MODEL COMPLETENESS FOR FINITE EXTENSIONS OF p-ADIC FIELDS

JAMSHID DERAKHSHAN AND ANGUS MACINTYRE

Abstract. We prove that the first-order theory of a finite extension of the field of p-adic numbers is model-complete in the language of rings, for any prime p.

1. Introduction

This paper proves model-completeness in the language of ring theory for each finite extension of the p-adic field $\mathbb{Q}_p$. Recall that a theory T is called *model-complete* if for any model M of T and any $n \geq 1$, any definable subset of M^n is defined by an existential formula. This concept was defined by Abraham Robinson (cf. [11]).

1. **Theorem.** *Let L be a finite extension of the field of p-adic numbers $\mathbb{Q}_p$, where p is a prime. Then the first-order theory of L in the language of rings is model-complete.*

Though we have a nagging feeling that we are neglecting something in the literature, we have not found any reference for such a model-completeness result. For $\mathbb{Q}_p$, model-completeness in the language of rings is a well-known consequence of Macintyre's quantifier elimination for p-adic fields in the Macintyre language (which is an extension of the language of rings by predicates for sets of nth powers, for all n) [9].

Quantifier elimination for a finite extension of $\mathbb{Q}_p$ was obtained by Prestel-Roquette [10] in an extension of the Macintyre language got by adding constant symbols for certain distinguished elements. However, the use of these constants does not readily give model-completeness.

Using relative quantifier elimination results of Basarab [1] and Kuhlmann [8] for the case of a fixed finite extension of $\mathbb{Q}_p$ in a many-sorted language involving sorts for higher residue ring and higher residue groups, we are reduced to proving model-completeness for these higher sorts. A key step, the model-completeness of the higher residue group sorts, is proved via defining a class of pre-ordered Abelian groups that we call finite-by-Presburger, and proving their model-completeness. We shall also interpret in such groups, each of the higher residue rings.

Given a valued field K, we shall denote the valuation by v, the valuation ring by $\mathcal{O}_K$, and the maximal ideal by $\mathcal{M}_K$. In [3], it was proved that given a finite

2000 *Mathematics Subject Classification.* Primary 03C10, 03C60, 11D88, 11U09; Secondary 11U05.

Key words and phrases. model theory, p-adic numbers, local fields, model completeness, quantifier elimination.

extension K of $\mathbb{Q}_p$, there is an existential definition of $\mathcal{O}_K$ without parameters in the ring language. In view of other results in [3] it is natural to ask if there is a universal definition of $\mathcal{O}_K$ without parameters in the ring language. Note that if we knew that the theory K is model complete, this and the existential definition of $\mathcal{O}_K$ would be immediate. In [3], a uniform parameter-free definition of $\mathcal{O}_K$ from the language of rings is given uniformly for all finite extensions of $\mathbb{Q}_p$ and all $\mathbb{F}_q((t))$ for all primes p and prime powers q (and more generally uniformly for all fields with a valuation of arbitrary rank with finite or pseudo-finite residue field). This uniform definition is not existential (however it is $\exists\forall$), and it is proved in [3] that there can not be any parameter-free uniform existential or universal definition from the language of rings. Interestingly, in our proof of Theorem 1, we first have to get the universal definition of valuation rings suggested above.

2. Proof of the Theorem

2.1. **First-order definitions of valuation rings.** We shall denote by $\mathcal{L}_{rings}$ the (first-order) language of rings with primitives $\{+, ., 0, 1\}$. Given a structure K, we let $Th(K)$ denote the $\mathcal{L}_{rings}$-theory of K, i.e., the set of all $\mathcal{L}_{rings}$-sentences that are true in K.

Let L be a finite extension of $\mathbb{Q}_p$, where p is a prime. By a theorem of F.K. Schmidt (cf. [5, Theorem 4.4.1]), any two Henselian valuation rings of L are comparable, so since L has a rank 1 valuation, it has a unique valuation ring $\mathcal{O}_L$ giving a Henselian valuation. By [3, Theorem 6], this valuation ring is defined by an existential $\mathcal{L}_{rings}$-formula $\psi(x)$. We remark that $\psi(x)$ depends on the field L. For any field K which is elementarily equivalent to L, $\psi(x)$ defines a valuation ring in K and hence a valuation.

By Krasner's Lemma (see [2, Section 1]), $L = \mathbb{Q}_p(\delta)$ for some δ algebraic over $\mathbb{Q}$, and L has only finitely many extensions of each finite dimension. This property (with the same numbers) is true for any K which satisfies $K \equiv L$.

From the Σ_1-definability of $\mathcal{O}_L$ we easily get a Σ_1-definition of the set

$$\{x : v(x) \leq 0\},$$

and of the set of units $\{x : v(x) = 0\}$. But it seems that no general nonsense argument gives a Σ_1-definition of the maximal ideal $\{x : v(x) > 0\}$.

We shall be working throughout in the language of rings, and our structures and morphisms and formulas are from this language unless otherwise stated.

Note that it is a necessary condition for model-completeness that

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

whenever $K_1 \to K_2$ is an embedding of models of $Th(L)$. We shall establish this condition for all embeddings of models of $Th(L)$. For this, we shall first prove the following lemma.

1. **Lemma.** *Let $K_1 \to K_2$ be an embedding of models of $Th(L)$. Then*

   (1) *K_1 is relatively algebraically closed in K_2,*

(2) *The valuation induced from $\mathcal{O}_{K_2}$ on K_1 is Henselian.*

Proof. We first give a proof of (1). Suppose $n = [L : \mathbb{Q}_p]$. Then $n = ef$, where e is the ramification index and f the residue field dimension (see [5],[2]). Clearly it is a first-order (but not yet visibly existential) property of $\mathcal{O}_L$ (defined by $\psi(x)$) expressed in the language of rings that the residue field has p^f elements. Thus both K_1 and K_2 have residue fields (with respect to $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$) of cardinality p^f. (Recall, of course, that we do not yet know 2.1.1, so we have no natural map of residue fields). Similarly, in both K_1 and K_2 we have that $v(p)$ is the eth positive element of the value group (a condition that can be expressed by a first-order sentence using the formula $\psi(x)$ defining the valuation).

We now argue by contradiction. Suppose K_1 is not relatively algebraically closed in K_2, then $K_1(\beta) \subset K_2$, for some β which is algebraic over K_1 of degree $m > 1$. The valuation v of K_1 defined by $\psi(x)$ has a unique extension w to $K_1(\beta)$ by Henselianity and [5, Theorem 4.4.1]. We have that $m = e'f'$, where e' is the ramification index and f' is the residue field dimension of $K_1(\beta)$ over K_1 with respect to w. (L satisfies all such equalities and so K_1 does too. All this is of course with respect to the topology defined by $\psi(x)$). Now if $f' > 1$ we may replace $K_1(\beta)$ by its maximal subfield unramified over K_1. So we can in that case assume $K_1(\beta)$ is unramified over K_1. Now K_1 has residue field $\mathbb{F}_{p^f}$, and then by Hensel's Lemma $K_1(\beta)$ contains a primitive $(p^{ff'} - 1)$th root of unity (similar arguments are used in [3]). So K_2 contains a primitive $(p^{ff'} - 1)$th root of unity. But K_2 certainly does not, since it's residue field (with respect to $\psi(x)$) is $\mathbb{F}_{p^f}$ also.

So we must have $f' = 1$, i.e. $K_1(\beta)$ is totally ramified over K_1. Now we can assume that β is a root of a monic Eisenstein (relative to $\mathcal{O}_{K_1}$) polynomial $F(x)$ over K_1. Let

$$F(x) = x^{e'} + c_1 x^{e'-1} + \cdots + c_{e'}.$$

Note that $F(x)$ can not be Eisenstein over K_2, for then it would be irreducible, and it has a root β in K_2.

Within K_1 the condition that c_j is in the maximal ideal (for $\mathcal{O}_{K_1}$!) is simply that

$$c_j^e p^{-1} \in \mathcal{O}_{K_1},$$

and the condition that $c_{e'}$ is a uniformizing element is simply that both

$$c_{e'}^e p^{-1} \in \mathcal{O}_{K_1},$$

and

$$c_{e'}^{-e} p \in \mathcal{O}_{K_1},$$

hold. Now these conditions go up into K_2 since $\psi(x)$ is a Σ_1-formula. So

$$c_j^e p^{-1} \in \mathcal{O}_{K_2}$$

for all $1 \leq j \leq e'$, and

$$c_{e'}^{-e} p \in \mathcal{O}_{K_2}.$$

Now $v(p)$ (in the sense of $\mathcal{O}_{K_2}$) is the eth positive element of the value group (true in L). So in fact each $v(c_j) > 0$ (in the sense of $\mathcal{O}_{K_2}$) for $1 \leq j \leq e'$.

Since $F(x)$ is not Eisenstein over K_2, $c_{e'}$ must fail to be a uniformizing element. But $ev(c_{e'}) = v(p)$ (in the sense of $\mathcal{O}_{K_2}$), and $v(p)$ is the eth positive element of value group for $\mathcal{O}_{K_2}$, so $c_{e'}$ does generate. So K_1 is relatively algebraically closed in K_2. This proves (1).

We now prove (2). The valuation ring of the induced valuation on K_1 is $K_1 \cap \mathcal{O}_{K_2}$, and its maximal ideal is $\mathcal{M}_{K_2} \cap K_1$. By [5, Theorem 4.1.3, pp.88], Henselianity of a valued field is equivalent to the condition that any polynomial of the form

$$f := X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0$$

where all the coefficients a_j are in the maximal ideal has a root in the field. So fix a polynomial f as above with the condition that the coefficients a_j are in the maximal ideal

$$\mathcal{M}_{K_2} \cap K_1$$

of the induced valuation. Since all a_j are in particular in $\mathcal{M}_{K_2}$, by Henselianity of K_2 and [5, Theorem 4.1.3, pp.88] we deduce that f has a root α in K_2. Since by the first part, K_1 is relatively algebraically closed in K_2, this α must lie in K_1, and by another application of [5, Theorem 4.1.3, pp.88] we deduce that K_1 is Henselian. The proof of the Lemma is complete. □

We can now prove the following.

2. **Lemma.** *Let $K_1 \to K_2$ be an embedding of models of $Th(L)$. Then*

$$\mathcal{O}_{K_2} \cap K_1 = \mathcal{O}_{K_1}. \tag{2.1.1}$$

Proof. Consider the valuation ring in K_1 induced from $\mathcal{O}_{K_2}$. By Lemma 1, it is Henselian. Since any two Henselian valuation rings in K_1 are comparable, and K_1 has rank one value group (since its value group is a $\mathbb{Z}$-group because it is elementarily equivalent to the value group of L), by [5, Theorem 4.4.1] the induced valuation on K_1 must agree with that given by $\mathcal{O}_{K_1}$ and 2.1.1 follows. □

It follows from Lemmas 1 and 2 that the valuation rings are $\forall_1$-definable uniformly for models of $Th(L)$.

2.2. **Basarab-Kuhlmann quantifier-elimination.** We shall use the results of Basarab [1] and Kuhlmann [8] on relative quantifier elimination for a given finite extension of $\mathbb{Q}_p$. It is a little bit easier to use Kuhlmann's version [8]. Basarab works with categories of valued fields. Because of the previous results on definability of valuation rings we may work with models of $Th(L)$ as above, imposing the valuation ring which is defined both existentially and universally, thereby giving automatically a category of valued fields. In Kuhlmann's language [8] there is no symbol for valuation but the valuation can be defined in the language.

Recall the ingredients of the main result in [8]. In fact only the following special case of the formalism and result is needed. We shall use some convenient notation from [1].

Let K be a valued field with $\mathcal{O}_K, \mathcal{M}_K$ as before. We suppose that K has residue characteristic $p > 0$. We denote the value group of K by Γ. For an integer $k \geq 0$, set

$$\mathcal{M}_{K,k} = \{a \in \mathcal{M}_K : v(a) > kv(p)\},$$
$$\mathcal{O}_{K,k} = \mathcal{O}_K/\mathcal{M}_{K,k},$$

a local ring, and

$$G_{K,k} = K^*/1 + \mathcal{M}_{K,k},$$

a multiplicative group. π_k denotes the canonical projection

$$\mathcal{O}_K \to \mathcal{O}_{K,k},$$

and π_k^* the canonical projection

$$K^* \to G_{K,k}.$$

Furthermore, we denote by

$$\Theta_k \subseteq G_{K,k} \times \mathcal{O}_{K,k}$$

the binary relation defined by

$$\Theta_k(x, y) \Leftrightarrow \exists z \in \mathcal{O}_K(\pi_k^*(z) = x \wedge \pi_k(z) = y).$$

We denote by $\mathcal{K}_k$ the many-sorted structure

$$(K, G_{K,k}, \mathcal{O}_{K,k}, \Theta_k).$$

Note that v is well-defined on $G_{K,k}$ and surjective to the value group Γ. Kuhlmann's language [8] for this structure is the many-sorted language

$$(\mathcal{L}_{rings}, \mathcal{L}_{groups}, \mathcal{L}_{rings}, \pi_k, \pi_k^*, \Theta_k),$$

which has a sort for the field K equipped with the language of rings, a sort for the groups $G_{K,k}$ equipped with the language of groups $\mathcal{L}_{groups}$, and a sort for the residue rings $\mathcal{O}_{K,k}$ equipped with the language of rings, for all $k \geq 0$. The language has symbols for the projection maps π_k and π_k^* and a predicate for the relation Θ_k. We call this the language of Basarab-Kuhlmann and denote it by $\mathcal{L}_{BK}$.

Note that $\mathcal{L}_{BK}$ does not have a symbol for the valuation on K and on $G_{K,k}$. However the valuation is quantifier-free definable from Θ_k.

2. **Theorem.** [8] *Let K be a Henselian valued field with characteristic zero and residue characteristic $p > 0$. Then given an $\mathcal{L}_{BK}$-formula $\varphi(\bar{x})$, there is an $\mathcal{L}_{BK}$-formula $\psi(\bar{x})$ which is quantifier free in the field sort such that for all $\bar{x}$*

$$K \models \varphi(\bar{x}) \Leftrightarrow \mathcal{K}_k \models \psi(\bar{x}).$$

Note that for $k = 0$, $\mathcal{O}_{K,k}$ is the residue field, and $G_{K,k}$ comes with an exact sequence

$$1 \to k^* \to G_{K,0} \to \Gamma \to 1.$$

We shall need a suitable description of the relation Θ_k as follows.

3. **Lemma.** *For any valued field K and $k \geq 0$,*

$$\Theta_k = \{(g, \alpha) \in G_{K,k} \times \mathcal{O}_{K,k} : (\alpha = 0 \wedge v(g) \geq k + 1) \vee (\alpha \neq 0 \wedge v(g) \leq k)\}.$$

Proof. Obvious. □

In the case that interests us, $K \equiv L$ and $[L : \mathbb{Q}_p] < \infty$, and in this case the multiplicative group of the residue field is isomorphic to the subgroup μ_{p^f-1} of (p^f-1)th roots of unity in K^*. If one has a cross-section $\Gamma \to K^*$, then $G_{K,0}$ is a subgroup of K^*, and in any case (with cross-section or not) it is elementarily equivalent to $\mu_{p^f-1} \times \Gamma$. Note that the μ_{p^f-1} factor is definable as the set of (p^f-1)-torsion elements.

So fix such an L, with its attendant numbers n, e, f with $n = ef$. For any field L such that $K \equiv L$, the value group is a $\mathbb{Z}$-group, and $v(p)$ is the eth positive element of the value group.

Now suppose $K_1 \to K_2$ is an extension of models of $Th(L)$. Let γ be a uniformizing parameter for K_1, i.e., $v(\gamma)$ is the least positive element if $v(K_1)$. By the preceding, γ is also a uniformizing element for $v(K_2)$.

4. **Lemma.** *For any $k = mv(p)$, where $m \geq 0$, the embedding of local rings*

$$\mathcal{O}_{K_1,k} \to \mathcal{O}_{K_2,k}$$

is elementary.

Proof. For any $k = mv(p)$, where $m \geq 0$, the rings $\mathcal{O}_{K_1,k}$ and $\mathcal{O}_{K,k_2}$ have the same cardinality since K_1 and K_2 have the same finite residue field, so the inclusion $\mathcal{O}_{K_1,k} \to \mathcal{O}_{K_2,k}$ is an isomorphism, and hence is elementary. □

The proof of the next lemma is harder.

5. **Lemma.** *For any $k = mv(p)$, where $m \geq 0$, the embedding of groups*

$$G_{K_1,k} \to G_{K_2,k}$$

is elementary

The proof Lemma 5 will be given in the next section. We shall deduce it from a more general theorem on model-completeness of a class of pre-ordered Abelian groups that we call finite-by-Presburger.

2.3. **Model Theory of finite-by-Presburger Abelian groups.** We consider the language of group theory with primitives $\{., 1, ^{-1}\}$, together with a symbol $\leq$ standing for pre-order. The intended structures are abelian groups G, equipped with a binary relation $\leq$ satisfying

$$\forall g\ (g \leq g),$$
$$\forall g \forall h \forall j\ (g \leq h \wedge h \leq j \Rightarrow g \leq j),$$
$$\forall g \forall h\ (g \leq h \vee h \leq g),$$
$$\forall g \forall h \forall j\ (g \leq h \Rightarrow gj \leq hj).$$

It would be natural to call such structures *pre-ordered abelian groups.*

Define $g \sim h$ to mean $g \leq h$ and $h \leq g$. This is obviously a congruence on G, and the quotient $G/\sim$ is naturally an ordered abelian group. *We restrict to the* *case when* $\{g : g \sim 1\}$ *is a finite group* H. We call such G *finite-by-ordered.* Note that the projection map

$$G \to G/\sim$$

is pre-order preserving.

6. **Lemma.** *H is the torsion subgroup of G if G is finite-by-ordered.*

Proof. $G/\sim$ is torsion free. □

Note that H is pure in G, indeed, if $g \in G$ satisfies $g^m \in H$ for some m, then $g \in H$. By [7, Theorem 7,pp.18], a pure subgroup of bounded exponent in an abelian group is a direct summand. Clearly H is of bounded exponent (being finite!), so H is a direct factor of G, so $G = H.\Gamma$, an internal direct product of subgroups, for some Γ.

Now Γ contains at most one element from each $\sim$-class, and the relation $\leq$ on Γ gives Γ the structure of an ordered abelian group. So in fact since G is the product of two pre-ordered groups, one of which H has only one $\sim$-class. So $\Gamma \cong G/H$ as ordered abelian groups.

Since G is a direct product of two pre-ordered groups, we have the following.

3. **Theorem.** *The theory of $(G, \leq)$ is determined by the theory of H and the theory of the ordered group $(G/H, \leq)$. Moreover, G is decidable if and only if $(G/H, \leq)$ is decidable.*

Proof. Follows from the Feferman-Vaught Theorem [6]. □

We would like model-completeness of $(G, \leq)$ but settle here for a special case when G/H is a model of Presburger arithmetic. Now Presburger arithmetic has quantifier elimination in the language with primitives $\{., 1, ^{-1}, \tau, P_n, \leq\}$, where . denotes multiplication, τ is a constant interpreted as the minimal positive element, $\leq$ is an ordering, and P_n is the subgroup of nth powers. Note that this is the multiplicative version of the usual formalism of Presburger arithmetic (cf. [4, Section 3.2, pp.197]).

So we augment the basic formalism of pre-ordered abelian groups with symbols τ and P_n, for all $n \geq 2$ as above, and to the axioms of pre-ordered groups we add the following set of axioms for any given finite group H. (In these axioms m denotes the exponent of H, and $Tor(G)$ the torsion subgroup of G.

i) If the relation $\leq$ is an order, then τ is the minimal positive element, and if not, then $\tau = 1$.

ii) If $g \in G$ and g has order k for some $k \in \mathbb{N}$, then k divides m (we have a sentence for each $k \geq 1$).

iii) $Tor(G) \models \sigma$, where σ denote a sentence that characterizes the group H up to isomorphism (note that this sentence exists since H is finite).

iv) If $g \in G$ satisfies $g \sim 1$, then $g \in H$.

v) G/T is totally ordered and is a model of Presburger arithmetic with τH the minimal positive element.

vi) The order $\leq$ on H is trivial (i.e. for any two $g, h \in H$ we have $g \leq h$ and $h \leq g$).

Note that given a model $\mathcal{M}$ of these axioms, H is the isomorphic to the torsion subgroup of $\mathcal{M}$ (by (iii)). Thus, given any finite group H, we obtain a theory which we denote by $\mathcal{T}_H$. Note that if $H = 1$ (the identity group!), then $\mathcal{T}_H$ is the theory of Presburger arithmetic. We call these the axioms of pre-ordered groups with torsion H and ordered Presburger quotient modulo H.

Clearly G from above enriches to a model of these axioms.

4. **Theorem.** *The theory determined by the above axioms is model-complete. It follows that $(G, \leq)$ is model-complete.*

Proof. Let $M_1 \to M_2$ be an embedding of models of the above axioms. We know as above that

$$M_2 = H.\Gamma_2$$

for some Γ_2. Let $\Gamma_1 := \Gamma_2 \cap M_1$. Then we have

$$M_1 = H.\Gamma_1.$$

Thus the embedding $M_1 \to M_2$ is the product embedding

$$H.\Gamma_1 \to H.\Gamma_2.$$

Now $H \to H$ is elementary (indeed, take $\gamma = 1$ in both copies of H), and

$$\Gamma_1 \to \Gamma_2$$

is elementary since the map

$$M_1/H \to M_2/H$$

is elementary because both ordered groups have the same minimal positive element. Therefore by the Feferman-Vaught Theorem [6] the map

$$H.\Gamma_1 \to H.\Gamma_2$$

is elementary. $\square$

2.4. **Proof of Lemma 5.** Let K be a valued field and $k \geq 0$. We first identify the torsion elements of $G_{K,k}$. Clearly these must be of the form $g(1 + \mathcal{M}_{K,k})$ where $v(g) = 0$. Note that

$$g^{p^f - 1} \in 1 + \mathcal{M}_K$$

and

$$(g^{p^f - 1})^{p^k} \in 1 + \mathcal{M}_{K,k}.$$

Thus g has (in $G_{K,k}$) order dividing $(p^f - 1)p^k$, and if

$$g \in 1 + \mathcal{M}_K,$$

then g has order dividing p^k in $G_{K,k}$. Thus the torsion subgroup of $G_{K,k}$ has order

$$(p^f - 1)(p^f)^{me} = (p^f - 1)p^{nm}.$$

Now let the embedding $K_1 \to K_2$ and k be as in Lemma 5. We have an inclusion

$$G_{K_1,k} \to G_{K_2,k},$$

and the groups $G_{K_1,k}$ and $G_{K_2,k}$ have isomorphic torsion subgroups, say H. The group $G_{K_1,k}/H$ (resp. $G_{K_2,k}/H$) is isomorphic to the value group of K_1 (resp. value group of K_2). Hence $G_{K_1,k}$ and $G_{K_2,k}$ are ordered groups satisfying the axioms in Subsection 2.3 on pre-ordered groups with torsion H and ordered quotient modulo H. Furthermore, the minimal positive elements of $G_{K_1,k}$ and $G_{K_2,k}$ are the same. Thus by Theorem 4 the embedding $G_{K_1,k} \to G_{K_2,k}$ is elementary.

1. *Remark.* In general, the theory of the structure $\mathbb{Z} \times (torsion\ subgroup)$ is not model-complete.

2.5. **Completion of proof of Theorem 1.** Let π denote an element of least positive value in K_1 (it follows that π is also an element of least positive value in K_2). We let μ denote a generator of the cyclic group consisting of the Teichmuller representatives in K_1 (and hence the same holds for μ in K_2). μ has order $p^f - 1$. As before we have $k = ef$ where f and e are respectively the residue field degree and ramification index of L over $\mathbb{Q}_p$.

An element of $\mathcal{O}_{K_1,k}$ can be written uniquely in the form

$$a + \mathcal{M}_{K_1,k},$$

where $a \in K$ can be uniquely represented as

$$\sum_{0 \leq j \leq k} c_j \pi^j$$

where c_j are either 0 or a power of μ. Similarly, an element of $\mathcal{O}_{K_2,k}$ is uniquely of the form $a + \mathcal{M}_{K_2,k}$. Now except when all $c_j = 0$, these elements map to elements of $G_{K_i,k}$ (where $i = 1, 2$) under the map

$$(\sum_{0 \leq j \leq k} c_j \pi^j + \mathcal{M}_{K_i,k}) \to (\sum_{0 \leq j \leq k} c_j \pi^j)(1 + \mathcal{M}_{K_i,k}).$$

This map is injective. Indeed, if two elements $\sum_{0 \leq j \leq k} c_j \pi^j$ and $\sum_{0 \leq j \leq k} c_j' \pi^j$ map to the same element, then their difference lies in $\mathcal{M}_{K_i,k}$, but if γ_1 and γ_2 are different powers of μ, then $v(\gamma_1 - \gamma_2) = 0$ by the usual Hensel Lemma argument that gives us the Teichmuller set, this gives a contradiction.

So we may construe the *nonzero* elements $\sum_{0 \leq j \leq k} c_j \pi^j + \mathcal{M}_{K_1,k}$ as constant elements of $G_{K_1,k}$ (and the same for $G_{K_2,k}$). We shall use the notation

$$[\sum_{0 \leq j \leq k} c_j \pi^j + \mathcal{M}_{K_1,k}]$$

for them (similarly for $G_{K_2,k}$). We have a multiplication on these elements coming from the group $G_{K_i,k}$, for $i = 1, 2$, which we denote by $\odot$. It is defined by

$$[r_1] \odot [r_2] = [r_1].[r_2],$$

where . is group multiplication in $G_{K_i,k}$. We also have an addition on these elements together with the zero element 0 coming from the ring $\mathcal{O}_{K_i,k}$, for $i = 1, 2$, which we denote by $\oplus$. It is defined by

$$[r_1] \oplus [r_2] = [r_1 + r_2].$$

We thus have a finite subset, denoted by R_1 (resp. R_2), of $G_{K_1,k}$ (resp. $G_{K_2,k}$) consisting of the nonzero elements

$$[\sum_{0\leq j\leq k} c_j\pi^j + \mathcal{M}_{K_1,k}]$$

(resp. $[\sum_{0\leq j\leq k} c_j\pi^j + \mathcal{M}_{K_1,k}]$) above together with the operations $\oplus, \odot$ satisfying

$$([r_1] \oplus [r_2]) \odot [r_3] = [r_1] \odot [r_1] \oplus [r_1] \odot [r_3],$$

and the properties that $[1]$ is the unit element of $\odot$ and $[\pi^{k+1}]$ is the zero element.

Now, for $i = 1, 2$, using Lemma 3, we can interpret in $G_{K_i,k}$ the relation Θ_k as the set Θ_k^+ of all pairs $(g, r) \in G_{K_i,k} \times R_i$ satisfying the formula

$$(r = [\pi^{k+1}] \wedge v(g) \geq k + 1)\vee$$
$$\bigvee_s (0 \leq v(g) \leq k \wedge v([s]) = v(g) \wedge r = [s])),$$

where s runs through the nonzero elements $\sum_{0\leq j\leq k} c_j\pi^j + \mathcal{M}_{K_i,k}$ from before. (In fact, the s satisfying the above is unique). Thus

$$G_{K_i,k} \times R$$

with the relation Θ_k^+ as above and with factors the two sorts is isomorphic to the structure

$$G_{K_i,k} \times \mathcal{O}_{K_i,k}$$

with the relation Θ_k and with factors the two sorts.

We can now finish the proof of model-completeness of $Th(L)$. Let $K_1 \to K_2$ be an embedding of models of $Th(L)$. We show that the embedding of K_1 in K_2 is elementary. Let $\varphi(\bar{x})$ be an $\mathcal{L}_{rings}$-formula and consider $\varphi(\bar{a})$ where $\bar{a}$ is a tuple from K_1. By Theorem 2, there is a constant $N \geq 0$ and an $\mathcal{L}_{BK}$-formula $\psi(\bar{x})$ which is quantifier-free in the field sort such that

$$Th(L) \vdash \forall\bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})).$$

Since K_1 and K_2 are models of $Th(L)$, the formula $\forall\bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$ holds in both K_1 and K_2. Hence

$$K_i \models \varphi(\bar{a}) \leftrightarrow \psi(\bar{a}),$$

where $i = 1, 2$. The subformula of $\psi(\bar{a})$ from the field sort is quantifier free and so will hold in K_1 if and only if it holds in K_2. Thus to prove that the inclusion of K_1 into K_2 is elementary, it suffices to consider the sub-formula of $\psi(\bar{a})$ involving the sorts other than the field sort. In K_i (for $i = 1, 2$), this formula is a Boolean combination of formulas of the sorts $\mathcal{O}_{K_i,k}$, formulas of the sorts $G_{K_i,k}$, and formulas involving the relation Θ_k for finitely many values of k. We claim that each subformula of $\psi(\bar{a})$ of each sort (including subformulas containing Θ_k) holds in K_1 if and only if it holds in K_2. This would imply that $\psi(\bar{a})$ holds in K_1 if and only if it holds in K_2, which implies that $\varphi(\bar{a})$ holds in K_1 if and only if it holds in K_2. To prove the claim, by Lemmas 4 and 5, the embedding of rings $\mathcal{O}_{K_1,k} \to \mathcal{O}_{K_2,k}$ and the embedding of groups $G_{K_1,k} \to G_{K_2,k}$ are both elementary for $k = m.v(p)$ and any $m \geq 0$. Using the above interpretation of $(G_{K_i,k} \times \mathcal{O}_{K_i,k}, \Theta_k)$ in $(G_{K_i,k} \times G_{K_i,k}, \Theta_k^+)$ (for $i = 1, 2$), we deduce that the embedding

$$(K_1, G_{K_1,k}, \mathcal{O}_{K_1,k}, \Theta_k) \to (K_2, G_{K_2,k}, \mathcal{O}_{K_2,k}, \Theta_k)$$

is elementary. This establishes the claim, and completes the proof.

References

1. Ş. Basarab, *Relative elimination of quantifiers for Henselian valued fields*, Ann. Pure Appl. Logic **53** (1991), no. 1, 51–74.
2. J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original. MR 911121 (88h:11073)
3. Raf Cluckers, Jamshid Derakhshan, Eva Leenknegt, and Angus Macintyre, *Uniformly defining valuation in henselian valued fields with finite or pseudofinite residue field*, Annals of Pure and Applied Logic, to appear.
4. Herbert B. Enderton, *A mathematical introduction to logic*, second ed., Harcourt/Academic Press, Burlington, MA, 2001. MR 1801397 (2001h:03001)
5. A.J. Engler and A. Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer-Verlag, 2005.
6. S. Feferman and R. L. Vaught, *The first order properties of products of algebraic systems*, Fund. Math. **47** (1959), 57–103. MR 0108455 (21 #7171)
7. Irving Kaplansky, *Infinite abelian groups*, University of Michigan Press, Ann Arbor, 1954. MR 0065561 (16,444g)
8. Franz-Viktor Kuhlmann, *Quantifier elimination for Henselian fields relative to additive and multiplicative congruences*, Israel J. Math. **85** (1994), no. 1-3, 277–306. MR 1264348 (95d:12012)
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. Abraham Robinson, *Introduction to model theory and to the metamathematics of algebra*, North-Holland Publishing Co., Amsterdam, 1963. MR 0153570 (27 #3533)

University of Oxford, Mathematical Institute, Andrew Wiles Building, Radcliffe Observatory Quarter, 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