The Journal of Symbolic Logic
Volume 66, Number 3, Sept. 2001

QUANTIFIER ELIMINATION IN TAME INFINITE p-ADIC FIELDS

INGO BRIGANDT

Abstract. We give an answer to the question as to whether quantifier elimination is possible in some infinite algebraic extensions of $\mathbb{Q}_p$ ('infinite p-adic fields') using a natural language extension. The present paper deals with those infinite p-adic fields which admit only tamely ramified algebraic extensions (so-called tame fields). In the case of tame fields whose residue fields satisfy Kaplansky's condition of having no extension of p-divisible degree quantifier elimination is possible when the language of valued fields is extended by the power predicates P_n introduced by Macintyre and, for the residue field, further predicates and constants. For tame infinite p-adic fields with algebraically closed residue fields an extension by P_n predicates is sufficient.

§1. Introduction. When the model theory of p-adic fields started around 1965, the analogy of $\mathbb{Q}_p$ with the real numbers played an important role.[1] Indeed, James Ax and Simon Kochen [1], as well as independently Yuri Ershov [3] established the decidability of the theory of p-adic numbers. Ax and Kochen set up a complete axiom system for $\mathbb{Q}_p$ in the language of valued fields and showed that it is model complete. However, the theory of $\mathbb{Q}_p$ does not admit quantifier elimination in the language of valued fields—whereas the theory of real closed fields admits elimination of quantifiers in the language of ordered fields. This is due to the fact that two p-adic closures of a given formally p-adic field are in general not isomorphic over the latter. For this reason, it is necessary to extend the language of valued fields in order to obtain quantifier elimination.

The pioneering work of Ax and Kochen included a quantifier elimination result for the theory of $\mathbb{Q}_p$ (see [2]). They extended the language by countably many functions f_n and a cross-section π.[2] In 1976, Angus Macintyre [10] was able to give an improved result by finding a language with which it is more straightforward to deal. He enlarged the language of valued fields by power predicates P_n in order to obtain elimination of quantifiers (P_n denotes the subset of n-th powers, where $n \in \mathbb{N}$). Seven years later the finding of Macintyre was generalized by Alexander Prestel and Peter Roquette [12] to finite extensions of $\mathbb{Q}_p$. They made use of P_n predicates and additional constants.

Received November 24, 1999; revised June 20, 2000.

The author is greatly indebted to Jochen Koenigsmann for helpful discussions on his work.

[1]A nice survey of p-adic model theory was given in 1986 by Macintyre [11]. Several theorems which support the analogy of $\mathbb{Q}_p$ and $\mathbb{R}$ can be found in the first chapter of [12].

[2]The function f_n maps every element of the valued field to the residue of its value modulo n. A cross-section is a homomorphism $\pi : vK \longrightarrow K^\times$ such that $v \circ \pi$ is the identity on vK.

0022-4812/01/6603-0032/$2.10

We want to extend the question of quantifier elimination by considering infinite algebraic extensions of $\mathbb{Q}_p$, which we call—in analogy to algebraic number fields—infinite p-adic fields. In their proof Prestel and Roquette essentially used the fact that the residue field of a finite extension of $\mathbb{Q}_p$ is a finite field and that the corresponding value group is discrete. This is, of course, not the case in infinite p-adic fields. While the mentioned earlier result generalized the quantifier elimination property of the theory of $\mathbb{Q}_p$ to finite extensions of it, we shall proceed—in some sense—in the opposite direction. For it will be dealt with fields which can be said to be 'closer' to the algebraic closure of $\mathbb{Q}_p$ than to $\mathbb{Q}_p$ itself. (According to a well-known result of Abraham Robinson the algebraic closure of $\mathbb{Q}_p$ admits elimination of quantifiers in the language of valued fields.) Namely, we consider those infinite p-adic fields which are tame, i.e., which admit only tamely ramified extension.

The focus is primarily on those tame fields of which the residue fields do not admit extensions of p-divisible degree (Kaplansky's condition). For in this case we are able to use an isomorphism theorem for maximal purely wild extensions (due to Kuhlmann, Pank, and Roquette), and obtain elimination of quantifiers in an acceptably extended language: The language of valued fields is enlarged by P_n predicates and further predicates and constants for the residue field (see §4). For tame infinite p-adic fields with algebraically closed residue fields it is sufficient to add the P_n predicates, i.e., to use Macintyre's language. Model completeness can be obtained in the mere language of valued fields. How to obtain quantifier elimination in the case of tame infinite p-adic fields with arbitrary residue fields will be explained in the last section. This involves profound properties of tame fields which were shown by Franz-Viktor Kuhlmann.

It should be said that we do not show quantifier elimination for the theory of *all* tame infinite p-adic fields. Rather, we prove that the theory of a given tame p-adic field admits elimination of quantifiers.

In the next section we shall explain what tame fields are and state some of their properties. §3 contains the axiom system which is used to obtain elimination of quantifiers. The following three sections give the proof of quantifiers elimination with respect to tame infinite p-adic fields with residue fields that do not admit extensions of p-divisible degree. At the end we summarize our results and explain what can be done in the case of arbitrary residue field.

§2. Tame fields. Before explaining the notion of a tame field let us recall some definitions from ramification theory. Let $(L \mid K, v)$ be a finite extension of Henselian valued fields of residue characteristic p. The value groups are denoted by vL and vK and the residue fields by $\overline{L}$ and $\overline{K}$. $L \mid K$ is said to be a *tamely ramified* extension if $[L:K] = [vL:vK] \cdot [\overline{L}:\overline{K}]$, p does not divide $[vL:vK]$, and $\overline{L} \mid \overline{K}$ is separable. (Otherwise, the extension is *wildly ramified.*) We call $L \mid K$ *inert* if $[L:K] = [\overline{L}:\overline{K}]$ and $\overline{L} \mid \overline{K}$ is separable. $L \mid K$ is a *purely wild* extension if $[vL:vK]$ is a p-power and $\overline{L} \mid \overline{K}$ is purely inseparable. An arbitrary extension of Henselian valued fields is tamely ramified, inert, or purely wild, respectively, if this holds for every finite subextension.

DEFINITION. A Henselian valued field is called a tame field if any algebraic extension of it is tamely ramified.

The value group of a tame field is always p-divisible and the residue field is perfect. A tame field can be obtained as follows. Let K be a Henselian ground field and let $E \mid K$ be a maximal purely wild extension. (Such an extension can be obtained by means of Zorn's lemma. There are in general several non-isomorphic maximal purely wild extensions of a ground field.) Then E is a tame field (this is an immediate consequence of Theorem 4.3 in [9]). The value group of E is the p-divisible closure of vK and its residue field is the perfect hull of $\overline{K}$. By definition, any algebraic extension of a tame field is again tame.

In our case, a maximal purely wild extension of $\mathbb{Q}_p$ is a tame infinite p-adic field. Its residue field is $\mathbb{F}_p$ and the value group is the p-divisible closure of $v(p)\mathbb{Z}$. Any algebraic extension of this field is a tame field. For this reason, while the finite or unramified extensions of $\mathbb{Q}_p$ could be said to be close to $\mathbb{Q}_p$ itself, the tame infinite p-adic fields are close to the algebraic closure of $\mathbb{Q}_p$.

Our proof makes use of the following isomorphism theorem concerning two maximal purely wild extensions. It was established by Kuhlmann, Pank, and Roquette, who generalized a result of Kaplansky. (See [9], Theorem 5.1. One cannot do without the assumption on the residue field.)

PROPOSITION 1. *Let K be a Henselian field whose residue field does not admit separable extensions of p-divisible degree. Then all maximal purely wild extensions of K are mutually K-isomorphic as valued fields.*

§3. The axiom system. We do not provide a single axiom system for all tame infinite p-adic fields such that this axiom system admits elimination of quantifiers in an acceptably extended language. Rather, the question is to find for every tame p-adic field an axiom system such that it admits quantifier elimination. (Similarly, Prestel and Roquette gave for every natural number d an axiom system $\Sigma_{p,d}$ such that the extensions of $\mathbb{Q}_p$ of degree d are models of $\Sigma_{p,d}$ and $\Sigma_{p,d}$ admits quantifier elimination, where the language of valued fields is extended by P_n predicates and d constants.) Elimination of quantifiers is equivalent to the fact that for any two models E and F with a common substructure K the valued fields E and F are elementarily equivalent over K: $E \equiv_K F$. This entails in particular $vE \equiv_{vK} vF$ and $\overline{E} \equiv_{\overline{K}} \overline{F}$ (in the language of ordered groups and fields, respectively). To obtain these necessary properties any of our axiom systems must include sufficient information on the residue field and the value group under consideration.

For this reason, we assign a specification F (of the residue field) and a specification Z (of the value group) to a given tame p-adic field. The axiom system for this tame field will be denoted by $\mathfrak{T}_{p,F,Z}$ and is called the theory of tame infinite p-adic fields with specified residue field and value group. These specifications can be represented by two functions F and Z which assign to every prime number q a natural number or ∞. They are defined as follows:

$$F(q) := \max_n\{n \mid \overline{K} \text{ contains a } q^n\text{-th root of unity}\}$$

$$Z(q) := \max_n\{n \mid vK \text{ contains an element of order } q^n \bmod v(p)\mathbb{Z}\}$$

The specification implies that two extensions of $\mathbb{Q}_p$ are models of the same axiom system $\mathfrak{T}_{p,F,Z}$ if and only if they have the same residue field and the same value group (over $v(p)\mathbb{Z}$). (For instance, all maximal purely wild extensions of $\mathbb{Q}_p$ belong to the same axiom system.)

The language of valued fields $(+, -, \cdot, \div, 0, 1, V)$ is used for the axiomatization in first-order logic. (We include to the language of fields a unary predicate V designating the valuation ring.) The language extension which is used to obtain elimination of quantifiers will be characterized later on.

The axiom systems $\mathfrak{T}_{p,F,Z}$ are given by the following scheme:

- (K, v) is a valued field of characteristic 0, it is Henselian and tame.
- Concerning the value group vK:
  - vK is regularly dense;
  - if $Z(q) = \infty$, then $vK = q \cdot vK$
  - otherwise $\{\frac{1}{q^{Z(q)}} v(p^i)\}_{0 \le i < q}$ is a set of representatives for vK/qvK
- Concerning the residue field $\overline{K}$:
  - if it is finite (according to F): characterization of it
  - otherwise: it is of characteristic p, perfect and PAC;
    - characterization of the purely algebraic part:
      $\max_n\{n \mid \overline{K} \text{ contains a } q^n\text{-th root of unity}\} = F(q)$;
    - characterization of the absolute Galois group:
      $\text{res} : \text{Gal}(\overline{K}) \longrightarrow \text{Gal}(\overline{K} \cap \widetilde{\mathbb{F}}_p)$ is an isomorphism

Let us explain the above outline. The property of being Henselian can be elementarily expressed by means of Hensel's lemma. As the axioms concerning the residue field and the value group include the fact that the residue field is perfect and the value group is p-divisible, in order to characterize the field as tame it is sufficient to say that every irreducible polynomial of which the degree is a p-power generates a residue field extension of the same degree.

A densely ordered, abelian group is called *regular*, if every non-empty interval contains for every natural number n an n-divisible element. (This property is used, because it is impossible to express the fact that an ordered group is archimedian in first-order logic.) In addition, we state that there is a specific set of representatives for vK/qvK. This entails that if K is a model of $\mathfrak{T}_{p,F,Z}$ contained in another model L of $\mathfrak{T}_{p,F,Z}$, then vK is divisibly closed in vL, i.e., vL/vK is torsion free. The axiom system of the value group is complete according to Robinson and Zakon. (See Theorem 4.6 of [13].)

When the residue field under consideration is not finite (according to F), then we state that it is a perfect PAC field of characteristic p. PAC is the abbreviation for *pseudo algebraically closed*. A field L is PAC if and only if every affine variety defined over L has a L-rational point. (This property can be expressed elementarily.) The Hasse-Weil theorem concerning the number of prime divisors of a function field entails that every infinite algebraic extension of a finite field is PAC. Our proof will make use of a model theoretic characterization of PAC fields: A field is PAC if and only if it is existentially closed (with respect to the language of fields) in every regular extension. Furthermore, the purely algebraic part as well as the absolute Galois group of the residue field are characterized (the latter by saying that the absolute Galois group is procyclic and by specifying whether $\overline{K}$ admits an extension of degree n or not, depending on whether the infinite algebraic extension of $\mathbb{F}_p$

defined by F admits an extension of degree n). These axioms form a complete theory of the residue field according to Theorem 18.6 of [4].

The models of our axiom system have the following properties, which will be important as far as model completeness and the reduction to relatively closed substructures are concerned:

LEMMA 2. *Let K be a model of a theory $\mathfrak{T}_{p,F,Z}$ which is contained in another model L of the same theory. Then K is algebraically closed in L, because $\overline{K}$ is algebraically closed in $\overline{L}$ and vK is divisibly closed in vL.*

Let K be a substructure of a model L of $\mathfrak{T}_{p,F,Z}$ such that K is algebraically closed in L. Then K is Henselian and tame, $\overline{K}$ is algebraically closed in the perfect field $\overline{L}$, and vK is divisibly closed in vL. (This does not imply that K is a model, since the residue field $\overline{K}$ need not be PAC.)

§4. Algebraic Isomorphism Theorem. Now we turn to the proof of quantifier elimination. First of all, those tame infinite p-adic fields whose *residue fields are p-closed* are considered. This means that the residue fields do not admit extensions of p-divisible degree (Kaplansky's condition). We primarily deal with this case because in this situation a more satisfying extension of language is sufficient (Proposition 1 can be applied). It is explained in the the last section what can be done to obtain quantifier elimination in the case of tame infinite p-fields with arbitrary residue field. (Note that an axiom system $\mathfrak{T}_{p,F,Z}$ tells us by means of the specification F whether the residue field is p-closed or not.)

As far as the case of p-closed residue field is concerned, we extend the language of valued fields $(+, -, \cdot, \div, 0, 1, V)$ by unary power predicates P_n (for every n relatively prime to the residue characteristic p), root predicates R_n of arity n (for every natural number n), and constants c_q (for every prime number q unequal to p). The set of axioms $\mathfrak{T}_{p,F,Z}$ is enlarged by the following defining sentences (the multiplicative subgroup of the residue field is abbreviated by $\overline{K}$):

- Concerning the extension by P_n and R_n predicates and c_q constants:

$$P_n(x) \longleftrightarrow \exists y\ x = y^n$$

$$R_n(a_0, \ldots, a_{n-1}) \longleftrightarrow \text{if } v(a_0) \geqslant 0, \ldots, v(a_{n-1}) \geqslant 0, \text{ then}$$

$$\exists \bar{y} \in \overline{K}\ \bar{y}^n + \bar{a}_{n-1}\bar{y}^{n-1} + \ldots + \bar{a}_0 = 0$$

$$1, \bar{c}_q, \ldots, \bar{c}_q^{q-1} \text{ form a set of representatives of } \overline{K}/\overline{K}^q$$

Let E and F be two models of $\mathfrak{T}_{p,F,Z}$ with a common substructure K in the extended language. Elimination of quantifiers means that E and F are elementarily equivalent over K. This property entails in particular that the relative algebraic closures of K in E and F are isomorphic over K. Because of the language enlargement the assumptions of the following Algebraic Isomorphism Theorem are satisfied, which yields that the relative algebraic closures of K in E and F are isomorphic (as valued fields, but also in the extended language according to Lemma 2). This means we have reduced the situation to the case where K is relatively algebraically closed in E and F.

THEOREM 3. *Let L and L' be tame fields with p-closed residue fields. Let K be a common subfield such that $L \mid K$ and $L' \mid K$ are algebraic extensions. Assume that (where n is relatively prime to p),*

i) $L^n \cap K = L'^n \cap K$,
ii) *every separable polynomial with coefficients from $\overline{K}$ has as root in $\overline{L}$ if and only if it has one in $\overline{L}'$,*
iii) *$\overline{K}$ contains a set of representatives for $\overline{L}/\overline{L}^n$ as well as for $\overline{L}'/\overline{L}'^n$.*

Then there exists a value-preserving isomorphism of L and L' over K.

PROOF. We shall proceed in four steps, following the canonical ramification theoretical subextensions. After each step image and inverse image of the isomorphism will be identified.

1. Let K_1 and K_1' be the henselizations of K in L and L', respectively. K_1 and K_1' are value-isomorphic over K. The following isomorphisms will at once be value-preserving.

2. Let K_2 and K_2' be the maximal inert subextensions of $L \mid K_1$ and $L' \mid K_1$. (A maximal inert extension is unique, because the composite of two inert extensions is inert again. K_2 is the intersection of L and the fixed field of the absolute inertia group of K_1.) $\overline{K}_2$ and $\overline{K}_2'$ are the separable closures of $\overline{K}$ in $\overline{L}$ and $\overline{L}'$ (according to Hensel's lemma). Using assumption ii) we obtain an isomorphism of $\overline{K}_2$ and $\overline{K}_2'$ over $\overline{K}_1$. Because of the separability we can apply Hensel's lemma and extend the isomorphism of the residue fields to an isomorphism of K_2 and K_2'.

3. Using assumptions i) and iii) we start by showing that $L^n \cap K_2 = L'^n \cap K_2$. According to assumption iii) we have a set of representatives for $\overline{L}/\overline{L}^n$ contained in $\overline{K}$. It is also a set of representatives for $\overline{K}_2/\overline{K}_2^n$, since n is relatively prime to the residue characteristic p and $\overline{K}_2$ is separably closed in $\overline{L}$. This means that we have $\overline{K} \cdot \overline{K}_2^n = \overline{K}_2$. Hensel's lemma and the fact that $vK = vK_2$ allows us to lift the last equation to $K \cdot K_2^n = K_2$. We conclude that $K \cdot K_2^n = K_2$ and similarly $K' \cdot K_2'^n = K_2'$. Using the assumption $L^n \cap K = L'^n \cap K$ it follows that $L^n \cap K_2 = L'^n \cap K_2$.

Let K_3 and K_3' be the maximal tamely ramified subextensions of $L \mid K_2$ and $L' \mid K_2$. (A maximal tamely ramified extension is unique, because the composite of two tamely ramified extensions is tamely ramified again. In fact, K_3 is the intersection of L and the fixed field of the absolute ramification group of K_2.) From ramification theory we know that $K_3 = K_2(t_i)_{i \in I}$ with $t_i^{n_i} = c_i \in K_2$. (This can be shown by means of Hensel's lemma and the fact that $\overline{K}_3 = \overline{K}_2$.) Using that $L^n \cap K_2 = L'^n \cap K_2$ we infer that K_3 can be embedded into L' and therefore into K_3' over K_2. Vice versa, K_3' can be embedded into K_3. This proves that K_3 and K_3' are isomorphic over K_2.

4. It remains to be shown that L and L' are isomorphic over K_3. By construction $L \mid K_3$ and $L' \mid K_3$ are purely wild. L and L' are tame and therefore admit no purely wild extensions. This means that both extensions of K_3 under consideration are maximal purely wild extensions. Since $\overline{K}_3$ is separably closed in $\overline{L}$ and $\overline{L}'$, which are p-closed, $\overline{K}_3$ does not admit separable extensions of p-divisible degree. Using Proposition 1 we finally obtain the desired isomorphism. ⊣

In the case of algebraically closed residue field not all assumptions of the foregoing theorem are needed. This will eventually enable us to carry out elimation of quantifiers in this situation by enlarging the language of valued fields only by P_n predicates.

COROLLARY 4. *Let L and L' be tame fields with algebraically closed residue fields. Let K be a common subfield such that $L \mid K$ and $L' \mid K$ are algebraic extensions. Assume that (where n is relatively prime to p)*

i) $L^n \cap K = L'^n \cap K$.

Then there exists a value-preserving isomorphism of L and L' over K.

§5. Elementary equivalence of the value groups and the residue fields. By means of the Algebraic Isomorphism Theorem we have reduced the situation to the case where E and F are two models of $\mathfrak{T}_{p,F,Z}$ (with p-closed residue fields) and K is a common substructure which is algebraically closed in E and F. According to Lemma 2 this entails that both $\overline{E} \mid \overline{K}$ and $\overline{F} \mid \overline{K}$ are regular and that vK is divisibly closed in vE and vF. In this case of relatively closed substructures it remains to be shown that E and F are elementarily equivalent over K. $E \equiv_K F$ can be proved even in the the language of valued fields; the extended language is not needed anymore.

We now show that the necessary properties $vE \equiv_{vK} vF$ and $\overline{E} \equiv_{\overline{K}} \overline{F}$ (considered in the language of ordered groups and fields, respectively) are fulfilled. In fact, the axioms of $\mathfrak{T}_{p,F,Z}$ concerning the value group and the residue field are just needed for these two statements. In the next section we shall prove how this can be transferred to an elementary equivalence property of the tame fields under consideration.

PROPOSITION 5. *Let vE and vF be two ordered groups for which the value group axioms of a specific theory $\mathfrak{T}_{p,F,Z}$ are valid. Let vK be a common substructure such that vK is divisibly closed in both vE and vF. Then $vE \equiv_{vK} vF$ (in the language of ordered groups).*

PROOF. This assertion is known from the model theory of ordered groups. See [14], for instance. ⊣

PROPOSITION 6. *Let $\overline{E}$ and $\overline{F}$ be two fields for which the residue field axioms of a specific theory $\mathfrak{T}_{p,F,Z}$ are valid. Let $\overline{K}$ be a common substructure such that $\overline{K}$ is algebraically closed in $\overline{E}$ and $\overline{F}$. Then $\overline{E} \equiv_{\overline{K}} \overline{F}$ (in the language of fields).*

PROOF. Only infinite residue fields must be considered. We show that the theory of the residue field admits quantifier elimination in the language of fields extended by $\overline{R}_n$ predicates, where $\overline{R}_n(\bar{a}_0, \dots, \bar{a}_{n-1}) \longleftrightarrow \exists \bar{y}\ \bar{y}^n + \bar{a}_{n-1}\bar{y}^{n-1} + \dots + \bar{a}_0 = 0$. That is to say that we assume that $\overline{E}$ and $\overline{F}$ are two fields for which the residue fields axioms of a specific theory $\mathfrak{T}_{p,F,Z}$ are valid and that $\overline{K}$ is a common substructure of $\overline{E}$ and $\overline{F}$ in the language extended by $\overline{R}_n$ predicates. The argument is essentially that of Koenigsmann (see Proposition 6.6 of [6]). A special case of our proposition is Theorem 2 of [5].

Because of the $\overline{R}_n$ predicates the relative algebraic closures of $\overline{K}$ in $\overline{E}$ and $\overline{F}$ are isomorphic and we may assume $\overline{K}$ to be algebraically closed in $\overline{E}$ and $\overline{F}$. In order to obtain elimination of quantifiers it is sufficient to show the following property. For every simple existential sentence $\exists x\phi$ with parameters from $\overline{K}$ the fact that $\exists x\phi$ is valid in $\overline{E}$ must entail the property that it is valid in $\overline{F}$. $\exists x\phi$ is a sentence in the language extended by $\overline{R}_n$ predicates. Nevertheless, it is equivalent to an existential sentence in the mere language of fields (with parameters from $\overline{K}$), as shown at the end of the proof.

Given this, consider $\mathrm{Quot}(\overline{E} \otimes_{\overline{K}} \overline{F})$. The fact that $\overline{E} \mid \overline{K}$ and $\overline{F} \mid \overline{K}$ are regular implies that $\overline{E} \otimes_{\overline{K}} \overline{F}$ is an integral domain containing the fields $\overline{E}$ and $\overline{F}$ canonically. In addition, the extensions $\mathrm{Quot}(\overline{E} \otimes_{\overline{K}} \overline{F}) \mid \overline{E}$ as well as $\mathrm{Quot}(\overline{E} \otimes_{\overline{K}} \overline{F}) \mid \overline{F}$ are regular. The assumption that the existential sentence under consideration is valid in $\overline{E}$ certainly entails that it is valid in $\mathrm{Quot}(\overline{E} \otimes_{\overline{K}} \overline{F})$. Since $\overline{F}$ is PAC, it is existentially closed (with respect to the language of fields) in every regular extension. This means that the considered sentence is satisfied by $\overline{F}$, as desired.

It remains to be shown that $\exists x\phi$ is equivalent to an existential sentence involving no predicates. Any occurence of the formula $\overline{R}_n(\dots)$ is by definition equivalent to an existential sentence. The negation $\neg\overline{R}_n(\dots)$ is equivalent to the fact that the polynomial of degree n under consideration is irreducible or some proper factor of it has a root. Using induction we may assume that $\neg\overline{R}_i$ and $\neg\overline{R}_{n-i}$ $(i < n)$ are already transformed as desired. Finally, the irreducibility of a polynomial $f(X)$ of degree n is equivalent to an existential sentence according to the axiomatization:

As we deal with a complete residue field theory, it is sufficient to show that such an equivalence holds in the infinite algebraic extension of $\mathbb{F}_p$ defined by F. We have to consider the case that this field, called L, admits an extension of degree n. Let $L(\alpha)$ be the unique extension of degree n and $\hat{g}$ the minimal polynomial of α over the prime field $\mathbb{F}_p$. Then the following sentence holds in L:

$$\begin{aligned} &f(X) \text{ of degree } n \text{ is irreducible} \\ &\qquad\longleftrightarrow \exists g(X) \text{ of degree } n, \exists a_0, \dots, a_{n-1} \in L \text{ such that} \\ &\qquad\qquad g(X) \mid \hat{g}(X) \text{ and } f(X) \mid g(a_{n-1}X^{n-1} + \dots + a_0) \text{ in } L(X). \end{aligned}$$

As a sentence expressing the divisibility of two polynomials is existential, the second part of the equivalence is an existential sentence, as desired. ⊣

§6. **Relative subcompleteness.** It remains to be shown that the conditions $\overline{E} \equiv_{\overline{K}} \overline{F}$ and $vE \equiv_{vK} vF$ entail $E \equiv_K F$, where K, E, and F are tame fields, vK is divisibly closed in vE and vF, and $\overline{E} \mid \overline{K}$ as well as $\overline{F} \mid \overline{K}$ are regular. This fact was already proved by Franz-Viktor Kuhlmann (he calls this property relative subcompleteness; see Theorem 14.13 of [8]). In this section, we give a proof of the relative subcompleteness of tame fields with p-closed residue fields. In the case of p-closed residue field it is possible to use arguments of our Algebraic Isomorphism Theorem, so that profound properties of tame fields are not needed.

The essential ingredient of the proof of relative subcompleteness is the following embedding property, which is analogous to that used by Ax and Kochen as well as Ershov concerning Henselian fields of residue characteristic 0.

PROPOSITION 7. *Let L and K^* be tame fields with p-closed residue field and let K be a common subfield of the same type such that (K^*, v^*) is $|L|^+$-saturated, vL/vK is torsion free and $\overline{L} \mid \overline{K}$ is separable. Then the existence of embeddings $\overline{\varphi} : \overline{L} \to \overline{K}^*$ over $\overline{K}$ and $v\varphi : vL \to vK^*$ over vK entails the existence of an embedding $\varphi : L \to K^*$ over K such that φ is compatible with $\overline{\varphi}$ and $v\varphi$.*

PROOF. (The compatibility assertion means that the embedding of vL into vK^* induced by φ is identical with the given $v\varphi$ and that the embedding of $\overline{L}$ into $\overline{K}^*$ induced by φ equals $\overline{\varphi}$.) Using Zorn's lemma we are able to reduce the situation and may assume that the transcendence degree of $L \mid K$ is at most 1. Three cases are to be distinguished:

1. $\overline{L} \mid \overline{K}$ is algebraic and vL/vK is a torsion group: As vL/vK is also torsion free, there is no value group extension. Since $\overline{L} \mid \overline{K}$ is separably algebraic the embedding $\overline{\varphi}$ of $\overline{L}$ into $\overline{K}^*$ over $\overline{K}$ can be lifted by means of Hensel's lemma. This means that we may assume that $L \mid K$ is an immediate extension. If it is transcendental, let $x \in L$ be transcendental over K. Since the tame field K does not admit any proper immediate algebraic extension, $K(x)$ can be value-preservingly embedded into the saturated structure K^* using standard arguments for immediate rational function fields (see, e.g., the proof of Proposition 4.10A in [12]). The henselization $K(x)^h$ can be embedded as well. Now there remains an immediate algebraic extension, which is in particular a purely wild extension. It can be embedded into the tame field K^* according to Proposition 1.

2. $\overline{L} \mid \overline{K}$ is transcendental: Choose an element x from L such that $\bar{x}$ is a separating transcendence base of $\overline{L} \mid \overline{K}$. We have the following minimum property in $K[x]$: $v(\sum_i a_i x^i) = \min_i\{v(a_i)\}$. To obtain a compatible embedding we choose an element x^* in K^* the residue of which is $\overline{\varphi}(\bar{x})$. As the same minimum property holds for $\overline{\varphi}(\bar{x})$, x^* is transcendental and the canonical mapping over K sending x to x^* is a value-preserving embedding of $K(x)$ into K^*. Now we proceed by embedding the henselization of $K(x)$ into K^*. The maximal tamely ramified and inert extension of this field in L can be embedded compatibly with $\overline{\varphi}$ as done in the first case. Since $L \mid K(x)$ is an algebraic extension, $vK(x) = vK$, and vL/vK is torsion free by assumption, there is no extension of value group. As $\overline{L}$ admits no separable extension of p-divisible degree, the remaining immediate extension can be embedded as in the first case.

3. vL/vK is not a torsion group: Since K^* is saturated, it is sufficient to embed every finitely generated subextension of $L \mid K$. We therefore may assume that vL is finitely generated over vK. As vL/vK is of $\mathbb{Q}$-rank 1, there is an $x \in L$ such that $vL = vK \oplus \mathbb{Z}v(x)$. The following minimum property holds: $v(\sum_i a_i x^i) = \min_i\{v(a_i x^i)\}$. We choose an element x^* in K^* such that $v^*(x^*) = v\varphi(vx)$. Since x^* has the same minimum property, the canonical mapping over K sending x to x^* is value-preserving. The remaining algebraic part $L \mid K(x)$ can be embedded as done in the second case, because $vK(x) = vL$. This accomplishes our proof. ⊣

Using standard model theoretic methods the foregoing proposition yields relative subcompleteness:

PROPOSITION 8. *Let E and F be two tame fields with a common tame subfield K such that $\overline{E} \mid \overline{K}$ is separable and vE/vK is torsion free. If an embedding property like that of the foregoing proposition holds, then the conditions $\overline{E} \equiv_{\overline{K}} \overline{F}$ and $vE \equiv_{vK} vF$ imply the elementary equivalence of E and F over K: $E \equiv_K F$.*

§7. The results. Collecting the results of the three preceding sections, we finally obtain the desired quantifier elimination property in the case of p-closed residue field:

THEOREM 9. *Every theory* $\mathfrak{T}_{p,F,Z}$ *of tame infinite p-adic fields with specified p-closed residue field and specified value group admits elimination of quantifiers in the language of valued fields extended by* P_n, R_n *predicates and* c_q *constants.*

If we consider tame infinite p-adic fields with algebraically closed residue fields, the language of valued fields must only be extended by P_n predicates, where n is relatively prime to p (use Corollary 4 instead of Theorem 3). This means that the language used by Macintyre with respect to $\mathbb{Q}_p$ is sufficient in this case.

THEOREM 10. *Every theory* $\mathfrak{T}_{p,F,Z}$ *of tame infinite p-adic fields with algebraically closed residue field and specified value group admits elimination of quantifiers in the language of valued fields extended by* P_n *predicates.*

As far as model completeness is concerned, there is no need for an extended language, because we have the situation of relatively closed substructures (according to Lemma 2) and do not need the Algebraic Isomorphism Theorem.

THEOREM 11. *Every theory* $\mathfrak{T}_{p,F,Z}$ *of tame infinite p-adic fields with specified p-closed residue field and specified value group is model complete in the language of valued fields.*

The presented theory $\mathfrak{T}_{p,F,Z}$ is, however, not complete. A complete theory (in the language of valued fields) can be obtained by enlarging the axiom $\mathfrak{T}_{p,F,Z}$ system by a specification of the purely algebraic part, i.e., for a considered tame infinite p-adic field we add axioms which state for every polynomial with coefficients from $\mathbb{Z}$ whether it has a root or not.

Up to now we have restricted our study to tame infinite p-adic fields with p-closed residue fields. In this case we were able to use Proposition 1 in the proofs of Theorem 3 and Proposition 7. The embedding property (Proposition 7) is valid also in the case of tame fields with arbitrary residue field. In order to obtain this result we need the following two properties of tame fields, which were proved by Kuhlmann (Theorem 7.1 and Theorem 3.1 of [7].)

PROPOSITION 12. *Immediate function fields of transcendence degree* 1 *over tame fields are Henselian rational. I.e., if K is a tame field and* $L \mid K$ *is a function field of transcendence degree* 1, *then there is an* $x \in L$ *such that the henselization of L is identical with that of* $K(x)$: $K(x)^h = L^h$.

PROPOSITION 13. *A function field without transcendence defect over a defectless field is again defectless. I.e., if K is a valued field such that for every finite extension the equation* $n = ef$ *holds and if* $L \mid K$ *is a function field such that the transcendence degree of* $L \mid K$ *is equal to the sum of the transcendence degree of* $\overline{L} \mid \overline{K}$ *and the* $\mathbb{Q}$-*rank of* vL/vK, *then L has the same ramification theoretical property as K.*

Using these two propositions in the proof of Proposition 7 yields

THEOREM 14. *The embedding property of* Proposition 7 *also holds in the case of arbitrary residue field. Therefore, the subcompleteness as stated in* Proposition 8 *is valid for tame fields in general. In particular, every theory* $\mathfrak{T}_{p,F,Z}$ *of tame infinite p-adic fields with specified residue field and specified value group is model complete in the language of valued fields.*

As far as quantifier elimination is concerned, we did not suceed in providing an algebraic isomorphism theorem by means of an acceptably slight extension of language. It is, of course, sufficient to use W_n predicates of arity n defined as follows $(n \in \mathbb{N})$.

- Concerning the language extended by W_n predicates:

$$W_n(a_0, \dots, a_{n-1}) \longleftrightarrow \exists x\ x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0.$$

Using these predicates we have an isomorphism result as that of Theorem 3 and obtain elimination of quantifiers according to the subcompleteness assertion of the foregoing theorem.

THEOREM 15. *The theory $\mathfrak{T}_{p,F,Z}$ of infinite p-adic fields with specified residue field and value group admits elimination of quantifiers in the language of valued fields extended by W_n predicates.*

REFERENCES

[1] J. AX and S. KOCHEN, *Diophantine problems over local fields II. A complete set of axioms for p-adic number theory*, ***American Journal of Mathematics***, vol. 87 (1965), pp. 631–648.

[2] ———, *Diophantine problems over local fields III. Decidable fields*, ***Annals of Mathematics***, vol. 83 (1966), pp. 437–456.

[3] YU. L. ERSHOV, *On elementary theories of local fields*, ***Algebra i Logika***, vol. 4 (1965), no. 2, pp. 5–30.

[4] M. D. FRIED and M. JARDEN, ***Field arithmetic***, Springer-Verlag, 1986.

[5] C. KIEFE, *Sets definable over finite fields: Their zeta-functions*, ***Transactions of the American Mathematical Society***, vol. 223 (1976), pp. 45–59.

[6] J. KOENIGSMANN, *Half-ordered fields*, ***Ph.D. thesis***, Universität Konstanz, Germany, 1993.

[7] F.-V. KUHLMANN, *Henselian function fields and tame fields*, unpublished manuscript, 1990.

[8] ———, *Valuation theory of fields, abelian groups and modules*, ***Habilitationsschrift***, Universität Heidelberg, Germany, 1994.

[9] F.-V. KUHLMANN, M. PANK, and P. ROQUETTE, *Immediate and purely wild extensions of valued fields*, ***Manuscripta Mathematica***, vol. 55 (1986), pp. 39–67.

[10] A. MACINTYRE, *On definable subsets of p-adic fields*, this JOURNAL, vol. 41 (1976), pp. 605–610.

[11] ———, *Twenty years of p-adic model theory*, ***Logic Colloquium***, vol. 84 (1986), pp. 121–153.

[12] A. PRESTEL and P. ROQUETTE, ***Formally p-adic fields***, Springer-Verlag, 1984.

[13] A. ROBINSON and E. ZAKON, *Elementary properties of ordered abelian groups*, ***Transactions of the American Mathematical Society***, vol. 96 (1969), pp. 222–236.

[14] V. WEISPFENNING, *Elimination of quantifiers for certain ordered and lattice-ordered abelian groups*, ***Bulletin de la Société Mathématique de Belgique***, vol. 33, series B (1981), pp. 131–155.

FACHBEREICH MATHEMATIK UND STATISTIK
UNIVERSITÄT KONSTANZ
78457 KONSTANZ, GERMANY

Current address: Department of History and Philosophy of Science, University of Pittsburgh, 1017 Cathedral of Learning, Pittsburgh, PA 15260, USA

E-mail: inb1+@pitt.edu