MODEL COMPLETENESS FOR HENSELIAN FIELDS WITH FINALTE RAMIFICATION VALUED IN A Z-GROUP

JAMSHID DERAKHSHAN, ANGUS MACINTYRE

Abstract. We prove that the theory of a Henselian valued field of characteristic zero, with finite ramification, and whose value group is a Z-group, is model-complete in the language of rings if the theory of its residue field is model-complete in the language of rings. We apply this to prove that every infinite algebraic extension of the field of p-adic numbers \( \mathbb{Q}_p \) with finite ramification is model-complete in the language of rings. For this, we give a necessary and sufficient condition for model-completeness of the theory of a perfect pseudo-algebraically closed field with pro-cyclic absolute Galois group.

1. Introduction

Model completeness for the theory of p-adic numbers \( \mathbb{Q}_p \) in the language of rings follows from the theorem of Macintyre [9] on quantifier elimination for \( \mathbb{Q}_p \) in the Macintyre language. For a finite extension of \( \mathbb{Q}_p \), model-completeness in the ring language can be deduced from a theorem of Prestel and Roquette [10, Theorem 5.1, pp. 86] on model-completeness in the Prestel-Roquette language combined with an existential definition of the valuation ring in the ring language due to Béral [2]. The language of Prestel-Roquette involves certain constant symbols and a symbol for the valuation. However, the proof of the theorem of Prestel-Roquette gives model completeness in the language of rings. Model-completeness for a finite extension of \( \mathbb{Q}_p \) in the language of rings has also been deduced in [3] from model-completeness for the groups of multiplicative residue classes of the field which follows from model-completeness for certain pre-ordered abelian groups which we call finite-by-Preburger groups. (Curiously, the model-completeness in the ring language for a finite extension of \( \mathbb{Q}_p \) was not observed till [5]). In this paper, we shall prove a general model-completeness result for Henselian fields, and apply it to certain infinite extensions of \( \mathbb{Q}_p \).

Let us recall that an ordered abelian group is called a Z-group if it is elementarily equivalent to \( \mathbb{Z} \) as an ordered abelian group. Let \( K \) be a valued field with valuation \( v \) and residue field \( k \). The (absolute) ramification index \( e \) of \( K \) is defined to be the cardinality of the set if elements \( \gamma \) such that \( 0 < \gamma \leq v(p) \) if \( k \) has characteristic \( p > 0 \), and defined to be 0 if \( k \) has characteristic 0. If \( e < \infty \), we say that \( K \) is finitely ramified or has finite ramification \( e \). If \( e = 0 \) or \( e = 1 \), we say that \( K \) is unramified. For example, the extension of \( \mathbb{Q}_p \) got by adjoining an \( e \)th root of \( p \), has

Key words and phrases. model theory, model completeness, Henselian valued fields.

\(^1\)Supported by a Leverhulme Emeritus Fellowship.
ramification index \( e \), whereas an extension of \( \mathbb{Q}_p \) got by adjoining roots of unity of order prime to \( p \) is unramified.

Our main result is the following.

1. **Theorem.** Let \( K \) be a Henselian valued field of characteristic zero with finite ramification. Suppose the value group of \( K \) is a \( \mathbb{Z} \)-group. If the theory of the residue field of \( K \) is model-complete in the language of rings, then the theory of \( K \) is model-complete in the language of rings.

In the case when the residue field of \( K \) has characteristic zero, the result is a well-known consequence of the Ax-Kochen-Ershov theory and was worked out in detail by Ziegler in [7]. Thus we shall assume that the residue field \( k \) has characteristic \( p > 0 \).

2. **Theorem.** Let \( K \) be an infinite algebraic extension of \( \mathbb{Q}_p \) with finite ramification. Then the theory of \( K \) in the language of rings is model-complete.

(The case of finite extensions of \( \mathbb{Q}_p \) is discussed earlier). Let us recall that a field \( K \) is called pseudo-algebraically closed if every absolutely irreducible variety defined over \( K \) has a \( K \)-rational point. To deduce Theorem 2 from Theorem 1 we prove the following result which gives a necessary and sufficient condition for model-completeness in the ring language of the theory of perfect pseudo-algebraically closed fields with pro-cyclic absolute Galois group. Given a field \( K \), we denote the absolute Galois group of \( K \) by \( \text{Gal}(K) \).

3. **Theorem.** Let \( K \) be a perfect pseudo-algebraically closed field such that \( \text{Gal}(K) \) is pro-cyclic. Let \( k \) denote the prime subfield of \( K \). Then the theory of \( K \) in the language of rings is model-complete if and only if

\[
K^{\text{alg}} = K \otimes_{\text{Abs}(K)} k^{\text{alg}},
\]

that is, every finite algebraic extension of \( K \) is generated by elements that are algebraic over \( k \).

To prove Theorem 3 we use the elementary invariants given by Cherlin-van den Dries-Macintyre [4] for the theory of pseudo-algebraically closed fields (using a model theory for \( G(K) \) dual to that of \( K \)) generalizing Ax’s work for the pseudo-finite case [1].

By the Lang-Weil estimates or the theorem of André Weil on the Riemann hypothesis for curves over finite fields, any infinite algebraic extension \( K \) of \( \mathbb{F}_p \) is pseudo-algebraically closed (see [6, Corollary 11.2.4] for details). For such a \( K \), \( \text{Gal}(K) \) is pro-cyclic (see [6, chapter 1]). Thus Theorem 2 follows from Theorem 3 and Theorem 1.

2. **Proof of Theorem 1**

Let \( K \) be a valued field. We shall denote the valuation on \( K \) by \( v_K \) or \( v \), the ring of integers of \( K \) by \( \mathcal{O}_K \), the valuation ideal by \( \mathcal{M}_K \), and the value group by \( \Gamma_K \) or \( \Gamma \). We denote the residue field by \( k \).
Assume throughout that $K$ has characteristic zero and residue characteristic $p > 0$. We take the smallest convex subgroup $\Delta$ of $\Gamma_K$ containing $v(p)$ and consider the quotient $\Gamma_K/\Delta$ with the ordering coming from convexity of $\Delta$ (see [11]). $K$ carries a valuation which is the composition of $v_K$ with the canonical surjection $\Gamma_K \rightarrow \Gamma_K/\Delta$. This valuation will be denoted by $\hat{v} : K \rightarrow \Gamma_K/\Delta \cup \{\infty\}$ and is called the coarse valuation corresponding to $v$. We denote the valued field $(K, \hat{v})$ by $\hat{K}$. The valuation ring of $\mathcal{O}_K$ of $\hat{v}$ is the set $\{x \in K : \exists \delta \in \Delta (v(x) \geq \delta)\}$. It is also the smallest overring of $\mathcal{O}_K$ in which $p$ becomes a unit, or the localization of $\mathcal{O}_K$ with respect to the multiplicatively closed set $\{p^m : m \in \mathbb{N}\}$. The maximal ideal $\mathcal{M}_K$ of $\hat{v}$ is the set $\{x \in K : \forall \delta (v(x) > \delta)\}$. Clearly $\mathcal{M}_K \subseteq \mathcal{M}_K$. The residue field of $K$ with respect to the coarse valuation $\hat{v}$ has characteristic zero, and is called the core field of $K$ corresponding to $v$. It is denoted by $K^\circ$. The core field carries a valuation $v_0$ defined by $v_0(x + \mathcal{M}_K) = v(x)$. The valuation $v_0$ has value group $\Delta$, valuation ring $\mathcal{O}_K/\mathcal{M}_K$, maximal ideal $\mathcal{M}_K/\mathcal{M}_K$, and residue field $k$. The residue degree of $K$ is defined to be the dimension over $\mathbb{F}_p$ of the residue field $k$.

1. **Lemma.** The ramification index and residue degree of $K$ and the core field $K^\circ$ are the same.

Proof. For a proof see [10] pp. 27].

We recall that a sequence $\{a_n\}_{n \in \omega}$ of elements of a valued field is called $\omega$-pseudo-convergent if for some integer $n_0$, we have $v(a_m - a_n) > v(a_n - a_k)$ for all $m > n > k > n_0$. An element $a \in K$ is called a pseudo-limit of the sequence $\{a_n\}$ if for some integer $n_0$ we have $v(a - a_n) > v(a - a_k)$ for all $n > k > n_0$. The field $K$ is called $\omega$-pseudo-complete if every $\omega$-pseudo-convergent sequence of length $\omega$ has a pseudo-limit in the field. We shall use the following lemma.

2. **Lemma.** An $\aleph_1$-saturated valued field is $\omega$-pseudo-complete.

Proof. Obvious.

We shall need the following result on existential definability of valuation rings.

3. **Lemma.** Let $K$ be a Henselian valued field of characteristic zero, residue characteristic $p > 0$, and ramification index $e > 0$. Let $n > e$ be an integer that is not divisible by $p$. Then the valuation ring $\mathcal{O}_K$ is existentially definable by the formula $\exists y (1 + px^n = y^n)$.

Proof. This is proved in [2, Lemma 1.5, pp. 4] under the assumption of a finite residue field but the same proof goes through in the more general case as follows. Let $x \in \mathcal{O}_K$. Let $f(y) := y^n - px^n - 1$. Then $v(f(1)) > 2v(f'(1))$, so $f$ has a root in $K$ by Hensel’s Lemma. Conversely, suppose $1 + px^n$ is an $n$th power. If $v(x) < 0$, then $v(px^n) < 0$, and so $v(y) < 0$, hence $nv(y) = e + nv(x)$, thus $n$ divides $e$, contradiction to the choice of $n$. □
Note The existential definition above is uniform once one fixes $p$ and a finite bound on the ramification index $e$. In particular, for any extension $K$ of $\mathbb{Q}_p$ with ramification index $e$, the valuation ring of $K$ is defined by an existential formula of the language of rings that depends only on $p$ and $e$, and not $K$.

4. Corollary. Suppose that $K_1 \subseteq K_2$ is an extension of Henselian valued fields of characteristic $0$ and residue characteristic $p > 0$, and whose value groups are $\mathbb{Z}$-groups. Suppose that the index of ramification of $K_1$ and $K_2$ is $e$ where $0 < e < \infty$. Then

$$\mathcal{O}_{K_2} \cap K_1 = \mathcal{O}_{K_1}.$$  

Proof. First note that given a valued field $K$ of residue characteristic $p > 0$ whose value group is a $\mathbb{Z}$-group and which has ramification index $e$, we have that

$$\mathcal{M}_K = \{x \in K : x^e p^{-1} \in \mathcal{O}_K\}.$$  

Indeed, suppose that $x \in \mathcal{M}_K$. Then $ev(x) - e \geq 0$, thus since $v(p) = e$, we deduce that $x^e p^{-1} \in \mathcal{O}_K$. Conversely, suppose that $x \in K$ satisfies the condition $x^e p^{-1} \in \mathcal{O}_K$. Then $ev(x) - e \geq 0$, hence $ev(x) \geq e$, so $v(x) \geq 1$.

From this observation and the existential definability of $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ by the same formula given by Lemma 3, we deduce that the maximal ideals $\mathcal{M}_{K_1}$ and $\mathcal{M}_{K_2}$ are definable by the same existential formula (of the language of rings).

Now we can complete the proof of the Corollary. From the existential definability of $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ by the same formula we deduce that $\mathcal{O}_{K_1} \subseteq \mathcal{O}_{K_2} \cap K_1$. For the other direction, suppose that there is an element $\beta \in K_1 \cap \mathcal{O}_{K_2}$ but $\beta \notin \mathcal{O}_{K_1}$. Then $\beta^{-1} \in \mathcal{O}_{K_1}$, hence $\beta^{-1} \in \mathcal{O}_{K_2}$. Thus $\beta$ is a unit in $\mathcal{O}_{K_2}$. From $\beta \notin \mathcal{O}_{K_1}$ we deduce that $\beta^{-1} \in \mathcal{M}_{K_1}$, so $\beta^{-1} \in \mathcal{M}_{K_2}$, contradiction. This proves the corollary. □

We can now give the proof of Theorem 4. Let $K_1 \subseteq K_2$ be an embedding of models of $Th(K)$. By Corollary 4, this is an embedding of valued fields. Thus there is a natural inclusion of the residue field (resp. value group) of $K_1$ into the residue field (resp. value group) of $K_2$. We make a series of reductions.

Step 1
We may assume that $K_1$ and $K_2$ are $\aleph_1$-saturated. Indeed, we can form ultrapowers $K_1^U$ and $K_2^U$ of $K_1$ and $K_2$, for a non-principal ultrafilter $U$. If we know that $K_1^U$ is an elementary substructure of $K_2^U$, then since $K_1$ is an elementary substructure of $K_i^U$ for $i = 1, 2$, we deduce that $K_1$ is an elementary substructure of $K_2$.

Step 2
It suffices to prove that the core field $K_1^o$ is an elementary substructure of the core field $K_2^o$. To see this, note that since the coarse valued fields $K_1$ and $K_2$ have characteristic zero residue fields $K_1^o$ and $K_2^o$ respectively, and divisible torsion-free abelian value groups, and the theory of divisible torsion-free abelian groups is model-complete, by the work of Ax-Kochen-Ershov as spelled out by Ziegler [?], we deduce that the embedding of $K_1$ in $K_2$ is elementary providing the embedding of $K_1^o$ into $K_2^o$ is elementary.
Step 3
We prove the embedding of $K_1^\circ$ into $K_2^\circ$ is elementary. Since the fields $K_1$ and $K_2$ are $\aleph_1$-saturated, by Lemma 2 they are $\omega$-pseudo-complete. Thus the valued fields $K_1^\circ$ and $K_2^\circ$ are also $\omega$-pseudo-complete (since the map $\Gamma \to \Gamma/\Delta$ is order-preserving). However, these fields are valued in $\Delta$ which is canonically isomorphic to $\mathbb{Z}$. Thus $K_1^\circ$ and $K_2^\circ$ are Cauchy complete. By Lemma 1 the ramification index of $K_1^\circ$ and $K_2^\circ$ is the same as the ramification index of $K_1$ and $K_2$ which equals the ramification index of $K$ which is $e$.

By the structure theorem for complete fields with ramification index $e$ (see [12, Theorem 4, pp.37]), $K_1^\circ$ and $K_2^\circ$ are respectively finite extensions of degree $e$, obtained by adjoining a uniformizing element, of the fields $W(k_1)$ and $W(k_2)$ which are fraction fields of the rings of Witt vectors of $k_1$ and $k_2$ respectively, where $k_1$ and $k_2$ are the residue fields of $K_1^\circ$ and $K_2^\circ$ (which coincide with the residue fields of $(K_1, v_{K_1})$ and $(K_2, v_{K_2})$ respectively).

Thus $K_1^\circ = W(k_1)(\pi)$ for some uniformizing element $\pi \in K_1^\circ$. $\pi$ is the root of a polynomial

$$E(x) := x^e + c_{e-1}^e x^{e-1} + \cdots + c_e$$

that is Eisenstein over $W(k_1)$. So

$$c_j \in M_{W(k_1)}$$

for all $j$ and

$$c_e \in M_{W(k_1)} - M^2_{W(k_1)}.$$

1. Claim. $E(x)$ is Eisenstein over $W(k_2)$ and $K_2^\circ = W(k_2)(\pi)$.

Proof. The condition that $c_j$ is in the maximal ideal $M_{W(k_1)}$ is equivalent to the condition that

$$c_j^e p^{-1} \in \mathcal{O}_{W(k_1)}$$

since this condition means that $ev(c_j) - e \geq 0$, that is $ev(c_j) \geq e$, which is $v(c_j) \geq 1$; and the condition that $c_e$ is a uniformizer, i.e. that it lies in $M_{W(k_1)}$ and does not lie in $M^2_{W(k_1)}$, is equivalent to the conjunction of the statements $c_e^e p^{-1} \in \mathcal{O}_{W(k_1)}$ and $c_e^{-1} p \in \mathcal{O}_{W(k_1)}$. Indeed, the latter condition is equivalent to $-ev(c_e) + e \geq 0$, i.e. $-ev(c_e) \geq -e$, i.e., $v(c_e) \leq 1$.

By Lemma 3 the valuations on $W(k_1)$ and $W(k_2)$ are existentially definable by the same formula since these fields are absolutely unramified and $p$ is a uniformizer in both. We deduce from the preceding argument that

$$c_j \in \mathcal{O}_{W(k_2)}$$

for all $j$ and

$$c_e \in M_{W(k_2)} - M^2_{W(k_2)}.$$

Therefore $E(x)$ is an Eisenstein polynomial over $W(k_2)$, and $\pi$ remains a uniformizer in $K_2^\circ$. 

Now $K_1^\circ$ is an extension of degree $e$ of $W(k_1)$ generated by $\pi$. As $\pi$ remains a uniformizer in $K_2^\circ$ and $E(x)$ is Eisenstein over $W(k_2)$, the extension $W(k_2)(\pi)$ has degree $e$ over in $W(k_2)$. But $\pi \in K_2^\circ$ and $K_2^\circ$ has degree $e$ over $W(k_2)$ as well, so we deduce that

$$K_2^\circ = W(k_2)(\pi).$$

\[\square\]

2. Claim. The embedding of $W(k_1)$ in $W(k_2)$ is elementary.

Proof. Since $k_1$ and $k_2$ are residue fields of $K_1$ and $K_2$ for the valuation $v_K$, the embedding of $k_1$ in $k_2$ is elementary. Since $K_1$ and $K_2$ are $\aleph_1$-saturated, the fields $k_1$ and $k_2$ are also $\aleph_1$-saturated. Given any finitely many elements $a_1, \ldots, a_m$ from $W(k_1)$, there is an isomorphism from $W(k_1)$ to $W(k_2)$ fixing $a_1, \ldots, a_m$ since elements of $W(k_1)$ and $W(k_2)$ can be represented in the form $\sum_i c_i p^i$, where $c_i$ are from the residue field. The countable subfields of $k_1$ and $k_2$ form a back-and-forth system. This induces a back-and-forth system between $W(k_1)$ and $W(k_2)$, and it follows that the embedding of $W(k_1)$ into $W(k_2)$ is elementary. □

It remains to prove that the embedding of $K_1^\circ$ into $K_2^\circ$ is elementary. We interpret $W(k_i)(\pi)$ inside $W(k_i)$ (for $i = 1, 2$) in the usual way as follows. We identify $W(k_i)(\pi)$ with $W(k_i)[\pi]$. On the $e$-tuples we define addition as the usual addition on vector spaces and multiplication by

$$(x_1, \ldots, x_e) \times (y_1, \ldots, y_e) = (x_1 I_e + x_2 M_\pi + \cdots + x_e M_\pi^{e-1}),$$

where $I_e$ is the identity $e \times e$-matrix and $M_\pi$ is the $e \times e$-matrix of multiplication by $\pi$. Note that $M_\pi$ depends uniformly only on the coefficients $c_0, \ldots, c_{e-1}$ of $E(x)$. Using Claim 2, we deduce that the embedding $W(k_1)(\pi) \to W(k_2)(\pi)$ is elementary. Thus $K_1^\circ \to K_2^\circ$ is elementary. The proof of Theorem 1 is complete.

3. Model completeness for pseudo algebraically closed fields and proof of Theorem 2

Given a field $K$, the field of absolute numbers of $K$ is defined by $\text{Abs}(K) := k^{alg} \cap K$, where $k$ is the prime subfield of $K$. By a result of Ax [1], two perfect pseudo-algebraically closed fields $K_1$ and $K_2$ whose absolute Galois groups are isomorphic to $\hat{\mathbb{Z}}$ are elementarily equivalent if and only if $\text{Abs}(K_1) = \text{Abs}(K_2)$. In other words, the theory of a such a field is determined by its absolute numbers $\text{Abs}(K)$ (equivalently by the polynomials $f \in k[x]$ that are solvable in $K$).

Elementary invariants for pseudo-algebraically closed fields were given by Cherlin-van den Dries-Macintyre in [2,3] in terms of the language for profinite groups. In this case one has to preserve the degree of imperfection and the co-elementary theory defined as follows. The language CSIS for complete stratified inverse systems is a language with infinitely many sorts indexed by $\mathbb{N}$, each sort is equipped with the
group operation. The $n$th sort describes properties for the set of groups in the
inverse system which have cardinality $n$. The language has in addition symbols for
the connecting canonical maps between the groups in different sorts. Given any
profinite group $G$, the set of finite quotients of $G$ with the canonical maps between
them is a stratified inverse system. A coformula is a formula of the language CSIS.
A profinite group cosatisfies a cosentence if the associated stratified inverse system
satisfies the cosentence. A cosentence or coformula has a translation to the language
of fields. For details see [4].

For any field $K$, the Galois diagram of $K$ is defined to be the theory
$$
\{ \exists \bar{x}, \bar{y}, \bar{z}, \bar{t} \ (\varphi(\bar{x}, \bar{y}, \bar{z}, \bar{t}) \land \delta(\bar{x}, \bar{y}, \bar{z}, \bar{t})) : \\
\exists a, b, c, d \in \text{Abs}(K) \ (K \models \varphi'(a, b, c) \land \delta(a, b, c, d)) \}
$$
where $\delta(\bar{x}, \bar{y}, \bar{z}, \bar{t})$ describes the isomorphism type of the field generated by
$\bar{x}, \bar{y}, \bar{z}, \bar{t}$, and $\varphi$ is a coformula and $\varphi'$ its "translation" into the language of rings (cf. [4]).

We then have the following result.

5. **Theorem.** [4] Two pseudo-algebraically closed fields $K$ and $L$ are elementarily
equivalent if and only if $K$ and $L$ have the same characteristic and same degree of
imperfection, and $\Delta(K) = \Delta(L)$.

We also need the following results.

6. **Theorem.** [6] Infinite finitely generated fields are Hilbertian.

*Proof. See [6], Theorem 13.4.2, pp. 242.*

7. **Theorem.** (Jarden) If $L$ is a countable Hilbertian field, then the set
$$
\{ \sigma \in \text{Gal}(L) : \text{Fix}(\sigma) \text{ is pseudofinite} \}
$$
has measure 1.

*Proof. See [7], pp.76] or [6] Theorem 18.6.1,pp. 380|.

Now we can give the proof of Theorem 8. The condition [1.0.1] implies that every
finite algebraic extension $K(\alpha)$ of $K$ is generated by elements algebraic over $k$, and
thus by the primitive element theorem, by a single algebraic element $\alpha$.

Now all this is part of the theory $Th(K)$. For example, the unique extension of
$K$ of dimension $n$ is generated by a root $\alpha$ of some polynomial $f$ over $k$. Fix the
minimum polynomial $f$ of $\alpha$. Then we just say that some root of $f$ generates the
unique extension of $K$ of dimension $n$. This will be true for any $L$ with $L \equiv K$.
It follows that any embedding $L \to K_1$ of models of $Th(K)$ is regular, and thus
elementary (cf. Cherlin-van den Dries-Macintyre [4] or Jarden-Kiehne [8]).

Conversely, Suppose that [1.0.1] does not hold. We shall prove that $Th(K)$ is not
model-complete. Since $K^{alg} \neq K \otimes_{\text{Abs}(K)} k^{alg}$, there is some finite algebraic extension
$K(\alpha)$ that is not included in any $K(\beta)$, where $\beta$ is algebraic over $k$. Now consider
such a field $K(\alpha)$ of minimal dimension $d$ over $K$. $K(\alpha)$ is normal cyclic over $K$, so
$d$ is a prime $p$, otherwise, $d = p_1^{k_1} \ldots p_r^{k_r}$, where $n > 1$, and each of the degree $p_j^{k_j}$
extensions is included in some $K(\beta)$ that is algebraic over $k$, and so $K(\alpha)$ is too, contradiction. Thus $K(\alpha)$ is a dimension $p$ extension of $K$.

Now let $f$ be the minimum polynomial of $\alpha$ over $k$. Put

$$\Lambda := \text{Diag}(K) \cup \Sigma_{PAC} \cup \{\exists x \ (f(x) = 0)\} \cup \{\forall x \ (g(x) \neq 0), \ g \in \Theta\} \cup \Delta(K)$$

were $\Sigma_{PAC}$ denotes the set of sentences expressing the condition of being pseudo-algebraically closed, $\Theta$ is the set of polynomials in one variable over $k$ which are unsolvable in $K$, and $\Delta(K)$ is the Galois diagram of $K$.

3. **Claim.** $\Lambda$ is consistent.

We do a compactness argument. Consider a finite subset $\Lambda_0$ of $\Lambda$. It involves a finite set $c_0, \ldots, c_m$ from $K$ including coefficients of $f$ and a finite part of $\text{Diag}(K)$, finitely many $g_1, \ldots, g_l$ from $\Theta$, a $t$ with $f(t) = 0$, and a finite part of the Galois diagram $\Delta(K)$. Given a finite part $S$ of the Galois diagram $\Delta(K)$, $S$ contains finitely many statements describing the isomorphism types of fields generated by finitely many finite subsets $S_1, \ldots, S_k$ of $K$, and translations to the language of rings of finitely many coformulas. The translations of the coformulas involve Galois groups of finitely many finite extensions of $K$. The compositum of these is a finite Galois extension $K(T)$ of $K$, for a finite set $T$.

Note that $\text{tr.deg.}(k(\alpha, c_0, \ldots, c_m, S_0, \ldots, S_k, T)) \geq 1$, so by Theorem 6, $k' := k(\alpha, c_0, \ldots, c_m, S_0, \ldots, S_k, T)$ is Hilbertian. Note that $f$ is irreducible of dimension $p$ over $k'$. Now if we adjoin to $k'$ a root $\alpha$ of $f$, then none of $g_1, \ldots, g_l$ get a root. For if one does, that root is either in $k'$ which is impossible, or has dimension congruent to zero modulo $p$ over $k'$, and then $\alpha \in K(\beta)$, for some $\beta$ which is algebraic over $k$.

So now apply Theorem 7 to $k'$ and deduce that the set of all $\sigma \in G(k')$ such that $\text{Fix}(\sigma)$ is pseudofinite has measure 1. Note that given a polynomial $g(x)$ over $k$, the set

$$G_g := \{\sigma \in G(k') : \text{Fix}(\sigma) \text{ does not contain a root of } g\}$$

is open in $G(k')$ since $U := \text{Gal}(k'_{\text{alg}}/F)$ is a basic open set containing the identity in $G(k')$ where $F$ is the splitting field of $g(x)$, and $\sigma U \in G_g$ for any $\sigma \in G_g$. Thus the set

$$\{\sigma \in G(k') : g_1, \ldots, g_l \text{ do not have a root in } \text{Fix}(\sigma) \text{ and } \text{Fix}(\sigma) \text{ is pseudofinite}\}$$

has non-zero measure. Note that for any such $\sigma$, the fixed field $\text{Fix}(\sigma)$ contains the given finite part of $\text{Diag}(K)$, contains a root of $f$ (namely $\alpha$), and contains $T$. Thus $\text{Fix}(\sigma)$ must satisfy the finitely many given statements from the Galois diagram $\Delta(K)$ and the diagram $\text{Diag}(K)$ as these can be witnessed by finitely many elements from $S_1 \cup \cdots \cup S_k \cup T$ (by adding constants symbols). We deduce that $\text{Fix}(\sigma)$ is a model of $\Lambda_0$. Thus $\Lambda$ has a model $L$.

We need to show that $\Delta(K) = \Delta(L)$. It is obvious that $\Delta(K) \subseteq \Delta(L)$. We show that $\Delta(L) \subseteq \Delta(K)$. Suppose that $\psi \in \Delta(L)$ and $\psi \notin \Delta(K)$. Then $\psi$ involves statements on isomorphism type and translations of coformulas corresponding to a finite subset of $\text{Abs}(L)$ that does not hold for $K$. But $\text{Abs}(K) = \text{Abs}(L)$, so $\neg \psi$ holds.
for the finitely many elements of $\text{Abs}(K)$, hence $\neg \psi \in \Delta(L)$ by adding constants for the distinguished elements of $\text{Abs}(K) = \text{Abs}(L)$, which is a contradiction.

Applying Theorem 5, we deduce that $K$ and $L$ are elementarily equivalent. Clearly $K$ is not an elementary submodel of $L$. This completes the proof.

References

1. James Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR 0229613 (37 #5187)
2. Luc Bélair, *Substructures and uniform elimination for $p$-adic fields*, Ann. Pure Appl. Logic **39** (1988), no. 1, 1–17. MR 949753 (89j:03026)
3. Gregory Cherlin, Lou van den Dries, and Angus Macintyre, *Decidability and undecidability theorems for PAC-fields*, Bull. Amer. Math. Soc. (N.S.) **4** (1981), no. 1, 101–104. MR 590820 (82g:03057)
4. ________, *The elementary theory of regularly closed fields*, Preprint (1981).
5. Jamshid Derakhshan and Angus Macintyre, *Model completeness for finite-by-Presburger groups and connections to valued fields*, Preprint (2015).
6. Michael D. Fried and Moshe Jarden, *Field arithmetic*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008, Revised by Jarden. MR 2445111 (2009j:12007)
7. Moshe Jarden, *Elementary statements over large algebraic fields*, Trans. Amer. Math. Soc. **164** (1972), 67–91. MR 0302651 (46 #1795)
8. Moshe Jarden and Ursel Kiehne, *The elementary theory of algebraic fields of finite corank*, Invent. Math. **30** (1975), no. 3, 275–294. MR 0435050 (55 #8012)
9. Angus Macintyre, *On definable subsets of $p$-adic fields*, J. Symbolic Logic **41** (1976), no. 3, 605–610. MR 0485335 (58 #5182)
10. A. Prestel and P. Roquette, *Formally $p$-adic fields*, Lecture Notes in Mathematics, vol. 1050, Springer-Verlag, 1984.
11. O. F. G. Schilling, *The Theory of Valuations*, Mathematical Surveys, No. 4, American Mathematical Society, New York, N. Y., 1950. MR 0043776 (13,315b)
12. Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82c:12016)

St. Hilda’s College, Cowley Place, Oxford OX4 1DY and Mathematical Institute, University of Oxford, Andrew Wiles Building, Woodstock Road, Oxford, OX2 6GG, UK

E-mail address: derakhsh@maths.ox.ac.uk

Queen Mary, University of London, School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK

E-mail address: angus@eecs.qmul.ac.uk