Annals of Pure and Applied Logic 39 (1988) 1–17
North-Holland

SUBSTRUCTURES AND UNIFORM ELIMINATION FOR p-ADIC FIELDS

Luc BÉLAIR*
CNRS, Université de Paris VII, Paris, France

Communicated by Y. Gurevich
Received 30 August 1985; revised 11 February 1987

0. Introduction

Let p be a prime. The theory $p\mathrm{CF}_d$ of p-adically closed fields of p-rank d was introduced in [21] to study the model theory of finite extension fields (of a given degree d) of the field $\mathbb{Q}_p$ of p-adic numbers. Among other things Prestel and Roquette generalize Macintyre's elimination theorem for $p\mathrm{CF}$ ($d = 1$, [19]) but with the addition of constants $c_1, \ldots, c_d$ such that the c_i yield a basis for the valuation ring modulo p as a vector space over $\mathbb{F}_p$. A primitive recursive procedure for this elimination has been given in [27] and [13]. For a counterexample to see that Macintyre's language alone doesn't suffice in general for $d > 1$ see [25].

The results of this paper consist of an explicit axiomatization for the universal part of $p\mathrm{CF}_d$ in the Macintyre–Prestel–Roquette language and a model-theoretic proof of an elimination theorem for $\mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\})$.

Section 1 contains basic definitions from [21], to which we refer for further details. We also give basic results we shall appeal to in Section 2.

In Section 2 we give our axiomatization for the universal part of $p\mathrm{CF}_d$ in the language of elimination to be called $\mathscr{L}_d(P_\omega)$ below. This adds a new element in the analogy between the p-adic fields and the real field by giving an exact analog to the notion of ordered field. The basic predicates P_n of $\mathscr{L}_d(P_\omega)$, denoting nth-powers, yield for each n a multiplicative subgroup of finite index which we denote by $P_n^\cdot$. In our axiomatization, emphasis is given to the fact that for each of these groups the language of elimination contains closed terms giving a full set of coset representatives. A different axiomatization for $(p\mathrm{CF})_\forall$ in Macintyre's language was obtained independently by E. Robinson [23, 25]. We discuss it at

* The results of this paper are based on parts of the author's doctoral dissertation, Yale University, 1985. I wish to express my thanks to my advisor, Angus Macintyre, for his guidance and encouragement.
This research was supported by NSERC of Canada and Fonds FCAC of Québec.
Current address of the author: Université du Québec à Montréal, Québec, Canada.

the end of Section 2. When establishing our axiomatization we get, as a byproduct, first-hand information on the model-theoretic rôle of coset representatives for $P_n^{\cdot}$ in the elimination theory. This can be illustrated by a simple proof of uniqueness of p-adic closures we give in [4]. In a similar way first-hand knowledge of the 1-types over models of $p\mathrm{CF}_d$ can be used to give a treatment of the model theory of $p\mathrm{CF}_d$ in parallel with Abraham Robinson's treatment of real closed fields: e.g., proofs are provided in [4] which readily transpose to the case $d>1$.

Finally, in Section 3, the key argument in the proof of uniqueness of p-adic closures alluded to above is used to give a model-theoretic proof of an elimination theorem for $\mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\})$. Coset representatives of the $P_n^{\cdot}$ are again in the foreground. This result might be relevant when looking for some uniformity with respect to p in Denef's work concerning Poincaré series (see [12]). Connection with known elimination theorems is made.

For valuation theory we refer to [22] and for model theory to [7]. We use script letters $\mathscr{A}$, $\mathscr{B}$, ... in the standard model-theoretic fashion. We write $R^{\mathscr{A}}$ or R^A for the interpretation of the relation symbol R in $\mathscr{A}$ and $R^{\mathscr{A}}(a)$ for $\mathscr{A} \models R(a)$. Further notation is listed below.

Notation

L = the language of fields $(0, 1, +, -, \cdot, ^{-1})$,

card X = the cardinality of the set X,

$\boldsymbol{x} = (x_1, \ldots, x_n)$,

$A^{\cdot}$ = the group of units of the ring A,

$v_p(n)$ = the p-adic valuation of the integer n.

If K is a field or a valued field,

char K = the characteristic of K,

val K = the value group of K,

$v(x)$ = the value of x for the valuation v,

V_K = the valuation ring of K,

res K = the residue field of K,

$\bar{x}$ = the residue of x via $^{-}: V_K \rightarrow \operatorname{res} K$.

1. Preliminaries

We construe a valued field as a domain equipped with a divisibility relation $D(x, y)$ to be interpreted as $v(x) \leqslant v(y)$ (see [20]). The relation D is axiomatized by the universal axioms

$$\neg D(0, 1),$$
$$D(x, y) \vee D(y, x),$$
$$D(x, y) \wedge D(y, z) \rightarrow D(x, z),$$
$$D(x, y) \wedge D(x', y') \rightarrow D(xx', yy'),$$
$$D(x, y) \wedge D(x, y') \rightarrow D(x, y + y').$$

Note that one can make sense of a valuation map v for a domain instead of a field. Then, both v and D extend uniquely to similar structures on the field of fractions, namely

$$v(a/b) = v(a) - v(b) \quad \text{and} \quad D(a/b, c/d) \leftrightarrow D(ad, cb).$$

Our language of valued fields, $\mathcal{L}$, is the language of fields L augmented with a binary predicate $D(x, y)$ to be interpreted as a divisibility relation. We will nonetheless currently refer to the valuation map associated to a given divisibility relation.

Definition 1.1. Let p be a prime. A valued field K of characteristic 0 is a p-valued field if res K is of characteristic p and the dimension of the vector space $V_K/(p)$ over $\mathbb{F}_p$ is finite. If $d = \dim V_K/(p)$, then K is said to be of p-rank d.

The fields $\mathbb{Q}$ and $\mathbb{Q}_p$ with the p-adic valuation are both p-valued fields of p-rank 1. Finite extensions of $\mathbb{Q}_p$ of degree d are p-valued of p-rank d. A p-valued field has finite absolute ramification index (and so has a discrete value group) and finite absolute residue degree (and so has a finite residue field). We refer to these numbers respectively as the p-ramification index, denoted by e, and the p-residue degree, denoted by f. We then have $ef = d$. A subfield of a p-valued field of a given p-rank need not have same p-rank. However it is the case if one augments the language with constants $c_2, \ldots, c_d$ and interpret $1, c_2, \ldots, c_d$ as giving a basis for $V/(p)$ over $\mathbb{F}_p$ in any p-valued field of p-rank d. We denote by $\mathcal{L}_d$ this extension of $\mathcal{L}$. We sometimes let c_1 stand for the constant 1 in $\mathcal{L}_d$. Note $\mathcal{L}_1 = \mathcal{L}$.

1.2. Let $\pi(w)$ denote the following formula of $\mathcal{L}_d$

$$D(1, w) \wedge \neg D(w, 1) \wedge D(w, p) \wedge \bigwedge\left\{D\left(\sum_1^d l_j c_j, 1\right) \vee D\left(w, \sum_1^d l_j c_j\right) : 0 \leq l_j < p\right\}.$$

Lemma 1.3. *In a p-valued field of p-rank d an element w is a prime element if and only if $\pi(w)$ holds.*

Proof. Suppose $\pi(w)$ holds and let $v(y) > 0$. There are $0 \leq l_j < p$ such that $v(y - \sum l_j c_j) \geq v(p)$. If $v(y) \geq v(p)$, then $v(y) \geq v(p) \geq v(w)$. Otherwise,

$v(\sum l_j c_j) < v(p)$ and $v(y) = v(\sum l_j c_j) \geq v(w)$. Hence $\pi(w)$ implies that $v(w)$ is the least positive element of the value group, as wanted. The converse is clear. □

We record a strong (but equivalent) form of Hensel's lemma.

Lemma 1.4. *Let K be an henselian valued field and $f \in V_K[X]$. If there is some $a \in V_K$ such that $v(f(a)) > 2v(f'(a))$, then there is $b \in V_K$ such that $f(b) = 0$ and $v(b-a) > v(f'(a))$.*

Lemma 1.5. *Let K be an henselian p-valued field with p-ramification index e and $\varepsilon \in \mathbb{N}$ such that $p \nmid \varepsilon$ and $\varepsilon > e$. Then the valuation ring of K is algebraically definable by $x \in V_K$ iff $1 + px^{\varepsilon}$ is an ε-th power.*

Proof. Necessity follows from Hensel's lemma. For sufficiency, if $1 + px^{\varepsilon} = y^{\varepsilon}$ and $v(x) < 0$, then $v(y) < 0$ and $v(p) = \varepsilon v(yx^{-1})$, contradicting the choice of ε. □

It follows that being an henselian p-valued field of a given p-rank can be axiomatized in the language of rings since we have $D(x, y)$ iff $D(1, yx^{-1})$ iff $1 + p(yx^{-1})^{\varepsilon}$ is an εth power iff $x^{\varepsilon} + py^{\varepsilon}$ is an ε-th power. We now state some key facts. Let K be an henselian p-valued field of p-rank d, $Y \subseteq V_K$ be a complete set of representatives for $\operatorname{res} K$, and $\pi \in K$ be a prime element. Let $\beta(d, n) = 2dv_p(n)$.

Fact 1.6. *For all $n \in \mathbb{N}$, any $x \in V_K$ has a finite expansion*

$$x = \sum_{0}^{n} y_i \pi^i + x' \quad \text{with} \quad y_i \in Y \quad \text{and} \quad v(x') > nv(\pi).$$

Fact 1.7. *If $x \in K$ and $v(x) = 0$, then x is an n-th power if and only if $v(x - \lambda^n) > 2v(n)$ for some $\lambda = \sum_0^{\beta(d,n)} y_i \pi^i$ with $y_i \in Y$ and $v(\lambda) = 0$.*

Fact 1.8. *If $x \in K$ and $v(x) = 0$, then λx is an n-th power for some λ as above.*

Fact 1.6 is true for any valued field with a discrete value group. The two others are combinations of 1.6 with Lemma 1.4: e.g. in 1.8 apply 1.6 to x^{-1} and 1.4 to $X^n - \lambda x$.

Definition 1.9. We denote by $p\mathrm{CF}_d$ the theory of henselian p-valued fields of p-rank d with value group a $\mathbb{Z}$-group. We write $p\mathrm{CF}$ when $d = 1$. Models of $p\mathrm{CF}_d$ are called p-adically closed fields of p-rank d.

Finite extensions of $\mathbb{Q}_p$ of degree d are models of $p\mathrm{CF}_d$, in particular $\mathbb{Q}_p \models p\mathrm{CF}$.

Lemma 1.10. *In the theory $p\mathrm{CF}_d$ the multiplicative subgroup $P_n^{\cdot}$ of non-zero n-th powers has finite index with coset representatives among the $\lambda\pi^r$, $0 \leq r < n$ and λ like in Fact* 1.7.

Proof. Let $K \models p\mathrm{CF}_d$, $x \in K$. We have $v(x) = nv(y) + rv(\pi)$ for some $y \in K$ and $0 \leq r < n$ since val K is a $\mathbb{Z}$-group. Hence $v(x\pi^{-r}y^{-n}) = 0$ and the result follows by Fact 1.8. □

Definition 1.11. We denote by $\mathcal{L}_d(P_\omega)$ the language $\mathcal{L}_d$ augmented with unary predicates P_n for $n \geq 2$, each P_n to be interpreted as the n-th powers in models of $p\mathrm{CF}_d$.

Prestel and Roquette showed that $p\mathrm{CF}_d$ admits elimination of quantifiers in $\mathcal{L}_d(P_\omega)$. Finally let us remark that if K is a p-valued field of p-rank d, then res K is a quotient ring of $V_K/(p)$ so that there is always a complete set of representatives for res K among the $\sum l_j c_j$, $0 \leq l_j < p$.

2. The universal theory of p-adic fields

Let p be a fixed prime throughout. We give here an explicit axiomatization for the universal part of the theory $p\mathrm{CF}_d$ in the language $\mathcal{L}_d(P_\omega)$. Recall that in $\mathcal{L}_d(P_\omega)$ substructures of models of $p\mathrm{CF}_d$ are p-valued fields of p-rank d.

It is convenient to establish the following notation.

Definition 2.1. For integers $n \geq 2$, $d > 1$ let

$$
\begin{aligned}
&\beta(n) = 2v_p(n),\\
&\beta(d, n) = 2dv_p(n),\\
&\Lambda_n = \{\lambda \in \mathbb{N} : 1 \leq \lambda \leq p^{\beta(n)+1}, p \nmid \lambda\},\\
&R_n = \{r \in \mathbb{N} : 0 \leq r < n\},\\
&\Delta_n = \{l \in \mathbb{N} : l = \lambda p^r, \lambda \in \Lambda_n, r \in R_n\},\\
&N_n = \{i \in \mathbb{N} : 0 \leq i < p^{\beta(n)+1}, \text{ } i \text{ is an } n\text{-th power mod } p^{\beta(n)+1}\},\\
&g_{d,n}(\alpha_0, \ldots, \alpha_{\beta(d,n)}, w) = \alpha_0 + \alpha_1 w + \cdots + \alpha_{\beta(d,n)} w^{\beta(d,n)},\\
&E_d = \{l_1 + l_2c_2 + \cdots + l_dc_d : 0 \leq l_i < p\},\\
&\pi(w) := D(1, w) \wedge \neg D(w, 1) \wedge D(w, p) \wedge \bigwedge\{D(\tau, 1) \vee D(w, \tau) : \tau \in E_d\},\\
&U(x) := D(1, x) \wedge D(x, 1).
\end{aligned}
$$

We point out that E_d is a finite set of closed terms in $\mathcal{L}_d$ and $\pi(w)$, $U(x)$ are quantifier free formulas in $\mathcal{L}_d$, $\mathcal{L}$ respectively. As we saw previously $\pi(w)$ defines a prime element in a p-valued field of p-rank d if $c_2, \ldots, c_d$ are correctly interpreted. In a valued field with divisibility relation D, $U(x)$ says that x is a unit in the valuation ring.

Let $T_1 = T$ be the following theory.

Axiom 1. Axioms for a field of characteristic 0.

Axiom 2. Axioms for a p-valuation.

2.1. Axioms for a divisibility relation $D(x, y)$.

2.2. $\neg D(p, 1)$, $D(x, 1) \vee D(p, x)$.

2.3. $D(1, x) \to \bigvee\{D(p, x-i) : 0 \leq i < p\}$.

Axiom 3. Explicit definition of P_n for units of the valuation ring.

$$U(x) \to [P_n(x) \leftrightarrow \bigvee\{D(p^{\beta(n)+1}, x-i) : i \in N_n\}].$$

Axiom 4. Behaviour of the P_n.

4.1. $P_n(x^n)$.

4.2. $P_n(x) \wedge P_n(y) \to P_n(xy)$.

4.3. $P_n(x) \to P_n(x^{-1})$.

4.4. $P_{nm}(x) \to P_n(x)$.

4.5. $P_n(x) \to P_{nm}(x^m)$.

4.6. $\bigvee\{P_n(\lambda p^r x) : \lambda \in \Lambda_n, r \in R_n\}$.

Axiom 5. $P_n(x) \to D(z^n x, 1) \vee D(p^n, z^n x)$.

The first two axioms are self explanatory in view of Section 1. Axiom 3 is the result we proved about the definability of n-th powers (Fact 1.7), solely in terms of the valuation. Axioms 4.1, 2, 3, 6 say that $P_n^{\cdot}$ is a subgroup of finite index of the multiplicative group, with coset representatives in Δ_n. Axiom 5 keeps the P_n consistent with the (lack of) ramification. The following lemma is crucial.

Lemma 2.2. *Let $q, n(1), \ldots, n(k) \geq 2$ and $\Delta = \Delta_{n(1)} \times \cdots \times \Delta_{n(k)}$. We have*

$$T \vDash P_q(x) \to \bigvee_{l \in \Delta} \bigwedge \{P_{n(s)q}(l_s^q x),\ P_{n(t)}(l_t l_u^{-1}) : 1 \leq s, t, u \leq k,\ n(t) \mid n(u)\}.$$

Proof. It suffices to see that for any $n \geq 2$ there is $l_n \in \Delta_n$ such that $P_{nq}(l_n^q x)$. Indeed, taking $n = \mathrm{lcm}(n(s))$ and $l_s \in \Delta_{n(s)}$ such that $P_{n(s)}(l_s l_n^{-1})$ (Axiom 4.6), we easily get $P_{n(s)q}(l_s^q x)$ (Axiom 4); moreover if $n(t) \mid n(u)$, then $P_{n(t)}(l_u l_n^{-1})$ by Axiom 4.4 so that $P_{n(t)}(l_t l_u^{-1})$ (Axiom 4).

Now let $\lambda p^r \in \Delta_{nq}$ be such that $P_{nq}(\lambda p^r x)$. By Axiom 4 we have $P_q(\lambda p^r x)$ and $P_q(\lambda p^r)$. Axiom 5 and $v_p(\lambda) = 0$ imply that $r = qr'$ for some $0 \leq r' < n$, so that $P_q(\lambda)$. Now λ is an integer and $v_p(\lambda) = 0$, so by Axiom 3 and since $\mathbb{Q}$ is dense in its henselization with respect to v_p (or alternatively, by arguing as if to 'construct' a q-th root of λ in $\mathbb{Q}_p$ but using only a finite number of steps (approximations)), there is an integer $\lambda_n \in \Lambda_n$ such that $\lambda^{-1}\lambda_n^q$ satisfies the conditions in Axiom 3 in order that $P_{nq}(\lambda^{-1}\lambda_n^q)$. It follows that $P_{nq}(l_n^q x)$ for $l_n = \lambda_n p^{r'} \in \Delta_n$, as wanted. □

To establish our axiomatization we have to show that we can embed a given model $\mathscr{A}$ of T in a p-adically closed field (of p-rank 1) $\mathscr{M}$. The process of going from $\mathscr{A}$ to $\mathscr{M}$ involves extending $\mathscr{A}$ to larger $\mathscr{L}(P_\omega)$-structures by adding an n-th root to each element $a \in \mathscr{A}$ for which $P_n(a)$ holds. Let $y^q = a$ in a p-adically closed field (of p-rank 1) and let l_n, $n \geq 2$, be integers such that $P_n(l_n y)$ holds. Then $P_{nq}(l_n^q a)$, and the statements of Lemma 2.2 hold uniformly for the l_n. The sequence (l_n) tells us in which coset of $P_n^{\cdot}$ y lies for each n and, as we shall see later, this information determines the type of y, at least as far as the P_n are concerned. Lemma 2.2 gives consistency conditions for $a \in \mathscr{A}$ such that $P_q(a)$ holds in order to keep available to us (in some elementary extension) the P_n-type of some q-th root of a.

Let T_d be the following theory, d a fixed integer $d > 1$.

Axiom 1*d*. Axioms for a field of characteristic 0.

Axiom 2*d*. Axioms for a p-valuation of p-rank d.

2.1*d*. Axioms for a divisibility relation $D(x, y)$.

2.2*d*. $\neg D(p, 1)$, $D(1, c_i)$, $i = 2, \ldots, d$.

2.3*d*. $D(1, x) \rightarrow \bigvee\{D(p, x - \tau) : \tau \in E_d\}$.

2.4*d*. $\neg D(p, l_1 + \cdots + l_d c_d)$, $0 \leq l_i < p$ not all 0.

Axiom 3*d*. Explicit definition of P_n for the units of the valuation ring.

$$U(x) \wedge \pi(w) \rightarrow [P_n(x) \leftrightarrow \bigvee\{D(n^2, x - (g_{d,n}(\boldsymbol{\tau}, w))^n) \wedge \neg D(x - (g_{d,n}(\boldsymbol{\tau}, w)^n, n^2) : \boldsymbol{\tau} \in E_d^{\beta(d,n)+1}\}].$$

Axiom 4*d*. Behaviour of the P_n.

4.1*d* to 4.5*d* are the same as 4.1 to 4.5.

4.6*d*. $\pi(w) \rightarrow \bigvee\{P_n(g_{d,n}(\boldsymbol{\tau}, w)w^r x) \wedge U(g_{d,n}(\boldsymbol{\tau}, w)) : r \in R_n, \boldsymbol{\tau} \in E_d^{\beta(n)+1}\}$.

Axiom 5*d*. $P_n(x) \wedge \pi(w) \rightarrow D(z^n x, 1) \vee D(w^n, z^n x)$.

The analogy between T_d and T_1 is clear anough. Note that T_d is universal and it is straightforward to verify $p\mathrm{CF}_d \models T_d$. The following is the analog of Lemma 2.2.

Lemma 2.3. *Let $d > 1$ and consider $q, n(1), \ldots, n(k) \geq 2$, $R = R_{n(1)} \times \cdots \times R_{n(k)}$ and $E = E_d^{\beta(d,n(1))+1} \times \cdots \times E_d^{\beta(d,n(k))+1}$. For $\boldsymbol{\tau} \in E$ and $1 \leq i \leq k$ let $\boldsymbol{\tau}_i$ be in $E_d^{\beta(d,n(i))+1}$ and denote the i*-th *component of* $\boldsymbol{\tau}$. *Then we have*

$$T_d \models P_q(x) \wedge \pi(w) \rightarrow \bigvee_{(\boldsymbol{\tau},r) \in E \times R} \bigwedge \{P_{n(s)q}((g_{d,n(s)}(\boldsymbol{\tau}_s, w)w^{r(s)})^q x), U(g_{d,n(s)}(\boldsymbol{\tau}_s, w)),$$

$$P_{n(t)}(g_{d,n(t)}(\boldsymbol{\tau}_t, w)w^{r(t)}(g_{d,n(u)}(\boldsymbol{\tau}_u, w)w^{r(u)})^{-1}) : 1 \leq s, t, u \leq k, n(t) \mid n(u)\}.$$

Proof. The proof is the same as in Lemma 2.2, but using the henselization of the field generated by the constants of $\mathscr{L}_d$ (Fact 1.6) instead of the henselization of $(\mathbb{Q}, v_p)$. $\square$

We shall see that every model of T_d can be embedded in a model of $p\mathrm{CF}_d$, thus showing $T_d = (p\mathrm{CF}_d)_\forall$.

Theorem 2.4. *Let $\mathscr{A} \models T_d$. Then $\mathscr{A} \hookrightarrow \mathscr{M}$ for some $\mathscr{M} \models p\mathrm{CF}_d$.*

Lemma 2.5. *We have $T \models P_n(x) \wedge D(x, y) \wedge D(y, x) \rightarrow \bigvee \{P_n(\lambda y) : \lambda \in \Lambda_n\}$, and for $d > 1$,*

$$T_d \models P_n(x) \wedge D(x, y) \wedge D(y, x) \wedge \pi(w) \\ \rightarrow \bigvee \{P_n(g_{d,n}(\boldsymbol{\tau}, w)y) \wedge U(g_{d,n}(\boldsymbol{\tau}, w) : \boldsymbol{\tau} \in E_d^{\beta(d,n)+1}\}.$$

Proof. Use Axiom 4.6d for $x^{-1}y$ and Axiom 5d to see that $r = 0$. $\square$

Lemma 2.6. *Let $\mathscr{A} \models T_d$ and $\mathscr{M} \models p\mathrm{CF}_d$ such that A is a $\mathscr{L}_d$-substructure of M. If $P_n^{\mathscr{A}} \subseteq P_n^{\mathscr{M}}$ for all n, then $\mathscr{A} \subseteq \mathscr{M}$.*

Proof. We have $P_n^{A^{\cdot}} \subseteq P_n^{M^{\cdot}}$ and $[A^{\cdot} : P_n^{A^{\cdot}}] = [M^{\cdot} : P_n^{M^{\cdot}}]$ is finite, and $P_n^{A^{\cdot}}$ and $P_n^{M^{\cdot}}$ have the same coset representatives already in $A^{\cdot}$. $\square$

Any p-valued field of p-rank d, in particular a model of T_d, can be embedded as a valued field in a model of $p\mathrm{CF}_d$, see e.g. [8] for a suitable Zorn's lemma argument. We are now reduced to show that given a model $\mathscr{A}$ of T_d we can start adding the required n-th roots and stay inside a model of T_d. First we reduce to the case when $\mathscr{A}$ is henselian.

Lemma 2.7. *Assume $\mathscr{A} \models T_d$ and B is an immediate henselian valued field extension of A. Then B can be expanded to a model $\mathscr{B} \supseteq \mathscr{A}$ of T_d.*

Proof. Put $c_i^B = c_i^A$. Since B/A is immediate, B is a p-valued field of p-rank d with the same p-ramification index and p-residue degree and $1, c_2, \ldots, c_d$ still form a basis for $V_B/(p)$. We do the case $d = 1$ for definiteness. If $x \in B$, there is some $y \in A$ such that $v(xy) = 0$. Since B is henselian p-valued we get $\lambda_n xy = b^n$ for some $\lambda_n \in \Lambda_n$ and $b \in B$. Define $P_n^B(x)$ iff $P_n^A(\lambda_n y)$.

(i) This definition is independent of the y and λ_n chosen. Indeed suppose $v(xy) = 0$, $v(xy') = 0$, λxy, $\lambda' xy'$ are n-th powers in B, $P_n^A(\lambda y)$ and λ, λ', y, y' as above. Then $v(\lambda^{-1}y^{-1}\lambda' y') = 0$ and $\lambda^{-1}y^{-1}\lambda' y'$ satisfies the residue condition in Axiom 3 so that $P_n^A(\lambda^{-1}y^{-1}\lambda' y')$ and $P_n^A(\lambda' y')$ by Axiom 4.

(ii) $P_n^B \cap A = P_n^A$, for all n: easily seen from (i) and using T.

(iii) We verify the remaining axioms for $\mathscr{B} = \langle B, P_n^B : n \geqslant 2\rangle$.

Axiom 3. Use Fact 1.7 and similar axiom in A.

Axiom 4.1. Use y^n for x^n if $v(xy)=0$.

Axioms 4.2–4.5. For example we verify Axiom 4.2. Suppose $P_n^B(x_1)$, $P_n^B(x_2)$, $v(x_i y_i)=0$, $\lambda_i x_i y_i$ is an n-th power and $P_n^A(\lambda_i y_i)$. Then $v(x_1 x_2 y_1 y_2)=0$. Let λ be chosen such that $\lambda\lambda_1^{-1}\lambda_2^{-1}$ is an n-th power, so $P_n^A(\lambda\lambda_1^{-1}\lambda_2^{-1})$ (Axiom 3). Thus $\lambda x_1 x_2 y_1 y_2$ is an n-th power and $P_n^A(\lambda y_1 y_2)$ (Axiom 4.2 in A) whence $P_n^B(x_1 x_2)$.

Axiom 4.6. Let $x\neq 0$, $v(xy)=0$, $y\in A$. It is not hard to get $P_n^A(\lambda p^{-r}y)$ for suitable λ, r, $v(\lambda)=0$ (cf. Axiom 4 and Lemma 2.5 in A). We have $v(\lambda xy)=0$ so $\lambda'\lambda xy$ is an n-th power for some suitable λ'. Hence $v(\lambda' p^r x p^{-r} y)=0$, $\lambda\lambda' p^r x p^{-r} y$ is an n-th power and $P_n^A(\lambda p^{-r}y)$. So $P_n^B(\lambda' p^r x)$.

Axiom 5. Let $x, z\in B$ be such that $P_n^B(x)$. So for some $y\in A$ and $\lambda\in\Lambda_n$, λxy is an n-th power and $P_n^A(\lambda y)$. Hence $P_n^A(\lambda^{-1}y^{-1})$, $v(x)=v(\lambda^{-1}y^{-1})$. The conclusion follows because the axiom is true in A. □

Note that we can drop the henselian assumption from the preceding lemma. First use Axiom 3*d* to define P_n for the units of the valuation ring. Then there is λ_n such that $\lambda_n xy$ satisfies Axiom 3*d*, etc.

Lemma 2.8. *Suppose that for all* $\mathscr{A}\models T_d$ *and all prime* q *and* $a\in A$ *such that* $P_q^A(a)$ *we can embed* $\mathscr{A}$ *in a model of* T_d *where* a *is a* q-th *power. Then the same is true for all natural numbers* n.

Proof. By induction on n and using Lemma 2.5 and Axiom 4.6*d* we can go to a model $\mathscr{B}\models T_d$ with $b\in B$ such that $P_n(ab^{-n})$ and $v(ab^{-n})=0$. By the previous lemma we can assume B henselian whence the result by Axiom 3*d* and Fact 1.7. □

Remark that as we just saw above, if $\mathscr{A}\models T_d$ is henselian and $P_n^A(a)$, then a is an n-th power iff $v(a)$ is divisible by n.

Lemma 2.9. *Let* $\mathscr{A}\models T_d$, q *prime,* $a\in A$ *such that* $P_q^A(a)$. *We can embed* $\mathscr{A}$ *in a model of* T_d *where* a *is a* q-th *power.*

Proof. Relying on the previous work we can assume A is henselian, $v(a)>0$ and $q\nmid v(a)$ in val A.

By Lemma 2.3 (2.2) and compactness, there is $\mathscr{B}\succcurlyeq\mathscr{A}$, $\rho_n\in B$, $n=2,3,\ldots$ such that $P_{nq}^B(\rho_n^q a)$ and $P_n^B(\rho_n\rho_{nm}^{-1})$ for all n, m. Then a is not a q-th power in B and X^q-a is irreducible over B. Note that B is also henselian p-valued of p-rank d.

Consider the valued field extension $B(\alpha)/B$, $\alpha^q=a$. It has degree q. Now $q\nmid v(a)$ in val B and q is prime, so for any $x\in B(\alpha)$, $v(x)=v(b\alpha^i)$ for some $b\in B$ and $0\leqslant i<q$. This together with Axiom 5*d* ensures that the p-ramification index does not increase in $B(\alpha)$. These considerations and $v(\alpha)>0$ imply also that the residue field does not extend. In fact, if $v(\sum b_i\alpha^i)\geqslant 0$, then $v(b_i\alpha^i)\geqslant 0$

for all i and $v(b_i\alpha^i) > 0$ for $i > 0$. Thus $\langle B(\alpha), c_i^B \rangle$ is a p-valued field of p-rank d and is henselian.

Let $Y = \{b\alpha^i : b \in B, b \neq 0, 0 \leq i < q\}$ and define $P_n^Y(b\alpha^i)$ iff $P_n^B(b\rho_n^{-i})$. We show that $\langle Y, c_i^B, P_n^Y \rangle$ satisfies the axioms of T_d concerning the P_n and then use those P_n^Y to expand $B(\alpha)$. Notice that if $b \in B$, $l \in \mathbb{N}$, $l = kq + i$, $0 \leq i < q$, then $P_n^B(b\rho_n^{-l})$ iff $P_n^B(b\rho_n^{-kq}\rho_n^{-i})$ iff $P_n^B(ba^k\rho_n^{-i})$ (as $P_n^B(\rho_n^q a)$) iff $P_n^Y(b\alpha^l)$. Also P_n^Y extends P_n^B, i.e., $P_n^Y \cap B = P_n^B$.

Axiom 3*d*. Notice that for $y \in Y$, $v(y) = 0$ iff $y \in B$.

Axiom 4*d*. For example Axiom 4.3*d*. Let $y = b\alpha^i \in Y$ be such that $P_n^Y(y)$, i.e., $P_n^B(b\rho_n^{-i})$. Then $P_n^B(b^{-1}\rho_n^i)$, $y^{-1} = b^{-1}a^{-1}\alpha^{q-i}$. Since $P_n^B(\rho_n^q a)$ we get $P_n^B(b^{-1}a^{-1}\rho_n^{i-q})$, i.e., $P_n^Y(y^{-1})$. Use the compatibility $P_n^B(\rho_n\rho_{nm}^{-1})$ in Axioms 4.4*d* and 4.5*d*.

Axiom 5*d*. We show that if $y \in Y$, $z, w \in B(\alpha)$, $\pi(w)$ and $P_n^Y(y)$, then $v(z^n y) \leq 0$ or $v(z^n y) \geq nv(w)$. Suppose $y = b\alpha^j$ and $P_n^B(b\rho_n^{-j})$. We have $v(z) = v(b'\alpha^i)$ for some $b' \in B$ and $0 \leq i < q$. Now if

$$0 < v(z^n y) = v(b'^n) + niv(\alpha) + v(b) + jv(\alpha) < nv(w),$$

then

$$(*) \qquad 0 < nqv(b') + v(a^{ni}b^q a^j) < nqv(w).$$

But $P_q^B(a)$, $P_{nq}^B(\rho_n^q a)$, $P_n^B(b\rho_n^{-j})$ yield $P_{nq}^B(a^{ni}b^q a^j)$ so that (*) would contradict the conclusion of the similar axiom in B for the element $a^{ni}b^q a^j$.

So we have established $\langle Y, c_i^B, P_n^Y \rangle \models$ "relevant axioms of T_d" and $P_n^Y \cap B = P_n^B$. Let $M = B(\alpha)$. For $x \in M$ there is $y \in Y$ such that $v(xy) = 0$, and since M is henselian p-valued of p-rank d there is some $\lambda \in B$, $v(\lambda) = 0$, such that λxy is an n-th power in M. Define $P_n^M(x)$ iff $P_n^Y(\lambda y)$. We can then proceed as in Lemma 2.7 to show that $\langle M, c_i^B, P_n^M \rangle \models T_d$ and $P_n^M \cap Y = P_n^Y$. This completes the proof. □

Proof of Theorem 2.4. Use Lemma 2.8, Lemma 2.9 and a standard model-theoretic argument to embed $\mathscr{A}$ in a model of T_d where every $a \in P_n^A$ is an n-th power. Embed this model (as a valued field) in a model of $p\mathrm{CF}_d$ and conclude by Lemma 2.6. □

Remark that since $p\mathrm{CF}_d \models D(x, y) \leftrightarrow P_\varepsilon(x^\varepsilon + py^\varepsilon)$ where ε can be any positive integer prime to p and larger than d, the above theory immediately gives also an axiomatization of $(p\mathrm{CF}_d)_\forall$ in $L(c_i, P_\omega)$, i.e., the language obtained when we drop the divisibility relation symbol D.

We now compare our axiomatization with that of [25]. Robinson's axiomatization of $(p\mathrm{CF})_\forall$ in $\mathscr{L}(P_\omega)$ relies on the fact that the group $P_n^\cdot$ of n-th powers is 'effectively open', namely there is an integer r_n such that if $x, y \neq 0$, $x \in P_n^\cdot$ and $v(x - y) > v(x) + r_n v(p)$, then $y \in P_n^\cdot$. It is clear how to relate this to Hensel's Lemma. He also includes the diagram of $\mathbb{Q}$ (in $\mathscr{L}(P_\omega)$) but it is not hard to see that it is contained in our Axiom 3 and Axiom 5. The other axioms are mainly the same as in Axiom 4. So the essential difference lies in Axiom 3. In fact, "$P_n^{\cdot}$ is effectively open" follows directly from Axiom 3 and conversely; they are interchangeable. To establish his axiomatization Robinson needs to know explicitly the (number of) n-th roots of 1 in pCF, which can be done easily because of lack of ramification. The proof is also tied to the rigidity of p-adic closures, which is established at the same time. It is clear that Axiom 3d is interchangeable as well with a suitable version of "$P_n^{\cdot}$ is effectively open" in $p\mathrm{CF}_d$.

Any axiomatization of $(p\mathrm{CF}_d)_\forall$ in $\mathscr{L}_d(P_\omega)$ relates to the description of the points of the p-adic spectrum associated to each completion of $p\mathrm{CF}_d$, see [24], [3], [26], [5]. Along these lines it is clear that Lemma 2.3 is closely related to the description of Bröcker and Schinke [5], via their neat use of $\varprojlim (L^{\cdot}/L^{\cdot n})$, $L/\mathbb{Q}_p$ a fixed finite extension.

3. Uniformity of elimination

We now state an elimination theorem for the $\mathbb{Q}_p$ when p varies through the primes, namely for the theory $\mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\})$. We take into account the residue theory $\mathrm{Th}(\{\mathbb{F}_p : p \text{ prime}\})$, which contains a theory of pseudo-finite fields. A reasonable elimination theorem was shown to hold for those by Kiefe [17], building on the work of Ax [1]. As a theory of valued fields our theory has two kinds of models:

(1) those with a residue field of non-zero characteristic p, which are p-adically closed of p-rank 1;

(2) those of equal characteristic zero, which are henselian valued in a $\mathbb{Z}$-group with residue field a pseudo-finite field.

Having Shoenfield's criterion for elimination of quantifiers (later E.Q.) in mind, we can split the analysis into those two possibilities. The first one is handled by Macintyre's Theorem. The second one can be taken care of by the Theorem 5 in [9], or Corollaire 2.21 in [11], or Theorem 4.12 in [27]. With techniques of Delon [11] we give here an independent proof based on the key argument in our proof of uniqueness of p-adic closures mentioned in Section 0. The global elimination theorem we get for $\mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\})$ can also be deduced from the Main Theorem 4.3 in [27]. We discuss this more precisely below. Similar questions are treated in an unpublished paper of Fried [14], but in the very different framework of [16] (see also [15]).

We refer to [1] for pseudo-finite fields, e.g., the first-order axiomatization we implicitly use. We need some preliminary results.

Lemma 3.1. *Let n be a fixed positive integer. There is a uniform bound $\delta(n)$ for the index $[\mathbb{Q}_p^{\cdot} : P_n^{\cdot}]$ when p varies through the primes.*

Proof. For all $p > n$, $(n, p) = 1$ and using Hensel's Lemma it is not difficult to see that $[\mathbb{Q}_p^{\cdot} : P_n^{\cdot}] = n[\mathbb{F}_p^{\cdot} : P_n^{\cdot}] = n(\gcd(n, p-1))$. □

Lemma 3.2. *The theory* $\mathrm{Th}(\{\mathbb{F}_p : p \text{ prime}\})$ *admits elimination of quantifiers in the language of fields augmented with n-ary predicates* Sol_n *interpreted as* $\mathrm{Sol}_n(x_1, \ldots, x_n) \leftrightarrow \exists y\ (y^n + x_1 y^{n-1} + \cdots + x_n = 0)$ *in the theory.*

Proof. See [17]. □

Lemma 3.3. *Let m, n, d be positive integers. We can find a positive integer* $\beta(m, n, d)$ *with the following property. If k is a finite field with* $\mathrm{card}\, k > \beta(m, n, d)$, *then for all* $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$, $\deg f_i \leq d$, *such that the ideal* $I = (f_1, \ldots, f_m)$ *in* $k[X]$ *is absolutely irreducible, the variety defined by I has a k-point.*

Proof. See [1, Section 8]. □

Lemma 3.4. *For any prime p,* $\mathcal{M} \models p\mathrm{CF}$, $x \in M$, *we have* $v(x) \geq 0$ *iff* $P_2(1 + px^2)$ *or* $P_2(1 + p(1+x)^2)$.

Proof. (Cf. Axiom 3 in Section 2.) Suppose $v(x) \geq 0$. If $p \neq 2$, then readily $P_2(1 + px^2)$. If $p = 2$, then $v(1 - (1 + 2x)^2) \geq 3$ when $v(x) > 0$, and $v(1 - (1 + 2(1+x)^2)) \geq 3$ when $v(x) = 0$, so that accordingly $P_2(1 + 2x^2)$ or $P_2(1 + 2(1+x)^2)$. Suppose $1 + px^2 = y^2$ and $v(x) < 0$. Then $v(y) < 0$ and $2 \mid v(p)$ which is absurd. Similarly if $1 + p(1+x)^2 = y^2$ and $v(x) < 0$. □

Let $\mathcal{L}'$ be the language whose vocabulary consists of the vocabulary of $\mathcal{L}(P_\omega)$, a new constant t, and for $n \geq 2$, a n-ary predicate Sol_n and new constants $u_{n,1}, \ldots, u_{n,\delta'(n)}$ where $\delta'(n) = n^{-1}\delta(n)$, $\delta(n)$ given by Lemma 3.1. We first give an explicit axiomatization for $\mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\})$.

Let T' be the theory in $\mathcal{L}'$ consisting of the following axioms:

(1) Axioms for an henselian valued field of characteristic 0.

(2) The value group is a $\mathbb{Z}$-group with unit $v(t)$.

(3) $P_n(x) \leftrightarrow \exists y\ (y^n = x)$, $D(u_{n,j}, 1) \wedge D(1, u_{n,j})$.

(4) $\mathrm{Sol}_n(x_1, \ldots, x_n) \leftrightarrow \bigwedge D(1, x_j) \wedge \exists y\ (D(1, y) \wedge D(t, y^n + x_1 y^{n-1} + \cdots + x_n))$.

(5) If the residue field has characteristic $p \neq 0$, then it has p elements and $t = p$.

(6) $D(x, y) \leftrightarrow P_2(x^2 + ty^2) \vee P_2(x^2 + t(x-y)^2)$.

(7) $\bigvee \{P_n(u_{n,j} t^r x) : 1 \leq j \leq \delta'(n), 0 \leq r < n\}$.

(8) If the residue field has more than $\beta(m, n, d)$ elements, $\beta(m, n, d)$ from Lemma 3.3, and $f_1(X_1, \ldots, X_n), \ldots, f_m(X_1, \ldots, X_n)$ are polynomials of degree $\leq d$ over the valuation ring such that their image $\bar{f}_j$ under the residue map generate an absolutely irreducible ideal over the residue field, then the $\bar{f}_j$ have a common zero in the residue field.

(9) The residue field is quasi-finite, i.e., it is perfect and has a unique extension of each degree.

Proposition 3.5. *The theories T' and* $\mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\})$ *have the same models.*

Proof. In view of our discussion it is clear that $\mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\}) \models T'$. On the other hand, let $M \models T'$. If $\operatorname{char} \operatorname{res} M$ is $p \neq 0$, then $M \models p\mathrm{CF}$, so $M \models \mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\})$. If $\operatorname{char} \operatorname{res} M$ is 0, then M is henselian of equal characteristic 0, $\operatorname{val} M$ is a $\mathbb{Z}$-group, and $\operatorname{res} M$ is a pseudo-finite field of characteristic 0. By [1] there is some ultrafilter $\mathscr{F}$ on the set of primes such that $\operatorname{res} M \equiv \prod \mathbb{F}_p / \mathscr{F}$. It follows by Ax–Kochen–Ershov that $M \equiv \prod \mathbb{Q}_p / \mathscr{F}$ as valued fields. So $M \models \mathrm{Th}(\{\mathbb{Q}_p : p \text{ prime}\})$. □

We need the next two lemmas in the proof of the elimination theorem.

Lemma 3.6. *Let K be an henselian valued field of equal characteristic* 0 *and K_0 be a subfield of K. The following are equivalent.*

(i) *The residue map induces an isomorphism of K_0 onto* $\operatorname{res} K$.

(ii) *K_0 is a maximal trivially valued subfield of K.*

Proof. See, e.g., [18, Lemma 8]. □

Lemma 3.7. *Let $E \subseteq F$ be valued fields, $F_0 \subseteq F$ be such that the residue map induces an isomorphism α of F_0 onto* $\operatorname{res} F$. *Suppose that $E_0 = \alpha^{-1}[\operatorname{res} E]$ is contained in E and let K_0 be such that $E_0 \subseteq K_0 \subseteq F_0$. Then*

(i) *E and F_0 are linearly disjoint over E_0.*

(ii) *Any $x \in E[K_0]$ can be written $x = \sum_1^n e_i k_i$, $e_i \in E$, $k_i \in K_0$ and $v(e_i) < v(e_j)$ if $i < j$.*

(iii) $\operatorname{val} EK_0 = \operatorname{val} E$ *and* $\operatorname{res} EK_0 = \operatorname{res} K_0$.

Proof. See [11, Proposition 2.15]. □

Theorem 3.8. *The theory T' admits elimination of quantifiers in $\mathscr{L}'$.*

Proof. We use Shoenfield's criterion. Let $\mathscr{M}_1$, $\mathscr{M}_2$ be models of T', $\mathscr{A}_i \subseteq \mathscr{M}_i$, $f : \mathscr{A}_1 \xrightarrow{\sim} \mathscr{A}_2$ such that $\operatorname{card} M_1 = \omega$ and $\mathscr{M}$ is ω_1-saturated. We have to see that f extends to an embedding $\mathscr{M}_1 \hookrightarrow \mathscr{M}_2$.

Case 1: *The field* $\operatorname{res} A_1$ *has characteristic* $p \neq 0$. Then so do $\operatorname{res} M_i$ and the M_i are p-adically closed of p-rank 1. We get the desired extension by Macintyre's Theorem.

Case 2: *The field* $\operatorname{res} A_1$ *has characteristic* 0. Then the M_i are henselian valued fields of equal characteristic 0 valued in a $\mathbb{Z}$-group with pseudo-finite residue fields. We argue in the style of [11] to reduce to $\operatorname{res} A_1 = \operatorname{res} M_1$; then use our argument to reduce further to $\operatorname{val} A_1$ being pure in $\operatorname{val} M_1$, and finally close the case with Ax–Kochen–Ershov.

(2.1) We may assume A_i is henselian. Let A_i^h be the henselization of A_i in M_i. Then f extends to an isomorphism of valued fields f^h between the A_i^h. This f^h is compatible with the Sol_n because those are determined at the level of residue fields and A_i^h/A_i is an immediate extension. For the P_n, let $y \in A_1^h$, $v(y) \geqslant 0$. There is $x \in A_1$ such that $v(x) = v(y) < v(x-y)$ and by Hensel's Lemma we have $x \in M_1^{\cdot n}$ iff $y \in M_1^{\cdot n}$. Clearly such a configuration transfers to M_2 via f^h (and vice versa) and the desired conclusion follows.

(2.2) We may assume $\operatorname{res} A_1 = \operatorname{res} M_1$. First, observe that with the interpretation of Sol_n in M_i, we can define in a natural way predicates $\overline{\mathrm{Sol}}_n$ in $\operatorname{res} M_i$ which coincide with the Sol_n of Lemma 3.2. By Lemma 3.2 there exists

$$g : \langle \operatorname{res} M_1, \overline{\mathrm{Sol}}_n \rangle \hookrightarrow \langle \operatorname{res} M_2, \overline{\mathrm{Sol}}_n \rangle$$

extending the map induced by f on the residue fields $\langle \operatorname{res} A_i, \overline{\mathrm{Sol}}_n \rangle$ considered as substructures. By Lemma 3.6 and (2.1), let $A_0 \subseteq A_1$ be such that the residue map induces an isomorphism of A_0 onto $\operatorname{res} A_1$, and $N_i \subseteq M_i$ with the similar property such that $A_0 \subseteq N_1$. Let $\alpha_i : N_i \to M_i$ be the inverse to the residue map. By Lemma 3.7, A_1 and N_1 are linearly disjoint over A_0, $\operatorname{val} A_1 N_1 = \operatorname{val} A_1$, $\operatorname{res} A_1 N_1 = \operatorname{res} N_1 = \operatorname{res} M_1$ and any $z \in A_1[N_1]$ can be written $z = \sum x_i y_i$ with $x_i \in A_1$, $y_i \in N_1$ and $v(x_i) < v(x_j)$ if $i < j$. We can thus define a map $f' : A_1(N_1) \to A_2(\alpha_2 g \alpha_1^{-1}[N_1])$ which extends f and is an isomorphism of valued fields. To see that f' is an $\mathscr{L}'$-isomorphism, first remark that the Sol_n are immediately taken care of because of g. For the P_n, let $z = \sum x_i y_i$ with x_i, y_i as above. Then $v(z) = v(x_j y_j)$ for some j and Hensel's Lemma implies $z \in M_1^{\cdot n}$ iff $x_j y_j \in M_1^{\cdot n}$. Let $u = u_{n,k}$ be such that $u y_j \in M_1^{\cdot n}$. Then $z \in M_1^{\cdot n}$ iff $x_j y_j \in M_1^{\cdot n}$ iff $x_j u^{-1} \in M_1^{\cdot n}$ iff $f(x_j) u^{-1} \in M_2^{\cdot n}$ iff $f(x_j) f'(y_j) \in M_2^{\cdot n}$ iff $f'(z) \in M_2^{\cdot n}$. (Note that the analytic configuration of z, x_j, y_j carries over to M_2.)

(2.3) We may assume $\operatorname{val} A_1$ is pure in $\operatorname{val} M_1$. First note that we need only worry about prime numbers. Let q be a prime. By axiom (7) of T' it suffices to add a q-th root to any $a_1 \in A_1$ such that $M_1 \vDash P_q(a_1)$ but $q \nmid v(a_1)$ in $\operatorname{val} A_1$, and extend f accordingly. So let $a_1 \in A_1$ be as above such that, w.l.o.g, $v(a_1) > 0$. Let $y_1 \in M_1$, $\rho_n = u_{n,j} t^r$ such that $y_1^q = a_1$ and $\rho_n y_1 \in M_1^{\cdot n}$. Let $a_2 = f(a_1)$ and consider the partial type

$$\Sigma(x) = \{x^q - a_2 = 0,\ P_n(\rho_n x),\ n \geqslant 2\}.$$

Claim. *Σ is realized in M_2.*

Assume the claim is true and let y_2 realize Σ. First observe that $X^q - a_i$ is irreducible over A_i and that the induced valuation on $A_i(y_i)$ is completely determined, namely

$$v(e_0 + e_1 y_i + \cdots + e_{q-1} y_i^{q-1}) = \min v(e_j y_i^j).$$

So we get an isomorphism of valued fields $f'' : A_1(y_1) \to A_2(y_2)$ extending f and sending y_1 onto y_2. Let us see that f'' preserves the P_n. Let $x_1 \in A_1(y_1)$, $x_2 = f''(x_1)$.

We have $v(x_1d_1y_1^{-j})=0$ for some $d_1 \in A_1$ and some $0 \leq j < q$. Let $d_2 = f(d_1)$; then $v(x_2d_2y_2^{-j})=0$. There exists $\lambda_1 \in A_1$ such that $v(\lambda_1)=0$ and $\lambda_1 x_1 d_1 y_1^{-j} \in M_1^{;n}$. Let $\lambda_2 = f(\lambda_1)$; then $\lambda_2 x_2 d_2 y_2^{-j} \in M_2^{;n}$ (cf. (2.2)). Hence $x_1 \in M_1^{;n}$ iff $\lambda_1 d_1 y_1^{-j} \in M_1^{;n}$ iff $\lambda_1 d_1 \rho_n^j \in M_1^{;n}$ iff $\lambda_2 d_2 \rho_n^j \in M_2^{;n}$ iff $\lambda_2 d_2 y_2^{-j} \in M_2^{;n}$ iff $x_2 \in M_2^{;n}$ and we are done. By (2.2) the Sol_n are again taken care of by the residue fields. So f'' is an $\mathscr{L}'$-isomorphism.

Proof of the Claim. Since we are in equal characteristic 0, the number of q-th roots of 1 in the M_i is decided in the residue fields and by (2.2) has to be the same. If there is only one q-th root of 1, there is only one choice for y_2 and nothing to prove since, then, $x \in M_i^{;n}$ iff $x^q \in M_i^{;nq}$ and $(\rho_n y_1)^q = \rho_n^q a_1 \in A_1$, etc. So let ζ be a primitive q-th root of 1 in M_2 and $b \in M_2$ be such that $b^q = a_2$. Suppose the claim false. Then there are $n_0, \ldots, n_{q-1}$ such that $\rho_{n_j} b\zeta^j \notin M_2^{;n_j}$. Let $n = \mathrm{lcm}(n_j)$, then $\rho_n b \zeta^j \notin M_2^{;n}$ for all j $(\rho_n^{-1}\rho_{n_j} \in M_2^{;n_j})$. But $\rho_n y_1 \in M_1^{;n}$ implies $\rho_n^q a_2 = (\rho_n b)^q \in M_2^{;n}$. So $(\rho_n b x^n)^q = 1$ for some $x \in M_2$ and $\rho_n b \zeta^j \in M_2^{;n}$ for some j, contradiction. This completes the proof of the claim and (2.3).

(2.4) So we now have A_1 henselian, $\mathrm{res}\, A_1 = \mathrm{res}\, M_1$ and $\mathrm{val}\, A_1$ pure in $\mathrm{val}\, M_1$. Since $\mathrm{val}\, M_1$ is a $\mathbb{Z}$-group and $\mathrm{val}\, A_1$ has the same unit, this implies that $\mathrm{val}\, A_1$ is a $\mathbb{Z}$-group as well. Hence by Ax–Kochen–Ershov $A_1 \preccurlyeq M_1$ as valued fields, so that clearly $\mathscr{A}_1 \preccurlyeq \mathscr{M}_1$. Now, since $\mathscr{M}_2$ is ω_1-saturated, it follows that f extends to an embedding $\mathscr{M}_1 \hookrightarrow \mathscr{M}_2$. □

The argument related to uniqueness of p-adic closures lies in part (2.3) of the preceding proof.

Theorem 3.8 can be deduced from the Main Theorem in [27] as follows. The setting is a 2-sorted language for valued fields, with additional sorts R_k, $k \in \omega$, for the residue rings $V/(t^{k+1})$. By Variant 4.5 (*ibid.*) with $1_\Gamma = v(t)$, $q = t$, $E_n = \{u_{n,j}t : 1 \leq j \leq \delta'(n)\}$ and $C = \emptyset$, there is a primitive recursive procedure to eliminate the base field quantifiers. To get rid of the R_k sorts for $k > 0$, we replace the R_k-variables (terms) by R_0-variables (terms), using the basic idea that an element of R_k is essentially determined by a finite sum $y_0 + y_1 t + \cdots + y_k t^k$, $v(y_i) = 0$. The problem is to do this in T'. Now for any non-principal ultrafilter $\mathscr{F}$ on the set of primes the ultraproducts $\prod \mathbb{Q}_p/\mathscr{F}$ and $\prod \mathbb{F}_p((T))/\mathscr{F}$ are elementarily equivalent as valued fields. So, given a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ and $k > 0$ there is a bound $N(f)$ and polynomials $g \in \mathbb{Z}[Y_1, \ldots, Y_n]$, $Y_i = (Y_{i1}, \ldots, Y_{ik})$, such that for all $p > N(f)$ the condition $R_k \models f(x_1, \ldots, x_n) = 0$ is equivalent (in T') to a finite set of conditions $R_0 \models g(y_1, \ldots, y_n) = 0$, where, e.g., if $x_i \equiv \sum z_j t^j \bmod t^{k+1}$, then $\bar{z}_j = y_{ij}$, those equations being obtained by identifying R_k with $R_0[T]/(T^{k+1})$, T transcendental over R_0, $\mathrm{char}\, R_0 = 0$. This $N(f)$ can be obtained primitive recursively as in [10, Section 5], or even explicitly by [6]. In this way we can replace the R_k-quantifiers by R_0-quantifiers. Clearly this procedure is still primitive recursive. This brings us into conditions similar to those of Theorem 4.2 (*ibid.*) allowing the transfer of (primitive recursive) E.Q.

from (the theory of...) the value group and the residue field to the whole structure. Hence we get Theorem 3.8 from axiom (7) of T' together with standard E.Q. for $\mathbb{Z}$-groups on the one hand, and the Sol_n predicates together with Lemma 3.2 on the other hand. It is well known that the theory of $\mathbb{Z}$-groups admits primitive recursive E.Q. It is also known that a primitive recursive E.Q. procedure exists for the elementary theory of finite fields, as given by [16], and that it can be put in the formalism of Lemma 3.2. Putting everything together we conclude that T' admits primitive recursive elimination of quantifiers in $\mathscr{L}'$.

One sees that a suitable version of Theorem 3.8 also holds for finite extensions of $\mathbb{Q}_p$ of a given degree d. The same kind of argument applies for the index of $P_n^{\cdot}$, etc. However there is no uniform bound for $[K^{\cdot}:P_n^{\cdot}]$ for arbitrarily large finite extensions $K/\mathbb{Q}_p$ for fixed n, even if p is fixed, so our method fails for such classes of local fields.

Example 3.9. Consider the index of $P_2^{\cdot}$ in $\mathbb{Q}_2(2^{1/2}), \ldots, \mathbb{Q}_2(2^{1/2^n}), \ldots$. Let $\alpha_n = 2^{1/2^n}$. The valuation ring of $\mathbb{Q}_2(\alpha_n)$ is $\mathbb{Z}_2[\alpha_n]$ and it suffices to look at the number of square roots of 1 mod α_n^{2n+1}. Now, e.g., consider $\mathbb{Q}_2(\alpha_2)$. A typical element of $\mathbb{Z}_2(2^{1/4})/(2 \cdot 2^{1/4})$ looks like $\sum_0^4 \lambda_i 2^{i/4}$, $\lambda_i \in \{0, 1\}$, and when it is squared the parameters λ_3, λ_4 disappear. So there are at least 2^2 square roots of 1. Similarly, there are at least 2^n square roots of 1 in $\mathbb{Z}_2[\alpha_n]/(\alpha_n^{2n+1})$. Hence $[\mathbb{Q}_2^{\cdot}(\alpha_n):P_n^{\cdot}] \geqslant 2^{n+1}$. A similar argument works for unramified extensions and any other p.

References

[1] J. Ax, The elementary theory of finite fields, Annals of Math. 88 (1968) 239–271.

[2] L. Bélair, The universal part of the theory of p-adically closed fields, Abstracts AMS, February 1984.

[3] L. Bélair, Spectres p-adiques en rang fini, C.R. Acad. Sci. Paris 305 (1987) 1–4.

[4] L. Bélair, Le théorème de Macintyre sur les ensembles définissables dans les corps p-adiques, Groupe d'Etude d'Analyse ultramétrique, 13e année (1985–86), Paris.

[5] L. Bröcker and J. H. Schinke, On the L-adic spectrum, Sch. Math. Inst. Univ. Münster 2, Ser. 40, 1986.

[6] S. S. Brown, Bounds on transfer principles for algebraically closed and complete discretely valued fields, Memoirs AMS 15 (1978) no. 204.

[7] C. Chang and J. Keisler, Model Theory (North-Holland, Amsterdam, 1973).

[8] G. Cherlin, Model Theoretic Algebra, Lecture Notes in Math. 521 (Springer, Berlin, 1976).

[9] G. Cherlin and M. Dickmann, Real closed rings II. Model theory, Ann. Pure Appl. Logic 25 (1983) 213–231.

[10] P. Cohen, Decision procedures for real and p-adic fields, Comm. Pure Appl. Math. 22 (1969) 131–151.

[11] F. Delon, Quelques propriétés des corps valués en théorie des modèles, Thèse d'Etat, Université de Paris VII, 1981.

[12] J. Denef, The rationality of the Poincaré series associated to the p-adic points on a variety, Invent. Math. 77 (1984) 1–23.

[13] J. Denef, P-adic semi-algebraic sets and cell decomposition, Crelle J. 369 (1986) 154–166.

[14] M. Fried, L-series on a Galois stratification, Preprint.

[15] M. Fried and M. Jarden, Field Arithmetic (Springer, Berlin, 1986).
[16] M. Fried and G.S. Sacerdote, Solving Diophantine problems over all residue class fields of a number field and all finite fields, Ann. of Math. (2) 104 (1976) 203–233.
[17] C. Kiefe, Sets definable over finite fields, their zeta-functions, Trans. AMS 223 (1976) 45–59.
[18] S. Kochen, Model Theory of local fields, *Logic Colloquium '74, Kiel,* Lecture Notes in Math. 499 (Springer, Berlin, 1975).
[19] A. Macintyre, On definable subsets of p-adic fields, J. Symbolic Logic 41 (1976) 605–610.
[20] A. Macintyre, K. McKenna and L.V.D. Dries, Elimination of quantifiers in algebraic structures, Adv. in Math. 47 (1983) 74–87.
[21] A. Prestel and P. Roquette, Formally p-adic Fields, Lecture Notes in Math. 1050 (Springer, Berlin, 1984).
[22] P. Ribenboim, Théorie des Valuations (Presses de l'Université de Montréal, Montréal, 1964).
[23] E. Robinson, Affine schemes and p-adic geometry, Thesis, Cambridge, Dec. 1983.
[24] E. Robinson, The p-adic spectrum, J. Pure Appl. Algebra 40 (1986) 281–297.
[25] E. Robinson, The geometric theory of p-adic fields, J. Algebra 110 (1987) 158–172.
[26] J.H. Schinke, Das (p, d)-adische spektrum, Thesis, Munster, 1985.
[27] W. Weispfenning, Quantifier elimination and decision procedure for valued fields, Logic Colloquium '83, Aachen, Lecture Notes in Math. 1103 (Springer, Berlin, 1986).