p^k)v(1 - \zeta_{p^k})$, which implies $v(1 - \zeta_{p^k}) = \frac{1}{\varphi(p^k)} = \frac{1}{p^k - p^{k-1}} = \frac{1}{p^{k-1}(p-1)}$. Of course, we can directly calculate it using the norm function as well. Hence the value group of $\mathbb{Q}_p^{\text{ab}}$ is $\Gamma = \frac{1}{p-1}\frac{1}{p^\infty}\mathbb{Z} \cong \frac{1}{p^\infty}\mathbb{Z}$. On the other hand, the value group of $\mathbb{Q}_p^{\text{uram}}$ is $\mathbb{Z}$, the same as for $\mathbb{Q}_p$ since there is no ramification. Using Proposition 2.5.3, we see the residue field of both $\mathbb{Q}_p^{\text{uram}}$ and $\mathbb{Q}_p^{\text{ab}}$ is $\overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$.

3 Axiomatization of $\mathbb{Q}_p^{\text{ab}}$

To show decidability of the theory of a given structure, the usual way is by identifying sufficiently many key properties of the structure, one finds a complete axiomatization. Using the fact that the list of these properties is first-order expressible and they are recursively enumerable, we obtain decidability for the complete theory (Theorem A.1 in [PD11]). In the case of the field of real numbers $\mathbb{R}$, the key properties are called real closed, and it is proved to be complete (Theorem 4.2.3 in [PD11]):

1. K admits an ordering $\leq$, which can be shown to be equivalent to the first-order property that it is formally real, i.e., -1 is not a sum of squares.
2. $(K, \leq)$ is real closed, i.e., it has no proper algebraic order field extension, which can be shown to be equivalent to these two first-order properties:
   (a) Every odd degree polynomial has at least one root.
   (b) Every element or its negative is a square.

In the case of $\mathbb{Q}_p$, the key properties are called p-adically closed (Theorem 3.1 in [PR84]), and it is proved to be complete (Theorem 5.1 in [PR84]):

1. K is a henselian valued field of mixed characteristic $(0, p)$, i.e., $\text{char}(K) = 0$ and $\text{char}(K_v) = p$. A henselian valued field is a valued field satisfies Hensel's lemma.
2. $K_v = \mathbb{F}_p$.
3. $\Gamma_v \equiv \mathbb{Z}$, i.e., it is a $\mathbb{Z}$-group.
4. $v(p)$ is minimal positive.

Due to a result by Derakhshan and Macintyre [DM16], which proved the model completeness for finitely ramified henselian valued field of characteristic zero having $\mathbb{Z}$-group as value group is model complete if the residue field is also model complete. Hence, we may axiomatize $\mathbb{Q}_p^{\text{uram}}$ by the following list of axioms:

1. K is a henselian valued field of mixed characteristic $(0, p)$.
2. K_v is algebraically closed.
3. Γ_v is a $\mathbb{Z}$-group.
4. $v(p)$ is minimal positive.

The following table sums up the valued fields we will encounter together with their value groups and residue fields. We added the field $\mathbb{Q}_p^{ab}(\sqrt[p]{p})$ for comparison: The residue field stays unchanged and the value group stays unchanged as well because $v_p(\sqrt[p]{p}) = \frac{1}{p} \in \frac{1}{p^\infty}(\frac{1}{p-1}\mathbb{Z})$.

Valued Field K	Residue Field K_v	Value Group Γ (without ∞)
$\mathbb{Q}_p^{\text{ab}}(\sqrt[p]{p})$	$\overline{\mathbb{F}_p}$	$\frac{1}{p^\infty}(\frac{1}{p-1}\mathbb{Z}) \cong \frac{1}{p^\infty}\mathbb{Z}$
$\mathbb{Q}_p^{\text{ab}} = \mathbb{Q}_p(\mu_\infty)$	$\overline{\mathbb{F}_p}$	$\frac{1}{p^\infty}(\frac{1}{p-1}\mathbb{Z}) \cong \frac{1}{p^\infty}\mathbb{Z}$
$\mathbb{Q}_p^{\text{uram}} = \mathbb{Q}_p(\mu_{q\neq p})$	$\overline{\mathbb{F}_p}$	$\mathbb{Z}$
$\mathbb{Q}_p$	$\mathbb{F}_p$	$\mathbb{Z}$

Table 1: Value groups and residue fields for some extensions of $\mathbb{Q}_p$

Now we can state the proposed axiomatization for $\mathbb{Q}_p^{ab}$ in the first order language $\mathcal{L}_{\text{val}} = \mathcal{L}_{\text{ring}} \cup \{\mathcal{O}\}$ of valued fields, where $\mathcal{O}$ is a unary predicate for the valuation ring. Note that in this language we can "talk" about the valuation, the value group, the residue field etc. via the canonical interpretations.

Theorem 3.1. There is a recursive set Σ of $\mathcal{L}_{\text{val}}$ sentences whose models are precisely the fields (K, v) satisfying the following properties:

1. (K, v) is a henselian valued field of mixed characteristic $(0, p)$.
2. K_v is algebraically closed.
3. $\Gamma_v \equiv \frac{1}{p^\infty}\mathbb{Z}$.
4. $K \cap \overline{\mathbb{Q}} = (\mathbb{Q}_p^{\text{ab}}) \cap \overline{\mathbb{Q}}$.
5. For each prime $q \neq p$, we have q does not divide $v(1 - \zeta_p)$.
6. v is the canonical p-henselian valuation.

Proof.

1. $\mathbb{Q}_p$ is henselian, so any algebraic extension of it is henselian as well using the uniqueness of valuation ring extension property. The residue field of $\mathbb{Q}_p^{\text{ab}}$ is $\overline{\mathbb{F}_p}$, so it has characteristic p. Henselianity has many equivalent formulations, they are first-order expressible and recursive (Theorem 4.1.3 in [EP05]). We can pick the statement about the existence of roots of certain polynomials as our candidate.

2. Because we can build arbitrarily large models, being the field $\overline{\mathbb{F}_p}$ exactly is not fisrst-order expressable, the best we can say is it is algebraically closed. The characteristic is stated in the previous axiom. We can express this property by stating the field has a root for each polynomial, which is first-order expressible and recursive.

3. This is equivalent to the following two conditions (Theorem 4.4 to Theorem 4.7 in [RZ60]):

   (a) Γ_v is regularly ordered.

   (b) For every prime q, $[\Gamma_v : q\Gamma_v] = q^{1-\delta_{p,q}}$, where δ is the Kronecker delta function.

   Both conditions can be shown to be elementary by Robinson and Zakon in [RZ60]. First, regularity is equivalent to being elementary equivalent to an Archmedian ordered group, which is first-order expressed by the following criterion (Definition 3.3 in [RZ60]): For every n and $\gamma_1 < \cdots < \gamma_n \in \Gamma$, there exists $\delta \in \Gamma$ such that $\gamma_1 \leq n\delta \leq \gamma_n$, i.e., for n elements in the group, we must have an n-divisible element in between the smallest one and the largest one. The second condition is equivalent to stating the maximum number of elements which are mutually incongruent modulo q, which is also elementary (Section 3 remark in [RZ60]).

4. This says the algebraic part of K is the same as the algebraic part of $\mathbb{Q}_p^{\text{ab}}$. This axiom is recursive, because $\mathbb{Q}_p$ is decidable: We have to say, for each monic irreducible polynomial of degree n over $\mathbb{Z}$, whether or not it has a zero in $\mathbb{Q}_p(\zeta)$, where ζ is a primitive $n!$-th root of unity (here we use the local Kronecker-Weber Theorem). We observe that this axiom was not needed for $\mathbb{Q}_p$ or $\mathbb{Q}_p^{\text{uram}}$. The example $\mathbb{Q}_p^{\text{ab}}(\sqrt[p]{p})$ showed in the first line of Table 1 satisfies all of the axioms except this one (for $p > 2$ of course).

5. The intuition behind axiom 5 is that the element $1 - \zeta_p$ behaves a bit like a uniformizer. Without it the theory is incomplete. In fact the group $\bigoplus_{q \neq p} a_q \mathbb{Z}_{(q)}$, where $a_q \in \mathbb{R}$ are all linearly independent over $\mathbb{Q}$, can be

shown to be elementarily equivalent to $\frac{1}{p^\infty}\mathbb{Z}$, but the type of the element $v(1-\zeta_p)$ is omitted in this group. One can construct a field of transcendence degree 1 over $\mathbb{Q}$ satisfying axioms 1, 2, 3, 4, 6, but not axiom 5. Again, it is clear how to effectively write down an axiom scheme for axiom 5 (note that this axiom holds in $\mathbb{Q}_p^{\mathrm{ab}}$ for any choice ζ_p of a primitive p-th root of unity).

6. First of all, the first-order expressability of this axiom is only recently established (Main Theorem in [JK15]). The term "p-henselian" means the valuation extends uniquely to $K(p)$, the compositum of all p-power degree Galois extensions of K, and the *canonical* p-henselian valuation of K is the coarsest p-henselian valuation of K with p-closed residue field, if any such exists, and the finest p-henselian valuation of K otherwise. By the Main Theorem of [JK15], there is an $\mathcal{L}_{\mathrm{ring}}$-formula φ_p in one free variable such that, for any field K containing ζ_p, $\varphi_p(K)$ is the valuation ring of the canonical p-henselian valuation on K. So axiom 6 is given by the single sentence expressing $\mathcal{O}_v = \varphi_p(K)$.

   The purpose of this axiom is to pick out the "correct" henselian valuation for our field. Let us briefly explain why this axiom is, indeed, necessary. This goes via saturated model theory. Let $(K, v) = (\mathbb{Q}_p^{\mathrm{ab}}, v_p)$ and take a saturated elementary extension $(K^*, v^*) \succeq (K, v)$. Since K^* is saturated, it can realize the type $\{0 < v(x) < \frac{1}{n}v(p) \mid n \geq 1\}$, so we can find a convex proper subgroup around 0 such that it does not contain $v(p)$. Let w be the coarsest coarsening of v^*, which has residue characteristic p and we know that $\mathcal{O}_{v^*} \subsetneq \mathcal{O}_w$. Let $\overline{v}^*$ be the valuation induced by v^* on K_w^*. And let $\overline{L}$ be the fixed field of a complement of the ramification subgroup of the absolute Galois group $G_{K_w^*}$ with respect to $\overline{v}^*$. Such complement exists due to [KPR86]. Now we have $\overline{L} = \overline{L}(p)$ and the field extension $\overline{L}/K_w^*$ is a separable algebraic extension. This extension lifts to a separable algebraic extension L/K^* which is purely inert with respect to w and immediate with respect to v^*. Hence we have the valued field (L, v^*) with all axioms satisfied except the last axiom because on L, w is the canonical p-henselian valuation: $\overline{L} = L_w = L_w(p)$.

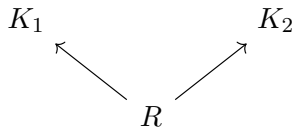
□

Our goal is to show Σ axiomatizes $\mathbb{Q}_p^{\mathrm{ab}}$, so we call them axioms. There are some key examples that satisfy these axioms: $\mathbb{Q}_p^{\mathrm{ab}}$, $\mathbb{Q}_p^{\mathrm{ab}} \cap \overline{\mathbb{Q}}$, and $\mathbb{Q}_p^{\mathrm{ab}}((\mathbb{Q}))$. Note Σ can also be rephrased as $\mathcal{L}_{\mathrm{ring}}$-axioms since the valuation predicate is definable by Koenigsmann and Hong in (Theorem 5 in [Hon13]). The original result by Koenigsmann (Lemma 3.6 in [Koe04]) applies to rank-1 henselian valuation with non-divisible value group. And Hong extended this result to regular value group.

4 Proof Strategy

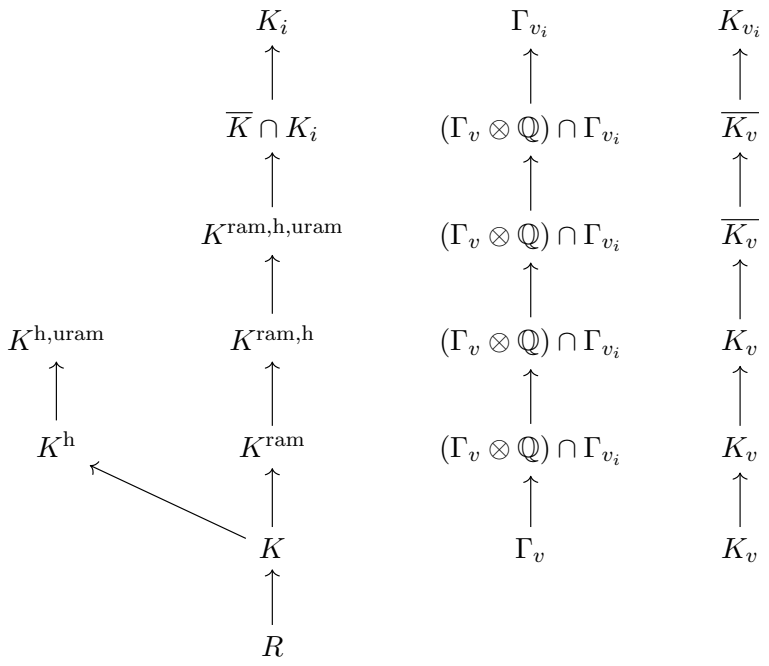
Our main method of showing completeness of Σ is to use the model-theoretical criterion for quantifier elimination, which is the following principle (Theorem 3.4.1 in [PD11]):

Theorem 4.1 (Quantifier Elimination Criterion)**.** Let Σ be an axiom set in a language $\mathcal{L}$. Σ admits quantifier elimination iff for any two models K_1, K_2 of Σ with common finitely generated substructure R, and for any primitive $\exists$-sentence in $\mathcal{L}_R$ that holds in K_1 holds also in K_2. (A primitive $\exists$-sentence has the form $\exists x \psi$, where ψ is quantifier-free.)



Many results like the decidability of algebraically closed fields can easily be shown using this criterion (Section 3.4 in [PD11]). If we assume K_2 is sufficiently saturated, then the criterion reduces to showing for every $x \in K_1 \setminus R$, there is an $\mathcal{L}_{\text{Mac}}$-embedding of $K(x)$ into K_2 over R, where K is the field of fraction of R (Theorem 2.5.4 in [PD11]).

The first thing to show in the direction of quantifier elimination in the Macintyre language would be to show that the relative algebraic closure of a common $\mathcal{L}_{\text{Mac}}$-substructure K of two models K_1 and K_2 of Σ in K_1 is isomorphic to that in K_2. Here it suffices to get an isomorphism in the language of rings, this will then automatically also be an $\mathcal{L}_{\text{Mac}}$-isomorphism. The most natural approach to this relative algebraic closure of K in K_1 (respectively K_2) would be to first pass to the henselisation of K, then to the maximal unramified extension of that, and etc. However, the problem is that the P_n-predicates may not survive these steps if n is a power of p, the residual characteristic (see Proposition 4.4 for conditions under which they do survive). On the other hand, the only place where those predicates are needed is for passing to the relative (p-)divisible hull of the value group and for making the residue field perfect. So the idea is to carry out these two steps first and only after that pass to the henselisation, then to the maximal unramified extension of that, and etc. The picture below provides a suggested route for taking those steps in turn.



Remark 4.2. Some key observations and intermediate steps behind this picture:

1. The usage of the unary predicate $\mathcal{O}$ does not behave so well in the substructures. So instead we should use the Macintyre language $\mathcal{L}_{\mathrm{Mac}} = \mathcal{L}_{\mathrm{ring}} \cup \{|\} \cup \{P_n\}_{n\in\mathbb{N}}$, where P_n is the Macintyre power predicate, $P_n(x)$ iff $\exists y(x = y^n)$. And $|$ is the binary divisibility predicate using elements in the valuation ring $a|b$ iff $b = ac$ for some $c \in \mathcal{O}$, or equivalently, $a|b$ iff $v(a) \leq v(b)$. The exact axioms $|$ has to satisfy is the following list (Section 4.4 in [PD11]):

   (a) $1|0$ but $0 \not| 1$.

   (b) $|$ is a weak linear order (antisymmetry not satisfied).

   (c) $x|y$ implies $xz|yz$.

   (d) $x|y$ and $x|z$ implies $x|y + z$.

   With the divisibility, we can define the valuation ring as $\mathcal{O} = \{x \in K \mid 1|x\}$.

   The advantage of using divisibility instead of valuation ring predicate is the following (extending Lemma 4.4.1 in [PD11]): An $\mathcal{L}_{\mathrm{ring}}$-substructure of a field is an integral domain, but if it also equipped with such divisibility relation, then there is a unique extension of the divisibility to its quotient field, so we can pass from the common substructure R, which is a ring in $\mathcal{L}_{\mathrm{Mac}}$, to its field of fractions K. This result is also stated in Lemma 4.2.

2. We can further pass from K to the henselization K^{h}. However, the extra assumptions we found in Proposition 4.4 can cause some trouble about the

Macintyre power predicates. So instead we go to the maximal ramified extension to make the value group divisible first then do the henselization step. We will use topological arguments here because K is dense in K^{h} and we may use elements in K to represent elements in K^{h} modulo n-th powers. Hensel's lemma will be used because it is a natural tool given by the henselization. Then we pass it to the maximal unramified extension to make the residue field algebraically closed.

3. We will deal with purely wild extension in the next step from $K^{\mathrm{ram,h,uram}}$ to the relative algebraic closure. Here we only had a few tools and theorems. But we shall nonetheless try to harvest some results from them.

4. All previous steps are algebraic extensions. The goal of the algebraic step is to show that the relative algebraic closure of K in K_1 and in K_2 are isomorphic. The final step is passing from the relative algebraic closure to K_i. This is a transcendental extension. However we remain optimistic because proving a simple transcendental step should be sufficient to prove the general case.

Now we begin the proof of each step. First we have the following simple step:

Lemma 4.3. If R is an integral domain with a divisibility binary relation $|$, then there is a unique extension of $|$ into its field of quotients (Lemma 4.4.1 in [PD11]). The Macintyre predicates also survive, i.e., they extend uniquely to the field of quotients. We write K for this quotient field.

Proof. We define $\frac{a}{b}|\frac{c}{d}$ iff $ad|bc$. Then it is well defined and extends the original relation. Any relation satisfies the divisibility also has this property. Hence it is the unique extension. The Macintyre predicates also extend uniquely because, for any elements $a, b \in R$, $P_n(\frac{a}{b})$ holds in K iff $P_n(ab^{n-1})$ holds in R. □

Next we discuss the purely ramified extension K^{ram}/K where we pass to the relative divisible hull of the value group of K inside the value group of K_1 and K_2 by adjoining n-th roots of certain elements whose value is n-divisible in K_i, but not in K, is unique up to isomorphism, given the Macintyre power predicates on K.

Next step is the henselization $K^{\mathrm{ram,h}}$. By general valuation theory, the henselization subextension is unique up to isomorphism as valued field, so the divisibility relation survives. In order to show the Macintyre predicates also survive in this step, it suffices to show that for every prime power q^k, every coset in $(K^{\mathrm{ram,h}})^\times/((K^{\mathrm{ram,h}})^\times)^{q^k}$ can be represented by elements in K^{ram}.

Proposition 4.4. Let (K, v) be a valued field with henselization K^{h}. Let q be a prime number with $q \neq \mathrm{char}(K)$, and in case $q = \mathrm{char}(K_v)$ is the residual

characteristic, assume that v has no proper coarsening of residual characteristic q. Let $k > 0$ be an integer. Then the canonical map

$$\rho_k : K^\times/(K^\times)^{q^k} \to (K^{\mathrm{h}})^\times/((K^{\mathrm{h}})^\times)^{q^k} \tag{18}$$

is surjective.

Proof. Let us first assume that we have proved the proposition for $k = 1$. Then, if $k > 1$ and ρ_{k-1} is assumed to be surjective, it is easy to see that ρ_k is surjective as well: Pick any $x \in (K^{\mathrm{h}})^\times$, then as ρ_1 is assumed to be surjective, we find $a \in K^\times$ with $x = ay^q$ for some $y \in (K^{\mathrm{h}})^\times$, and as ρ_{k-1} is assumed to be surjective, we find $b \in K^\times$ with $y = bz^{q^{k-1}}$ for some $z \in (K^{\mathrm{h}})^\times$, but then $x = (ab^q)z^{q^k}$ and so $\rho_k(\overline{ab^q}) = \overline{x}$, where $\overline{x}$ denotes the multiplicative class modulo q^k-th power. Thus, by induction, we have shown that ρ_k is surjective for all k.

So it remains to prove the proposition for $k = 1$. Let us first deal with the easy case that $q \neq \mathrm{char}(K_v)$. In that case $1 + \mathfrak{m}_{v^{\mathrm{h}}} \subseteq ((K^{\mathrm{h}})^\times)^q$ by Hensel's lemma. As K^{h}/K is an immediate extension, we find given any $x \in (K^{\mathrm{h}})^\times$, some $a \in K$ with $x \in a(1 + \mathfrak{m}_{v^{\mathrm{h}}})$, and so, by the above, $x \in a((K^{\mathrm{h}})^\times)^q$.

Now assume $k = 1$ and $q = \mathrm{char}(K_v)$. Then $\mathrm{char}(K) = 0$. Let us also first assume that v is of (archimedean) rank 1. In that case K is dense in K^{h} and so any $x \in (K^{\mathrm{h}})^\times$ can be approximated by some $a \in K^\times$ such that $x \in a(1+q^2\,\mathfrak{m}_{v^{\mathrm{h}}})$. By Hensel's lemma, $1 + q^2\,\mathfrak{m}_{v^{\mathrm{h}}} \subseteq ((K^{\mathrm{h}})^\times)^q$: Pick $y \in \mathfrak{m}_{v^{\mathrm{h}}}$ and consider the polynomial $f(X) = X^q - (1 + q^2y)$, then $v(f(1)) = v(q^2y) > 2v(q) = 2v(f'(1))$. Hence $x \in ((K^{\mathrm{h}})^\times)^q$ and we are done.

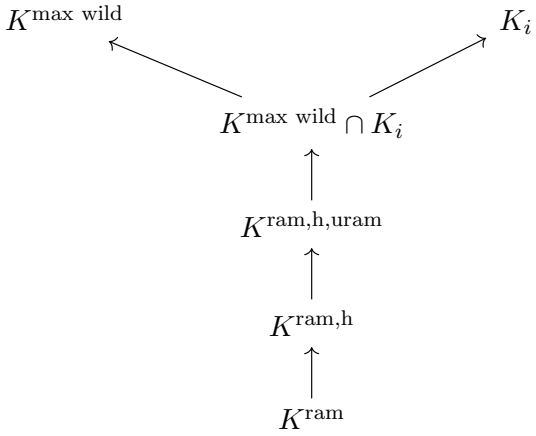
Finally, let $k = 1$, $q = \mathrm{char}(K_v)$, and v of arbitrary rank. Let w be the coarsening of v with $\mathcal{O}_w = \mathcal{O}_v[\frac{1}{q}]$. Then, as v has no proper coarsening of residual characteristic q (by assumption), v induces a rank-1 valuation $\overline{v}$ on K_w of mixed characteristic $(0, q)$. Moreover, $\mathfrak{m}_w \subsetneq \mathfrak{m}_v \subsetneq \mathcal{O}_v \subsetneq \mathcal{O}_w$ and $K^{\mathrm{h},w} \subsetneq K^{\mathrm{h},v}$, so

$$K^\times/(K^\times)^q \xrightarrow{\rho_w} (K^{\mathrm{h},w})^\times/((K^{\mathrm{h},w})^\times)^q \xrightarrow{\overline{\rho}} (K^{\mathrm{h},v})^\times/((K^{\mathrm{h},v})^\times)^q \tag{19}$$

By the $q \neq \mathrm{char}(K_v)$ case, ρ_w is surjective, so for the surjectivity of $\rho = \overline{\rho} \circ \rho_w$, it suffices to show that $\overline{\rho}$ is surjective. So pick $x \in K^{\mathrm{h},v}$ and observe that $K^{\mathrm{h},v} = (K^{\mathrm{h},w})^{\mathrm{h},v}$. As $K^{\mathrm{h},v}/K$ is immediate, we may assume that $x \in 1 + \mathfrak{m}_{v^{\mathrm{h}}} \subseteq \mathcal{O}^\times_{v^{\mathrm{h}}} \subseteq \mathcal{O}^\times_w$ and so $\overline{x}^w \in (K_w^{\mathrm{h},\overline{v}})^\times$. By the rank-1 case applied to $(K_w, \overline{v})$, there is some $y \in K^{\mathrm{h},w}$ such that $\overline{x}^w \in \overline{y}^w((K_w^{\mathrm{h},\overline{v}})^\times)^q$. Notice that $K_w^{\mathrm{h},\overline{v}} = (K^{\mathrm{h},v})_w$. Hence $x \in y(1 + \mathfrak{m}_w)((K^{\mathrm{h},v})^\times)^q = y((K^{\mathrm{h},v})^\times)^q$, which completes the proof. □

By the same reasoning of the extension K^{ram}/K we can make the residue field perfect by adjoining suitable p^k-th roots of elements to $K^{\mathrm{ram,h}}$. And by general valuation theory, the purely inert extension $K^{\mathrm{ram,h,uram}}/K^{\mathrm{ram,h}}$ is also unique up to isomorphism as valued field.

Now we have the following picture (isomorphism up to $K^{\mathrm{ram,h,uram}}$):



We mentioned before that it is sufficient to prove the simple transcendental step if we had completed the algebraic step. To elaborate on this, suppose that $K \subseteq K_i$ is a relatively algebraically closed $\mathcal{L}_{\text{Mac}}$-substructure. Let $x \in K_1 \setminus K$, then $K(x)/K$ is a purely transcendental extension. We expect to be able to realize the $\mathcal{L}_{\text{Mac}}$-type of x over K in K_2, say by x', by showing that this type is finitely realizable in K and then using that K_2 is saturated. The isomorphism respects the Macintyre predicates simply because it is a valued field isomorphism. Then we may repeat the process of such algebraic-transcendental steps to get the full isomorphism. Now the only gap left to be filled is the step of maximal wild extension. We hope the following theorem by Kaplansky [Kap42] [Kap45] [KPR86] can be used to prove this:

Theorem 4.5 (Kaplansky)**.** If a valued field (K, v) satisfies the following conditions:

1. (K, v) is henselian with $\operatorname{char} K_v = p > 0$.
2. The value group is p-divisible: $\Gamma_v = p\Gamma_v$.
3. The residue field K_v has no degree p-divisible extension.

Then the maximal algebraic immediate purely wild extension of K is unique up to isomorphism.

One possible direction is the following. Let w be the coarsest coarsening of v with residue characteristic p. Let $\overline{v}$ be the valuation induced by v on $K_w^{\text{ram,h,uram}}$. If $K^{\text{max wild}} \cap K_i$ induces a maximal wild extension on $K_w^{\text{ram,h,uram}}$ via $\overline{v}$. Then by Kaplansky, it is unique up to isomorphism. However we do not know if the conditions are satisfied in our case, nevertheless this statement is the most plausible one to postulate. This will certainly serve as a bedrock for further development and investigation. We also hope that the explicit axiomatization

for v being the canonicial p-henselian valuation as in [JK15] will be useful for this last algebraic step.

Note that in this last remaining algebraic step it suffices to show that the relative algebraic closure of $K^{\mathrm{ram,h,uram}}$ in K_1 is isomorphic to that in K_2 over $K^{\mathrm{ram,h,uram}}$ where the isomorphism is just a valued field isomorphism: it will then automatically be an $\mathcal{L}_{\mathrm{Mac}}$-isomorphism because any relatively algebraically closed subfield is an $\mathcal{L}_{\mathrm{Mac}}$-substructure in a unique way. So even if our isomorphism for $K^{\mathrm{ram,h,uram}}$ was not an $\mathcal{L}_{\mathrm{Mac}}$-isomorphism a priori, it will become one in retrospective.

5 Acknowledgement

I would like to express sincere gratitude to my supervisor Prof. Jochen Koenigsmann for bringing me this problem and helping me understand it. I am also thankful for the very detailed suggestions and insights given by Dr. Sylvy Anscombe and Dr. Jamshid Derakhshan.

References

[AK65a] James Ax and Simon Kochen. "Diophantine problems over local fields I". In: *American Journal of Mathematics* 87.3 (1965), pp. 605–630.

[AK65b] James Ax and Simon Kochen. "Diophantine problems over local fields II. A complete set of axioms for p-adic number theory". In: *American Journal of Mathematics* 87.3 (1965), pp. 631–648.

[AK66] James Ax and Simon Kochen. "Diophantine problems over local fields: III. Decidable fields". In: *Annals of Mathematics* (1966), pp. 437–456.

[Bél11] Luc Bélair. "Panorama of p-adic model theory". In: *Annales des sciences mathématiques du Québec.* 2011.

[DM16] Jamshid Derakhshan and Angus Macintyre. "Model Completeness for Henselian Fields with finite ramification valued in a Z-Group". In: *arXiv preprint arXiv:1603.08598* (2016).

[Dri14] Lou van den Dries. "Lectures on the model theory of valued fields". In: *Model Theory in Algebra, Analysis and Arithmetic.* Springer, 2014, pp. 55–157.

[EP05] Antonio J Engler and Alexander Prestel. *Valued fields.* Springer Science & Business Media, 2005.

[Eršo67] Ju L Eršov. "On the elementary theory of maximal normed fields. III". In: *Algebra i Logika Sem.* 6.3 (1967), pp. 31–38.

[Göd31] Kurt Gödel. "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I". In: *Monatshefte für mathematik und physik* 38.1 (1931), pp. 173–198.

[Gou03] Fernando Gouvea. *p-adic Numbers: An Introduction*. Springer Science & Business Media, 2003.

[Hen97] Kurt Hensel. "Über eine neue Begründung der Theorie der algebraischen Zahlen." In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 6 (1897), pp. 83–88.

[Hon13] Jizhan Hong. "Definable non-divisible Henselian valuations". In: *Bulletin of the London Mathematical Society* (2013), bdt074.

[JK15] Franziska Jahnke and Jochen Koenigsmann. "Uniformly defining p-henselian valuations". In: *Annals of Pure and Applied Logic* 166.7 (2015), pp. 741–754.

[Kap42] Irving Kaplansky. "Maximal fields with valuations". In: *Duke Math. J.* 9.2 (June 1942), pp. 303–321.

[Kap45] Irving Kaplansky. "Maximal fields with valuations, II". In: *Duke Math. J.* 12.2 (June 1945), pp. 243–248.

[Kob77] Neal Koblitz. "P-adic numbers". In: *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer, 1977, pp. 1–20.

[Koe04] Jochen Koenigsmann. "Elementary characterization of fields by their absolute Galois group". In: *Siberian Advances in Mathematics* 14.3 (2004), pp. 16–42.

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

[KPR86] Franz-Viktor Kuhlmann, Matthias Pank, and Peter Roquette. "Immediate and purely wild extensions of valued fields". In: *manuscripta mathematica* 55.1 (1986), pp. 39–67.

[Kun09] Kenneth Kunen. *The foundations of mathematics*. College Publications London, 2009.

[Mac76] Angus Macintyre. "On definable subsets of p-adic fields". In: *The Journal of Symbolic Logic* 41.03 (1976), pp. 605–610.

[MF93] Yuri V Matiyasevich and Jens Erik Fenstad. *Hilbert's tenth problem*. Vol. 105. MIT press Cambridge, 1993.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 1999.

[Poo03] Bjorn Poonen. "Hilbert's Tenth Problem over rings of number-theoretic interest". In: *Note from the lecture at the Arizona Winter School on "Number Theory and Logic* (2003).

[PD11] Alexander Prestel and Charles Delzell. *Mathematical logic and model theory: A brief introduction*. Springer Science & Business Media, 2011.

[PR84] Alexander Prestel and Peter Roquette. *Formally p-adic fields*. Springer, 1984.

[RZ00] Luis Ribes and Pavel Zalesskii. "Profinite groups". In: *Profinite Groups*. Springer, 2000, pp. 19–77.

[Rob00] Alain M Robert. *A Course in p-adic Analysis*. Vol. 198. Springer Science & Business Media, 2000.

[RZ60] Abraham Robinson and Elias Zakon. "Elementary properties of ordered abelian groups". In: *Transactions of the American Mathematical Society* 96.2 (1960), pp. 222–236.

[Rob49] Julia Robinson. "Definability and decision problems in arithmetic". In: *The Journal of Symbolic Logic* 14.2 (1949), pp. 98–114.

[Tar51] Alfred Tarski. "A decision method for elementary algebra and geometry". In: *Quantifier elimination and cylindrical algebraic decomposition*. Springer, 1951, pp. 24–84.

[Yan98] Song Y Yan. *An introduction to formal languages and machine computation*. World Scientific, 1998.