The Journal of Symbolic Logic
Volume 82, Number 1, March 2017

THE FIELD OF p-ADIC NUMBERS WITH A PREDICATE FOR THE POWERS OF AN INTEGER

NATHANAËL MARIAULE

Abstract. In this paper, we prove the decidability of the theory of $\mathbb{Q}_p$ in the language $(+, -, \cdot, 0, 1, P_n(n \in \mathbb{N}))$ expanded by a predicate for the multiplicative subgroup $n^{\mathbb{Z}}$ (where n is a fixed integer). There are two cases: if $v_p(n) > 0$ then the group determines a cross-section and we get an axiomatization of the theory and a result of quantifier elimination. If $v_p(n) = 0$, then we use the Mann property of the group to get an axiomatization of the theory.

Let K be a p-adically closed field and $\mathcal{L} = (+, -, \cdot, 0, 1, P_n(n \in \mathbb{N}))$ be the language of p-adically closed fields (i.e., P_n is interpreted by the group of nth power). Let G be a multiplicative subgroup of $\mathbb{Q}_p$. What can be said about the theory of $Th(K, G_K)$ in the language $\mathcal{L}$ expanded by a unary predicate interpreted in $\mathbb{Q}_p$ as G? Can we give conditions on G so that we have axiomatization/decidability/quantifier elimination or quantifier simplification?

If K is real or algebraically closed, they are many results of this type: the first one is due to L. van den Dries [10], he considers the theory of $(\mathbb{R}, +, -, \cdot, 0, 1, <, 2^{\mathbb{Z}})$, gives a result of quantifier elimination, and proves the decidability of the theory. B. Zilber considers the case where G is the group of roots of unity in $\mathbb{C}$ (in the language of fields [13] or in the field of reals where $\mathbb{C}$ is identified with the $\mathbb{R}$-vector space of dimension 2 [14]). Later on these results were generalised by A. Günaydin and L. van den Dries [4] to subgroups of a real closed field or an algebraically closed field with the Mann property and by O. Belegradek and B. Zilber [1] for some subgroups of the unit circle in the field of reals. But so far, very little is known about the case of valued fields.

In this article, we will consider the case where $K = \mathbb{Q}_p$ and $G = n^{\mathbb{Z}}$, where n is a fixed integer. Unlike [10] (where 2 can be replaced by any natural number), we have two different cases: if $v_p(n) > 0$ then $n^{\mathbb{Z}}$ is a discrete subgroup (essentially it determines a cross-section) while if $v_p(n) = 0$ then $n^{\mathbb{Z}}$ is dense in a (definable) open subset of $\mathbb{Z}_p^*$. We will treat the first case in Section 1 in the special case $n = p$. In Section 3, we describe the second case (for $n = 1 + p$). For this we need some results on the theory of the additive group of integers with the p-adic valuation in the language of valued groups. These results are proved in Section 2. Finally in Section 4, we give a description of the definable sets in our theories.

Received July 21, 2015.
Key words and phrases. p-adically closed fields, expansion of valued fields.

0022-4812/17/8201-0010
DOI:10.1017/jsl.2016.22

Notation. Let A be a ring. We denote the set of invertible elements of A by A^*. If K is a valued field, we denote its value group by $v(K)$ or vK and its valuation ring by $\mathcal{O}_K$. K^h denotes the henselization of K. If Γ is an ordered set, $\gamma \in \Gamma$ then $\Gamma_{\geq\gamma}$ denotes the set of elements greater than γ in Γ.

Remark. Let K be a p-adically closed then for all $x, y \in K$,

$$v_p(x) \geq v_p(y) \text{ iff } y^2 + px^2 \text{ is a square in } K \text{ if } p \neq 2, \text{ and}$$
$$v_2(x) \geq v_2(y) \text{ iff } y^3 + 2x^3 \text{ is a cube in } K \text{ (for } p = 2).$$

So, in this context, we will consider $\mathcal{L}$-formulas using valuations even though the valuation symbol is not part of the language. Indeed, the valuation symbol can be replaced by (quantifier-free) formulas in the language $\mathcal{L}$ according to the above property.

§1. Case $n = p$. In the case $n = p$, the group $n^{\mathbb{Z}}$ is discrete in $\mathbb{Q}_p$. Therefore this case is similar to the structure $(\mathbb{R}, +, -, \cdot, 0, 1, <, 2^{\mathbb{Z}})$ from [10]. We follow the same strategy as that paper. The key property in our case is that $p^{\mathbb{Z}}$ is an isomorphic copy of the value group. Let $\mathcal{L}_p = (+, -, \cdot, 0, 1, P_n (n \in \mathbb{N}), A)$ be the language of p-adically closed fields expanded by a unary predicate A interpreted in $\mathbb{Q}_p$ by $p^{\mathbb{Z}}$. Let $pCF(p)$ be the $\mathcal{L}_p$-theory defined by: if $\mathcal{M} = (M, +, -, \cdot, 0, 1, P_n, A)$ is a model of $pCF(p)$ then

- $(M, +, -, \cdot, 0, 1, P_n)$ is a p-adically closed field;
- $(A, \cdot, 1)$ is a subgroup of $(M^*, \cdot, 1)$ and $p \in A$;
- $\forall x (x \neq 0 \rightarrow \exists! y A(y) \wedge v_p(x) = v_p(y))$.

Theorem 1.1. *$pCF(p)$ axiomatizes a complete theory.*

Therefore, $Th(\mathbb{Q}_p, +, -, \cdot, 0, 1, P_n, p^{\mathbb{Z}})$ is decidable.

Let $\mathcal{L}'_p$ be the expansion of $\mathcal{L}_p$ by a function symbol for $\lambda : M^* \longrightarrow A$ such that $\lambda(x)$ is the unique element y of A such that $v_p(x) = v_p(y)$. Let $pCF(p)'$ be the expansion of $pCF(p)$ by the definition of λ.

Theorem 1.2. *$pCF(p)'$ admits the elimination of quantifiers.*

As any model of $pCF(p)$ has a unique expansion to a model of $pCF(p)'$, it is sufficient to prove the second theorem. We will use the following criterion of quantifier elimination (from [10]):

Proposition 1.3. *Let T be a $\mathcal{L}$-theory where $\mathcal{L}$ has at least one constant. Then T admits the elimination of quantifiers if*

(i) *for all models $\mathcal{M}$ of $T_\forall$, $\mathcal{M}$ admits a T-closure $\overline{\mathcal{M}}$ i.e., $\mathcal{M} \subset \overline{\mathcal{M}} \models T$ and $\overline{\mathcal{M}}$ can be embedded over $\mathcal{M}$ in any model of T that contains $\mathcal{M}$;*

(ii) *Let $\mathcal{M} \subsetneq \mathcal{N}$ be models of T then there is $b \in N \setminus M$ such that the $T_\forall$-model generated by $\mathcal{M}$ and b can be embedded over $\mathcal{M}$ in an elementary extension of $\mathcal{M}$.*

Proof of condition (i). Let $\mathcal{M} = (M, +, -, \cdot, 0, 1, P_k, A, \lambda)$ be a model of $T_\forall$ contained in $\mathcal{N} = (N, +, -, \cdot, 0, 1, Q_k, B, \mu)$ a model of $pCF(p)'$. Let $Frac\ M \subset N$ be the fraction field of M in N. Then $Frac\ M$ is closed under μ: $\mu(a/b) = \mu(a)/\mu(b) = \lambda(a)/\lambda(b) \in Frac\ M$. So $A_{Frac\ M} := B \cap Frac\ M = \{a/b \mid a, b \in A\}$. Let $\overline{M}$ be the p-adic closure of $Frac\ M$ in N (i.e., $\overline{M} = (Frac\ M)^h$ the henselization

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

of $Frac\ M$). Then as $v((Frac\ M)^h) = v(Frac\ M)$, $\overline{M}$ is closed under μ: if $x \in (Frac\ M)^h$ nonzero then there is $y \in Frac\ M$ such that $v(x) = v(y)$. So $\mu(y) = \mu(x) \in A_{Frac\ M}$. We take $\overline{\mathcal{M}} := (\overline{M}, +, -, \cdot, 0, 1, Q_k \cap \overline{M}, \mu, A_{Frac\ M})$ (where μ is restricted to $\overline{M}$).

Proof of condition (ii). Let $\mathcal{M} = (M, +, -, \cdot, 0, 1, P_n, A, \lambda) \subset \mathcal{N} = (N, +, -, \cdot, 0,\ 1,\ Q_n, B, \mu)$ be models of $pCF(p)'$. Let $\mathcal{M}' = (M', +, -, \cdot, 0, 1, {P'}_n, A', \lambda')$ be an elementary $|M|$-saturated expansion of $\mathcal{M}$. We want to find $b \in N \setminus M$ so that we can embed the $T_\forall$-expansion of $M(b)$ in $\mathcal{M}'$ over $\mathcal{M}$.

Case 1: if $v(M) = v(N)$ then $A = B$ and we can pick any $b \in N \setminus M$ and embed $M(b)$ over M: this is the classical quantifier elimination for p-adically closed fields (see [8]).

Case 2: if $v(M) \neq v(N)$, we make use of the proof of quantifier elimination in [8]. In particular, in this case (Lemma 4.7 in [8]), there exists $x \in N \setminus M$ such that $v(M(x)) = v(M) + v(x)\mathbb{Z} \subset v(N)$. Furthermore, $v(\sum a_i x^i) = \min\{v(a_i) + iv(x)\}$ for all $\overline{a}$ in M. Let b be the unique element of B such that $v(b) = v(x)$. Also, (Proposition 4.10B in [8]), there is $\eta \in v(M')$ which realizes the same type as $v(x)$ over $v(M)$ and if $z \in M'$ with $v(z) = \eta$ then the map $b \longmapsto z$ is an embedding of valued fields of $M(b)$ into M' over M. Let z be the unique element of A' with $v(z) = \eta$. Then we obtain an embedding in our language. This concludes the proof of Theorem 1.2. ⊣

Let us remark than in the two theorems of this section, we can replace the group $p^{\mathbb{Z}}$ by $n^{\mathbb{Z}}$ for any integer n with positive valuation. If $v_p(n) = k > 0$, we define the theory $pCF(n)$ using the same axioms as $pCF(p)$ where we replace the third axiom by $\forall x(x \neq 0 \rightarrow \exists! y A(y) \wedge v_p(x^k) = v_p(y))$. We define the map λ_n according to this new axiom and the proof of Theorem 1.1 and 1.2 are the same as in the case $n = p$.

§2. p-valued $\mathbb{Z}$-groups.

In the real case [4], the authors make use of results on the model theory of abelian densely ordered groups [9][12]. In this section, we prove similar results for a class of abelian groups with p-valuation.

Definition 2.1. Let G be an abelian group and $V : G \rightarrow \Gamma \cup \{\infty\}$ where Γ is a discrete totally ordered set with no largest element. We say that (G, V) is a p-valued group if for all $x, y \in G$ and all $n \in \mathbb{Z}$,

- $V(x) = \infty$ iff $x = 0_G$;
- $V(nx) = V(x) + v_p(n)$;
- $V(x + y) \geq \min\{V(x), V(y)\}$;

where v_p is the p-adic valuation, $nx = x + \cdots + x$ (n times) (if $n \in \mathbb{N}$), $nx = -nx$ (if $n < 0$) and $0x = 0_G$; if $x \in G$, $V(x) + k$ denotes the kth successor of $V(x)$ in $\Gamma \cup \{\infty\}$ (by convention the successor of ∞ is ∞).

Lemma 2.2. *Let (G, V) be a p-valued group. Then,*

(a) *G is torsion-free.*

(b) *For all $x, y \in G$, if $V(x) \neq V(y)$, then $V(x + y) = \min\{V(x), V(y)\}$.*

Proof. (a) Let $x \in G$. Assume that $nx = 0_G$. Then, $V(nx) = V(x) + v_p(n) = \infty$. So, $V(x) = \infty$ and $x = 0_G$.

(b) Assume that $V(x) < V(y)$. Then,

$$V(x) \geq \min\{V(x + y), V(-y)\}.$$

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

As $V(-y) = V(y) + v_p(-1)$, we have that

$$V(x) \geq V(x+y) \geq \min\{V(x), V(y)\} = V(x). \qquad \dashv$$

$(\mathbb{Z}, v_p)$ is a p-valued group. We want to describe the first-order theory of this structure. We will use a two-sorted language $\mathcal{L}_{pV} := ((+, -, 0_G, 1_G, \equiv_n\ (n \in \mathbb{N})), (0, \infty, S, <), V)$. The first sort will be $(\mathbb{Z}, +, -, 0, 1, \equiv_n)$ ($\equiv_n$ is interpreted by the congruences relation) and the second sort will be $(\mathbb{N} \cup \{\infty\}, 0, \infty, +1, <)$ and the function symbol V is interpreted by v_p. We also have the equality relation on each sort (though we do not specify these relations in the language). The first sort is called the group sort while the second is called the value sort (or value set).

We axiomatize $T_{p,\mathbb{Z}}$, the theory of p-valued $\mathbb{Z}$-groups as follows:
Let $((G, +, -, 0_G, 1_G, \equiv_n), (VG \cup \{\infty\}, 0, \infty, S, <), V)$ be a $\mathcal{L}_{pV}$-structure. Then it is a model for the theory $T_{p,\mathbb{Z}}$ iff the following conditions hold:

- $(G, +, -, 0_G, 1_G, \equiv_n)$ is a $\mathbb{Z}$-group i.e., an abelian group such that $0_G, 1_G, 1_G + 1_G, \dots, (n-1)\cdot 1_G$ form a set of representatives of the cosets of nG. This means that for all $x \in G$ and $n \in \mathbb{N}$ there is a unique $y \in G$ and a unique $0 \leq i < n$ such that $x = ny + i \cdot 1_G$. $x \equiv_n y$ iff $x - y \in nG$.
- $(VG, 0, <)$ is a discrete ordered set with first but no last element. 0 is the first element. ∞ is an element such that $x < \infty$ for all $x \in VG$. S is the successor function i.e., $S(x) = y$ iff $x \neq \infty$ and $x < y \leq z$ for all $z \in VG$ such that $x < z$, $S(\infty) := \infty$.
- $V : G \to VG \cup \{\infty\}$ satisfies the axioms of p-valued groups. Note that the second axiom in our language is written as $V(nx) = S(S(\cdots S(V(x))))$ where we compose S $v_p(n)$ times.
- $V(x) \geq n$ iff $x \in p^n G$ and for all x, y if $V(x) = V(y)$ then there is $1 \leq i < p$ such that $V(x - iy) > V(x) = V(y)$.
- G is regularly dense i.e., nG is dense in $\{x \in G \mid V(x - 0_G) \geq v_p(n)\}$ i.e.,

$$\forall x \in G\ V(x) \geq v_p(n) \to \left[\forall \gamma \geq v_p(n) \in VG \exists y \in nG\ V(x-y) = \gamma\right].$$

Remark. Let $n \in \mathbb{Z}$, $x \in G$. We say that n divides x if there is $y \in G$ such that $x = ny$. In this case, by uniqueness of the composition $x = ny + i \cdot 1_G$, y is unique.

Lemma 2.3. *Let (G, V) be a p-valued $\mathbb{Z}$-group. Then for all $n > 1$, 1_G is not n-divisible.*

Proof. Assume that $1_G = nx$ for some $x \in G \setminus \{0_G\}$. As $1_G = n0_G + 1_G$, we obtain a contradiction with the uniqueness of the decomposition, $1_G = ny + i \cdot 1_G$. ⊣

Note that for the rest of this paper, we will denote $i \cdot 1_G$ by i and the set $\{\dots, -2\cdot 1_G, -1\cdot 1_G, 0_G, 1\cdot 1_G, 2\cdot 1_G, \dots\}$ by $\mathbb{Z}$.

Theorem 2.4. *$T_{p,\mathbb{Z}}$ is complete and model-complete.*

As $((\mathbb{Z}, +, -, 0, 1, \equiv_n), (\mathbb{N} \cup \{\infty\}, 0, <, +1), v_p)$ is a prime model of this theory, it is actually sufficient to prove the model-completeness.

First, let us recall a classical result on system of congruences (in the ring of integers) that also holds for p-valued $\mathbb{Z}$-groups.

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

Proposition 2.5. *Let M be a p-valued $\mathbb{Z}$-group. Let $a_1, \cdots, a_k \in M$ (actually we can assume $a_i \in \mathbb{N}$). Then, the system*

$$\begin{cases} x \equiv_{n_1} a_1 \\ \quad \vdots \\ x \equiv_{n_k} a_k \end{cases}$$

has a solution in M iff $\gcd(n_i - n_j)$ divides $(a_i - a_j)$. In this case, the set of solution is of the type $x \equiv_{n^*} a^*$ for some $a^* \in M$ and $n^* = lcm(n_1, \cdots, n_k)$.

It is not hard to adapt classical proofs when $M = \mathbb{Z}$ to our more general case.

We will now prove the result of model-completeness. We will use Robinson's test i.e., we will show that if $M \subset M'$ are models of $T_{p,\mathbb{Z}}$ and if $\varphi(\overline{x}, \overline{y})$ is a quantifier-free formula, then for all $\overline{b}$ in M, $M \vDash \exists \overline{x} \varphi(\overline{x}, \overline{b})$ iff $M' \vDash \exists \overline{x} \varphi(\overline{x}, \overline{b})$. Let us remark that φ is a disjunction of systems of the type

$$(\alpha) \begin{cases} (\neg) \sum_j q_{ij} x_j = a_i (1 \leq i \leq T_1) & (1) \\ (\neg) V\left(\sum q_{ij} x_j - a_i\right) + n_i \,\square_i\, V\left(\sum r_{ij} x_j - b_i\right) + m_i \ (T_1 < i \leq T_2) & (2) \\ (\neg) \sum_j q_{ij} x_j \equiv_{N_i} a_i \ (T_2 < i \leq T_3), & (3) \end{cases}$$

where $\overline{a}, \overline{b}$ in M,$\overline{n}, \overline{m} \in \mathbb{Z}$,$\overline{q}, \overline{r} \in \mathbb{Z}$ and $\overline{N}, T_1, T_2, T_3 \in \mathbb{N}$ and $\square_i$ holds for $<$ or $=$ (depending on i). Say, $\varphi \equiv \bigvee_l (\alpha)_l$ where $(\alpha)_l$ is a system like above. Then we have to show that any $(\alpha)_l$ in φ realised in M' is realised in M i.e., the system $(\alpha)_l$ has a solution in M whenever it has a solution in M'.

First, let us start with a simple case: a single equation $mx = a$.

Lemma 2.6. *Let $M \subset M'$ be models of $T_{p,\mathbb{Z}}$ then M is a pure subgroup of M'*

Proof. Let $x \in M$ and assume that there is $y \in M'$ such that $x = ny$. Then there is $x_0 \in M$ and $0 \leq i < n$ such that $x = nx_0 + i$. By uniqueness of this decomposition (in M'), we find that $i = 0$ and $y = x_0$. ⊣

We will now reduce the complexity of the systems $(\alpha)_l$ at the price of a higher number of disjunctions in φ. Let $(\alpha) = (\alpha)_l$ be a disjunct in φ.

- We can remove inequalities in (1). Indeed, $x \neq 0$ is equivalent to $V(x) < \infty$ i.e., we replace inequalities by inequations of type (2).
- We can remove negations in (2). Indeed, $\neg V(x) = \gamma$ is equivalent to $V(x) < \gamma$ or $V(x) > \gamma$. So, if $\neg V\left(\sum q_{ij} x_j - a_i\right) + n_i = V\left(\sum r_{ij} x_j - b_i\right) + m_i$ appear in the system (α), let (α') be the system obtained when one remove $\neg V\left(\sum q_{ij} x_j - a_i\right) + n_i = V\left(\sum r_{ij} x_j - b_i\right) + m_i$ from (α). Then (α) is equivalent to

$$\left[(\alpha') \wedge V\left(\sum q_{ij} x_j - a_i\right) + n_i < V\left(\sum r_{ij} x_j - b_i\right) + m_i\right] \\ \vee \left[(\alpha') \wedge V\left(\sum q_{ij} x_j - a_i\right) + n_i > V\left(\sum r_{ij} x_j - b_i\right) + m_i\right].$$

  We replace $(\alpha) = (\alpha)_l$ by the above disjunction in φ. We repeat the argument for any equation of the type $\neg V(x) = \gamma$ in $(\alpha)_l$ and for all l. After rearranging the formula φ, we see that it is equivalent to a disjunction of formulas of type (α) where no negation of atomic formula of the type $\neg V(x) = \gamma$ appear. Similarly, $\neg V(x) < \gamma$ is equivalent to $V(x) = \gamma$ or $V(x) > \gamma$. So we may also assume that the system (α) does not contain any negation of this type.

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

- Similarly incongruences can be replaced by congruences as $x \not\equiv_n a$ iff $x \equiv_n a+i$ for some $0 < i < n-1$.

So, we have shown that we can assume that our formula φ is of the type $\varphi \equiv \bigvee_l (\alpha)_l$ where for all l, $(\alpha) := (\alpha)_l$ is of the type:

$$(\alpha)\begin{cases} \sum_j q_{ij}x_j = a_i(1 \leq i \leq T_1) & (1)\\ V\left(\sum q_{ij}x_j - a_i\right) + n_i \,\square_i\, V\left(\sum r_{ij}x_j - b_i\right) + m_i \;(T_1 < i \leq T_2) & (2)\\ \sum_j q_{ij}x_j \equiv_{N_i} a_i \;(T_2 < i \leq T_3). & (3)\end{cases}$$

We will now remove equalities (1) in the group sort in our system (α) (this step is the same as for ordered group see [12]):

As M, M' are torsion-free, their divisible closure is a $\mathbb{Q}$-vector space. Therefore, we can apply the usual theory of linear equations over vector spaces (e.g., Cramer's rules) to show that (1) is equivalent in M (and M') to one of the following case:

(a) $kx_i = c_i$, $c_i \in M$, $k \in \mathbb{Z}$ for all $1 \leq i \leq l := |\overline{x}|$;
(b) $kx_{m+j} = c_j + \sum_{i=1}^m k_{ij}x_i$ for all $0 < j \leq l-m$;
(c) The system (1) has no solution in M'.

In case (a), as M is a pure subgroup of M', any solution of (1) actually belongs to M. So, if (α) has a solution in M', it has a solution in M.

In case (b), we can remove (1) (at the price of extra congruences):

- Multiply by k each equation in (2) and (3) where x_{m+j} is involved. It means that we replace
$$V\left(\sum q_{ij}x_j - a_i\right) + n_i \,\square_i\, V\left(\sum r_{ij}x_j - b_i\right) + m_i$$
by
$$V\left(\sum k \cdot q_{ij}x_j - k \cdot a_i\right) + n_i + v_p(k) \,\square_i\, V\left(\sum k \cdot r_{ij}x_j - k \cdot b_i\right) + m_i + v_p(k)$$
and
$$\sum_j q_{ij}x_j \equiv_{N_i} a_i$$
by
$$\sum_j k \cdot q_{ij}x_j \equiv_{k \cdot N_i} k \cdot a_i$$
for all i such that q_{im+j} or r_{im+j} nonzero.
- Replace the variables kx_{m+j} by $c_j + \sum_{i=1}^m k_{ij}x_i$ in (2) and (3).
- Replace (3) by
$$\begin{cases} \sum_{j=1}^m q_{ij}x_j \equiv_{N_i} a_i \;(T_2 \leq i \leq T_3)\\ c_j + \sum_{j=1}^m k_{ij}x_i \equiv_k 0 \;(1 \leq j \leq l-m).\end{cases}$$
- Remove the equations (1) from the system (α).

Then the new system is equivalent to the old one i.e., any solution $x_1, \ldots, x_m$ of the new system induces a solution $x_1, \ldots, x_l$ of the old one (where x_{m+j} is uniquely determined thanks to the above rule (b) and the congruences $c_j + \sum k_{ij}x_i \equiv_k 0$). By the above discussion, we can assume that our system (α) is of the type:

$$(\alpha)\begin{cases} V\left(\sum q_{ij}x_j - a_i\right) + n_i \,\square_i\, V\left(\sum r_{ij}x_i - b_i\right) + m_i \;(1 \leq i \leq N) & (2)\\ \sum_j q_{ij}x_j \equiv_{N_i} a_i \;(1 \leq i \leq N). & (3)\end{cases}$$

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

Let $M \subset M'$ be models of $T_{p,\mathbb{Z}}$. Let $x_0 \in M' \setminus M$. We define

$$M\langle x_0\rangle := \{x \in M' \mid nx = mx_0 + y \text{ where } y \in M, n, m \in \mathbb{N}\}.$$

Lemma 2.7. *Let $M \subset M^*$ be p-valued $\mathbb{Z}$-groups. Let $c \in M^* \setminus M$. Then either $V(M\langle c\rangle) = V(M)$ or there exists $d \in M\langle c\rangle$ such that $M\langle c\rangle = M\langle d\rangle$ and $V(M\langle d\rangle) = V(M) \coprod V(d) \oplus \mathbb{Z}$.*

In the above lemma, $V(d) \oplus \mathbb{Z} := \{V(d) + n \mid n \in \mathbb{Z}\}$ and $\coprod$ denotes the disjoint union. $V(d) - k$ denotes the kth predecessor of $V(d)$ $(k \in \mathbb{N})$. We will prove in the lemma that such predecessor exists.

Proof. Assume that $V(M\langle c\rangle) \neq V(M)$. Then, there is $d \in M\langle c\rangle$ such that $V(d) \notin V(M)$. Say, $Nd = Lc + y$ for some $L, N \in \mathbb{Z}$, $y \in M$.

Claim 1. $M\langle c\rangle = M\langle d\rangle$.

It is sufficient by symmetry of the problem to show one inclusion. Let $x \in M\langle c\rangle$ then $nx = mc + z$ for some $m, n \in \mathbb{Z}$ and $z \in M$. So,

$$Lnx = mLc + Lz = mNd + Lz - my.$$

So, $x \in M\langle d\rangle$.

$V(M\langle d\rangle) \supseteq V(M) \coprod V(d) \oplus \mathbb{Z}$. Indeed, $V(p^n d) = V(d) + n$ for all n nonnegative and for all $n \in \mathbb{N}$ as $V(d) \geq n$ $(V(d) \notin VM)$, there is $d' \in M^*$ such that $d = p^n d'$. So $d' \in M\langle d\rangle$ and $V(d') = V(d) - n$. Note that $V(d) \oplus \mathbb{Z}$ is disjoint from $V(M)$. Otherwise, $V(d) + n \in V(M)$ for some n and therefore, $V(d) \in V(M)$.

Let $x \in M\langle d\rangle$. Then, $nx = md + y$ with $y \in M$. So, $V(nx) = V(md + y)$ i.e., $V(nx) = V(md)$ if $V(y) > V(d), m \neq 0$ and $V(nx) = V(y)$ otherwise. This implies that $V(x) \in V(M) \coprod V(d) \oplus \mathbb{Z}$.

So, $M\langle d\rangle = V(M) \coprod V(d) \oplus \mathbb{Z}$. ⊣

Lemma 2.8. *For all $x \in M\langle c\rangle$, for all $\gamma \in V(M\langle c\rangle)$ there is $y \in M\langle c\rangle$ such that $V(x - y) = \gamma$.*

Proof. Let $t \in M\langle c\rangle$ with $V(t) = \gamma$. Take $y = x + t$. ⊣

Lemma 2.9. *Let M' be a model of $T_{p,\mathbb{Z}}$ and M be a pure subgroup of M'. Let $a_1, \ldots, a_k \in M, n_1, \ldots, n_k, m_1, \ldots, m_k \in \mathbb{Z}, \gamma_1, \ldots, \gamma_k \in VM$. Let (α) be the system*

$$(\alpha)\begin{cases} V(X - a_i) + n_i \,\square_{ij}\, V(X - a_j) + m_j \ (1 \leq i \leq k) & (2)\\ V(X - a_i) \,\square_i\, \gamma_i \ (1 \leq i \leq k). & (3)\end{cases}$$

If (α) has a solution in M', then it has a solution in M. Furthermore, if c is a solution of the system in M such that $c \neq a_i$ and $c \neq b_i$ for all i then there is $\delta \in VM$ such that for all

$$y \in B(b, \delta) := \{z \in M \mid V(c - z) > \delta\}$$

y is a solution of (α).

Proof. Let x be a solution of (α) in M'. First if $V(x - a_i) \notin VM$ for some i. Then without loss of generality, we can assume that $x \in M\langle c\rangle \setminus M$ with $VM\langle c\rangle = VM \coprod V(c) \oplus \mathbb{Z}$ and $nx = lc + r$. So, $V(x - a_i) = \min\{V(lc), V(na_i - r)\} - v_p(n) = V(c) + v_p(l) - v_p(n)$ (as $V(x - a_i) \notin VM$). We will pick y such that $V(y - a_i) = \tilde{\gamma} \in VM$ with $\tilde{\gamma} < V(c)$ for some $\tilde{\gamma}$ large enough (to be determined) and $\tilde{\gamma} \,\square_i\, \gamma_i$. For fixed $\tilde{\gamma}$, we can find such a y by density. Then $V(x - y) = V(x - a_i + a_i - y) = \tilde{\gamma}$.

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

Let $j \neq i$. There are 3 cases:

(1) $V(x-a_j) > V(c)$ and $V(x-a_j) \in VM$. Therefore, $V(x-a_j) > V(c)+k$ for all $k \in \mathbb{Z}$. But, $V(nx-na_j) = V(lc+r-na_j) = \min\{V(lc), V(r-na_j)\}$. This gives a contradiction. Therefore this case never happens.

(2) $V(x-a_j) < V(c)$ and $V(x-a_j) \in VM$. Therefore, $V(x-a_j) < V(c)+k$ for all $k \in \mathbb{Z}$. So, the condition $V(x-a_i)+m_i \,\square_{ij}\, V(x-a_j)+n_j$ is of the type $V(x-a_i)+m_i > V(x-a_j)+n_j$. Take $\widetilde{\gamma}$ so that $V(c) > \widetilde{\gamma} > V(x-a_j)+n_j-m_i$. Then, $V(y-a_j) = V(y-x+x-a_j) = V(x-a_j)$. So, $V(y-a_i)+m_i \,\square_{ij}\, V(y-a_j)+n_j$ holds by choice of $\widetilde{\gamma}$.

(3) $V(x-a_j) \notin VM$. Then $V(x-a_j) = V(lc)-v_p(n) = V(x-a_i)$. So, $V(x-a_i)+n_i \,\square_{ij}\, V(x-a_i)+m_j$ is equivalent to $n_i \,\square_{ij}\, m_j$. So, it is sufficient that $V(y-a_j) = V(y-a_j)$. As we have $V(y-a_j) = V(y-x+x-a_j) = V(y-x) = \widetilde{\gamma} = V(y-a_i)$, this is the case.

So, we see that $\widetilde{\gamma}$ needs to satisfy only finitely many conditions

$$\widetilde{\gamma} > V(x-a_j)+n_j-m_i \qquad \widetilde{\gamma}\,\square_i\,\gamma_i,$$

for all j such that situation (2) holds. And as $V(lc)-v_p(n)$ satisfies these conditions, it is obvious that we can find $\widetilde{\gamma}$ such that these conditions holds: take $\widetilde{\gamma} < V(c)$ large enough in VM.

Now, if $V(x-a_i) \in VM$ for all i. Then, without loss of generality we can assume that $\gamma := V(x-a_1) = \cdots = V(x-a_k) > V(x-a_i)$ for all $i > k$. If we find y such that $V(y-a_j) = V(x-a_j)$ for all j we are done. For it is sufficient to find y such that $V(y-a_j) = \gamma$ for all $j \leq k$. Indeed, in this case if $l > k$, $V(y-a_l) = V(y-x+x-a_l) = V(x-a_l)$ as $V(x-y) = V(x-a_1+a_1-y) > V(x-a_l)$.

(1) If $V(x) > \gamma$ then $V(a_i) = \gamma$ for all $i \leq k$ and we just have to pick y such that $V(y) > \gamma$.

(2) If $V(x) = \gamma$ then if we find y such that $V(y) = \gamma$ then for all $i \leq k$ such that $V(a_i) > \gamma$, $V(y-a_i) = \gamma$. So we can assume that $V(a_i) = \gamma$ for all $i \leq k$ if we require the extra-condition on y: $V(y) = V(y-a_i) = \gamma$. By the axioms of p-valued $\mathbb{Z}$-groups there is $0 < i < p$ such that $V(x-ia_1) > \gamma$. As $V(x-a_1) = \gamma$, $i > 1$. Take $y = ia_1$. Then $V(y-x) > \gamma$ and for all $1 < j \leq k$, $V(y-a_j) = V(y-x+x-a_j) = V(x-a_j)$. Also, $V(y-a_1) = V(ia_1-a_i) = V(a_1)+v_p(i-1) = \gamma$ and $V(y) = V(ia_1) = V(a_1) = \gamma$. This complete the proof of the first assertion.

Let $c \in M$ be a solution of (α) distinct from a_i, b_i. Let $\delta = \max\{V(c-a_i), V(c-b_i)\}+1 < \infty$. Let $z \in B(c,\delta)$. Then,

$$V(z-a_i) = \min\{V(z-c), V(c-a_i)\} = V(c-a_i).$$

Similarly, $V(z-b_i) = V(c-b_i)$ and therefore z is a solution of (α) ⊣

PROPOSITION 2.10. *Let M^*, N^* be models of $T_{p,\mathbb{Z}}$, M, N be pure subgroups of M^* and N^* resp. Assume that N^* is $|M|$-saturated. Let $h : M \longrightarrow N$ be an isomorphism of p-valued groups. Let $a \in M^* \setminus M$. Then there is $b \in N^* \setminus N$ such that for all $n \in \mathbb{N}, k \in \mathbb{Z}, x \in M, \gamma \in VM$*

$$ka - x \equiv_n 0 \text{ iff } kb - h(x) \equiv_n 0) \tag{1}$$

$$V(ka-x)\,\square\,\gamma \text{ iff } V(kb-h(x))\,\square\,h(\gamma). \tag{2}$$

Furthermore h can be extended to an isomorphism of p-valued groups $\widetilde{h} : M\langle a\rangle \longrightarrow N\langle b\rangle$ such that $\widetilde{h}(a) = b$.

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

Proof. To prove the existence of b it is sufficient to prove that the partial type

$$\begin{aligned} p(y) =&\{ky - h(x) \equiv_n 0 \mid \ M^* \vDash ka - x \equiv_n 0, x \in M, k, n \in \mathbb{Z}\} \\ &\cup \{V(ky - h(x)) \,\square\, h(\gamma) \mid \ M^* \vDash V(ka - x) \,\square\, \gamma, x \in M, \gamma \in VM, k \in \mathbb{Z}\} \end{aligned}$$

is finitely satisfied in N^* (by $|M|$-saturation) i.e., that any finite collection of formulas in p, say

$$\begin{cases} \qquad k_i y - h(x_i) \equiv_{n_i} 0 \; (1 \leq i \leq T) & (a) \\ V(k_i y - h(x_i)) \,\square\, h(\gamma_i) \; (1 \leq i \leq T) & (b) \end{cases}$$

is realised in N^*. First, let us remark that $V(k_i y - h(x_i)) < +\infty$. Indeed, if this is not the case, then $k_i y - h(x_i) = 0$ i.e., $k_i a - x_i = 0$. As M is a pure subgroup of M^*, this implies that $a \in M$. Then, we multiply each equation in (a) and (b) by $\prod_{j \neq i} k_j$. Then the above collection of formulas is equivalent to

$$\begin{cases} y - h(\prod_{j \neq i} k_j x_i) \equiv_{n_i \prod_{j \neq i} k_j} 0 (1 \leq i \leq T) & (a) \\ y \equiv_K 0 & (a_2) \\ V(y - h(\prod_{j \neq i} k_j x_i)) \,\square\, h(\gamma_i) + v_p(\prod_{j \neq i} k_j)(1 \leq i \leq T), & (b) \end{cases}$$

where $K = \prod_i k_i$. Then by Proposition 2.5 $(a) - (a_2)$ is equivalent to

$$y \equiv_S h(x)$$

for some $x \in M$ and $S = lcm(n_i \prod_{j \neq i} k_j, K)$. Let (α) be the system

$$\begin{cases} V(y - h(x)) \geq v_p(S) & (a') \\ V(y - h(\prod_{j \neq i} k_j x_i)) \,\square\, h(\gamma_i) + v_p(\prod_{j \neq i} k_j)(1 \leq i \leq N). & (b') \end{cases}$$

By Lemma 2.9 and its proof, the existence of a solution of (α) only depends on the centres and on the radii. As these centres and radii belongs to N and as (the image by h^{-1} of) the system is realised in M^*, it is realised in N^*. Furthermore, let c be a solution of the system (α) then there is a ball B such that any element of B is a solution of (α). As B is contained in $B(h(x), v_p(S))$ and by regular density, the set of points in N^* congruent to $h(x)$ modulo S is dense in B. Take b in B such that $b - h(x) \equiv_S 0$. Then b is a solution of (a) and (b).

It remains to prove that $\widetilde{h}$ is indeed an isomorphism. It is not hard to see that this is in fact a morphism of groups.

$\widetilde{h}$ is a morphism of p-valued groups: If $V(M\langle a \rangle) = V(M)$, there is nothing to show: By condition (2), for all $x \in M\langle a \rangle$, $V(h(x)) = h(\gamma)$, where $\gamma = V(x)$. So let assume that $V(M\langle a \rangle) \neq V(M)$. Then, we can assume that $V(M\langle a \rangle) = V(M) \coprod V(a) \oplus \mathbb{Z}$ (if necessary change a and b like in Lemma 2.7). Let $x, y \in M\langle a \rangle$.

Then $nx = ka + c$ and $my = la + d$ for some $n, m, k, l \in \mathbb{Z}$ and $c, d \in M$. We have to show that

$$V(x) \,\square\, V(y) \text{ iff } V(\widetilde{h}(x)) \,\square\, V(\widetilde{h}(y)).$$

If $V(y) = \gamma \in V(M)$, (then $V(\widetilde{h}(y)) = h(\gamma)$ by condition (2)), we have

$$\begin{aligned} V(x) \,\square\, \gamma \quad & \text{iff} \quad V(nx) \,\square\, \gamma + v_p(n) \\ & \text{iff} \quad V(ka + c) \,\square\, \gamma + v_p(n) \\ & \text{iff} \quad V(kb + h(c)) \,\square\, h(\gamma + v_p(n)) \\ & \text{iff} \quad V(\widetilde{h}(x)) \,\square\, \widetilde{h}(\gamma) \\ & \text{iff} \quad V(\widetilde{h}(x)) \,\square\, V(\widetilde{h}(y)). \end{aligned}$$

If $V(x), V(y) \notin V(M)$, then $V(x) + v_p(n) = V(a) + v_p(k)$ and $V(y) + v_p(m) = V(a) + v_p(l)$. So,

$$V(x) \square V(y) \text{ iff } v_p(k) + v_p(m) \square v_p(l) + v_p(n).$$

Similarly, $V(\widetilde{h}(x)) + v_p(n) = V(b) + v_p(k)$ and $V(\widetilde{h}(y)) + v_p(m) = V(b) + v_p(l)$. So,

$$V(\widetilde{x}) \square V(\widetilde{y}) \text{ iff } v_p(k) + v_p(m) \square v_p(l) + v_p(n).$$

$\widetilde{h}$ is surjective: let $y \in N\langle b\rangle$. Then $ny = kb + h(c)$ for some $n, k \in \mathbb{Z}$ and $c \in M$. Therefore, $ny = kb + h(c)$ iff $kb + h(c) \equiv_n 0$ iff $ka + c \equiv_n 0$ iff there is $x \in M^*$ such that $nx = ka + c$. Then $\widetilde{h}(x) = y$.

$\widetilde{h}$ is injective: let $x, x' \in M\langle a\rangle$. Then $nx = ka + c$ and $n'x' = k'a + c'$. Let us note that as M is a pure subgroup of M^*, we can assume that $(k, n) = (k', n') = 1$. Assume that $\widetilde{h}(x) = \widetilde{h}(x')$. Then, $nn'\widetilde{h}(x) = nn'\widetilde{h}(x')$. So, $n'kb + n'h(c) = nk'b + nh(c)$. Therefore $(n'k - nk')b = nh(c) - n'h(c)$. As $b \notin N$, it implies that $n'k = nk'$. So as $(n, k) = (n', k') = 1$, $n = n'$ and $k = k'$. So $n'h(c) - nh(c') = 0$. Therefore $c = c'$ and $x = x'$. ⊣

We can now prove the model-completeness result:

Proof. Let $M \subset M'$ be models of $T_{p,\mathbb{Z}}$. By the discussion of the beginning of this section, it is sufficient to prove that the following system

$$(\alpha) \begin{cases} V\left(\sum q_{ij}x_j - a_i\right) + n_j \square_j V\left(\sum r_{ij}x_j - b_i\right) + m_j \; (1 \leq i \leq N) & (2) \\ \sum_j q_{ij}x_j \equiv_{N_i} a_i \; (1 \leq i \leq N) & (3) \end{cases}$$

(where $a_i, b_i \in M$, $q_{ij}, r_{ij}, n_j, m_j, N_i \in \mathbb{Z}, N \in \mathbb{N}$) has a solution in M if it has a solution in M'. Let $\overline{d}$ be a solution of the system in M', say $\overline{d} \in M\langle c_1, \ldots, c_l\rangle$. Let M^* be a $|M'|$-saturated elementary extension of M. Then, if we apply inductively Proposition 2.10, we can construct an elementary embedding of $M\langle c_1, \ldots, c_l\rangle$ into M^*. So the system (α) has a solution in M^* and therefore in M. ⊣

Using Proposition 2.10, one can also prove:

Corollary 2.11. *$T_{p,\mathbb{Z}}$ admits the elimination of quantifiers.*

Remark. In the late stage of the redaction of this paper, the author was informed that the quantifier elimination and a similar axiomatization have been proved independently by F. Guignot [3].

§3. **Case $n = (1 + p)$.** Unless specified, in this section, we assume that $p \neq 2$. First, we will see that $(1 + p)^{\mathbb{Z}}$ carries the structure of a p-valued $\mathbb{Z}$-group. Furthermore, we will also see that this structure is axiomatizable in the language of p-adically closed fields. Let $n \in \mathbb{Z}$ then

$$(1 + p)^n = exp(\log(1 + p)n),$$

where exp, log are the p-adic exponential (resp. p-adic logarithm). Let us note that this is well-defined as $p \neq 2$. As $v_p(exp(x) - 1) = v_p(x)$ and $v_p(\log(1 + x)) = v_p(x)$ for all $x \in p\mathbb{Z}_p$,

$$v_p((1 + p)^n - 1) = v_p(n) + 1.$$

So, we can define a structure of p-valued group: let

$$V : (1+p)^{\mathbb{Z}} \longrightarrow \mathbb{N} \cup \{\infty\} : x \longmapsto v_p(x-1)-1.$$

Then $((1+p)^{\mathbb{Z}}, V)$ is a p-valued $\mathbb{Z}$-group (isomorphic to $(\mathbb{Z}, v_p)$.

Let $\mathcal{L}_{1+p} = (+, -, \cdot, 0, 1, P_n (n \in \mathbb{N}), U, \equiv_n \ (n \in \mathbb{N}))$ (where U is a predicate interpreted in $\mathbb{Q}_p$ by $(1+p)^{\mathbb{Z}}$). Let (K, G) be a $\mathcal{L}_{1+p}$-structure. Assuming that K is p-adically closed we can express the property that G is a p-valued $\mathbb{Z}$-group in the language $\mathcal{L}_{1+p}$. As the p-adic valuation ring is definable in the language of rings we can interpret a map

$$V_K : G \longrightarrow vK \cup \{\infty\} : x \longmapsto v\left(\frac{x-1}{p}\right),$$

which coincides with the map V on $(1+p)^{\mathbb{Z}}$. Then one can express in the language $\mathcal{L}_{1+p}$ that (G, V) is a p-valued $\mathbb{Z}$-group:

- $(G, \cdot, 1, (1+p), \equiv_n)$ is a $\mathbb{Z}$-group can be expressed in the language of rings and with the predicates $\equiv_n$. These latters are interpreted in G by $x \equiv_n y$ iff there is $g \in G$ such that $x = g^n y$ (as we are now using multiplicative notation for the group operation);
- $(VG, 0, <)$ is a discrete ordered set with first but no last element. For these axioms, we express that $VG = vK_{\geq 0}$ i.e.,

$$\forall x \left[v(x) \geq 0 \rightarrow \exists y U(y) \wedge v(x) = v\left(\frac{y-1}{p}\right)\right],$$

  or more formally

$$\forall x \left[P_2(1+px^2) \rightarrow \exists y U(y) \wedge P_2\left(x^2 + p\left(\frac{y-1}{p}\right)^2\right) \wedge P_2\left(\left(\frac{y-1}{p}\right)^2 + px^2\right)\right].$$

  Then $(VG, 0, <)$ is a discrete ordered set as K is p-adically closed. Note that the successor function is determined by $S(V(x)) = V(x^p)$.
- $V : G \longrightarrow VG \cup \{\infty\}$ satisfies the axioms of p-valued groups can be also expressed using the predicates P_n. We proceed similarly for the rest of the axioms.

A crucial property of $(1+p)^{\mathbb{Z}}$ that will be used in our axiomatization is that this group satisfies Mann property. We define now this property: let K be a field and G a subgroup of its multiplicative group. Let $a_1, \dots, a_n$ nonzero in the prime field of K and consider the equation

$$a_1 x_1 + \cdots + a_n x_n = 1.$$

A solution $(g_1, \dots, g_n)$ in G of this equation is called nondegenerate if $\sum_{i \in I} a_i g_i \neq 0$ for all non-empty $I \subset \{1, \dots, n\}$. We say that G has the Mann property (in K) if any equation like above has finitely many nondegenerate solutions in G. This property was isolated by H. Mann [7] who proved that U the group of roots of unity in $\mathbb{C}$ has Mann property. More generally, any multiplicative group of finite rank in any field of characteristic zero has Mann property; see [2, 6, 11] (where the rank of an abelian group G is the dimension of the $\mathbb{Q}$-vector space $\mathbb{Q} \otimes G$ where G is seen as a $\mathbb{Z}$-module and the tensor product is over $\mathbb{Z}$). In particular, $a^{\mathbb{Z}}$ has the Mann

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

property for any a in a field of characteristic zero. An alternative proof for the Mann property of $a^{\mathbb{Z}}$ is given in [4]. This last proof has the advantage to be effective (this is necessary to prove that our theory is decidable).

A part of the axiomatization says that is that if (K, G) is a model of the theory of $(\mathbb{Q}_p, (1+p)^{\mathbb{Z}})$ then G has the same nondegenerate solutions as in $(1+p)^{\mathbb{Z}}$. Formally, let $a_1, \ldots, a_n \in \mathbb{Q}^*$ and let $\overline{g}_1 := (g_{11}, \ldots, g_{1n}), \ldots, \overline{g}_k$ be the list of the nondegenerate solutions in $(1+p)^{\mathbb{Z}}$ of the equation

$$a_1 x_1 + \cdots + a_n x_n = 1.$$

The corresponding Mann axiom is

$$\forall \overline{y} \left[\left(\bigwedge_i U(y_i) \wedge \sum_i a_i y_i = 1 \wedge \bigwedge_{\varnothing \neq I \subset \{1,\ldots,n\}} \sum_{i \in I} a_i y_i \neq 0 \right) \rightarrow \bigvee_{i=1}^{k} \overline{y} = \overline{g}_i \right].$$

In [4], the authors prove the following results that will be useful later:

Lemma 3.1 (Lemmas 5.12 and 5.13 in [4]). *Let Γ be a subgroup of G such that for all $a_1, \ldots, a_n \in \mathbb{Q}^*$ the equation $a_1 x_1 + \cdots + a_n x_n = 1$ has the same nondegenerate solutions in Γ as in G. Then we have for any $g, g_1, \ldots, g_n \in G$:*

- *if g is algebraic over $\mathbb{Q}(\Gamma)$ of degree d then $g^d \in \Gamma$;*
- *if $g_1, \ldots, g_n$ are algebraically dependent over $\mathbb{Q}(\Gamma)$ then they are multiplicatively dependent over Γ.*

If furthermore Γ is pure in G. Then $G \cap \mathbb{Q}(\Gamma) = \Gamma$ and $\mathbb{Q}(G)$ is a purely transcendental extension of $\mathbb{Q}(\Gamma)$.

The second property from [4] that we will use is the notion of smallness. In general, this notion can be defined as follow: let $\mathcal{L}$ be a language, let $\mathcal{M} = (M, \ldots)$ be a $\mathcal{L}$-structure and $G \subset M$. By $f : X \xrightarrow{n} Y$ we denote a map from X to the subsets of Y of size at most n. We say that G is large in M if there is $f : M^m \xrightarrow{n} M$ definable such that $f(G^m) := \bigcup_{x \in G^m} f(x) = M$. We say that G is small if G is not large. In particular, if $|M|$ is infinite and $|G| < |M|$ then G is small. So, $(1+p)^{\mathbb{Z}}$ is small in $(\mathbb{Q}_p, +, \cdot, 0, 1, P_n)$. Note that if M is a p-adically closed field (so we have definable Skolem functions) then we can assume that the map f in the definition of large is of the type $f : M^m \longrightarrow M$. Furthermore, the property of smallness is first-order: we can axiomatize this property in $\mathcal{L}(U)$ where U is a predicate interpreted in M by G. The axioms are as follow: for all $\mathcal{L}(U)$-formula $\Phi(\overline{x}, y, \overline{z})$, we add

$$\forall \overline{z} \left[(\forall \overline{x} \exists ! y \Phi(\overline{x}, y, \overline{z})) \rightarrow \exists y \forall \overline{x}\, U(\overline{x}) \wedge \neg \Phi(\overline{x}, y, \overline{z}) \right].$$

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

In the main theorem of this section, we will use the following consequence of smallness:

Lemma 3.2. *Let $K \subset K'$ be p-adically closed fields. Let G be a subgroup of K'^* such that G is small in K'. Assume that K' is $|K|$-saturated (in the language of p-adically closed fields expanded by a predicate for G). Then $K(G)^h \neq K'$.*

Proof. We show that the type *transcendental over* $K(G)$ is realised in K^*. Let $p(x)$ be the type consisting of the formulas

$$\forall \overline{g} \in G^l f(\overline{g}, x) := \sum_j \left(\sum_i a_{ij} g_i \right) x^j \neq 0$$

for all $\overline{a}$ in K. Let us show that this type is finitely satisfiable. Then by saturation it is realised in K'. Note that any realisation of p is transcendental over $K(G)$. Assume that this is not the case. Then there is $f_1(\overline{z}, y), \ldots, f_n(\overline{z}, y)$ polynomials in $K[\overline{Z}, Y]$ such that for all $y \in K$ there is $\overline{g} \in G$ such that $f_i(\overline{g}, y) = 0$ for some i. Let

$$F : K'^m \xrightarrow{n} K' : \overline{x} \longmapsto \{y \in K' \mid \vee_i f(\overline{x}, y) = 0\}.$$

So, $F(G^n) = K'$ i.e., G is large in K': contradiction. $\dashv$

Remark. In the above lemma, we can also pick the transcendental number such that it realises a fixed cut over K (i.e., the set of formulas $v(x - a) \Box \gamma$ with $a \in K$, $\gamma \in vK$ satisfied by a fixed element in a saturated expansion of K). For, like in the lemma, we can show (by contradiction) that G is large in a ball B definable with parameters in K (for any ball B that determines the cut). Then as B is large in K', we would obtain that G is large in K'.

Let $pCF(1+p)$ be the theory determined by: if $(K, G, +, -, \cdot, 0, 1, P_n, \equiv_n \ (n \in \mathbb{N}))$ is a model of $pCF(1 + p)$ then

- $(K, +, \cdot, 0, 1, P_n)$ is a p-adically closed field;
- $1_G := (1+p) \in G$, (G, V) is a p-valued $\mathbb{Z}$-group (where $V(g) = v_p(g-1)-1$) and $V : G \to vK_{\geq 0}$ is surjective;
- G is dense in $1 + p\mathcal{O}_K$;
- (K, G) satisfies the Mann axioms of $(1 + p)^{\mathbb{Z}}$;
- G is small in K.

Problem. *If K is algebraically closed or real closed and G is a subgroup of K^* with the Mann property then it is proved in* [4] *that G is small. Is it also the case if K p-adically closed*?

Theorem 3.3. $pCF(1 + p) = Th(\mathbb{Q}_p, (1 + p)^{\mathbb{Z}}, +, -, \cdot, 0, 1, P_n, \equiv_n)$.

The proof is now a straightforward translation of the proof of theorem 7.1 in [4] for real closed fields. In the proof, we will use the notions of free, linearly disjoint and regular extensions. We refer to [5] for the definitions and properties.

Proof. Let $(K, G), (L, H)$ be two models of $pCF(1 + p)$ κ-saturated for some $\kappa > \aleph_0$. Let $Sub(K, G)$ be the collection of $\mathcal{L}_{1+p}$-structures (K', G') where

- K' is a p-adically closed field, $|K'| < |K|$;
- G' is a pure p-valued subgroup of G;
- K' and $\mathbb{Q}(G)$ are free over $\mathbb{Q}(G')$.

$Sub(L, H)$ is defined similarly. Let Γ be the set of isomorphisms between elements of $Sub(K, G)$ and $Sub(L, H)$. Then Γ is non-empty since $(\mathbb{Q}^h, (1+p)^{\mathbb{Z}})$ is in $Sub(K, G)$ and $Sub(L, H)$. It remains to prove that Γ is a back-and-forth system to prove the theorem. Let $\imath : (K', G') \longrightarrow (L', H')$ in Γ. Let $\alpha \in K \setminus K'$. We have to find an extension of $\imath$ which contains α in its domain. There are three cases:

(1) $\alpha \in G$. We need to find $\beta \in H$ such that β realises the same $\mathbb{Z}$-type over H' as $tp_{\mathbb{Z}}(\alpha/G')$ (i.e., the formulas of Proposition 2.10) and β realises the same cut as α over K' (i.e., the set of formulas $v_p(x - \imath(c)) \square \imath(\gamma)$ such that $(K', G') \vDash v_p(\alpha - c) \square \gamma$ for all $c \in K', \gamma \in vK'$). By density of G in $1 + p\mathcal{O}_K$, we can assume that the cut of α over K' is determined by the cut over G': indeed, $v_p(\alpha - c) \square \gamma$ iff $v_p(\alpha - g) \square \gamma$ for all $g \in G$ such that $v_p(g - c) > \gamma$. (Note that if $c \notin 1 + p\mathcal{O}_K$, then $v_p(\alpha - c) = 0$ if $v_p(c) \geq 0$ and $v_p(\alpha - c) = v(c)$ otherwise i.e., in this case the valuation does not depends on the choice of $\alpha \in G$.) Furthermore, $v_p(\alpha - g) = v_p(\alpha g^{-1} - 1) = V_G(\alpha - g) + 1$. So, the cut in the group determines the cut in the field. Let β given by Proposition 2.10. Let $K'' = K'(\alpha)^h$, $G'' = G \cap K''$, $L'' = L'(\beta)^h$ and $H'' = H \cap L''$. By the properties of p-valued $\mathbb{Z}$-groups, p-adically closed fields and Lemma 3.1, $(K'', G'') \in Sub(K, G)$ and $(L'', H'') \in Sub(L, H)$ and we have an isomorphism $\imath' : (K'', G'') \longrightarrow (L'', H'')$.

(2) $\alpha \in K'(G)^h$. Then, $\alpha \in K'(g_1, \dots, g_n)^h$ and we can apply case (1) n times.

(3) $\alpha \notin K'(G)^h$. Consider the cut of α over K'. By saturation and smallness of H, $L'(H)^h \neq L$ and there is $\beta \in L \setminus L'(H)$ which realises the corresponding cut (remark following Lemma 3.2). Take $K'' = K'(\alpha)^h$, $L'' = L'(\beta)^h$. Note that by Lemma 3.1 $\mathbb{Q}(G)$ is a regular extension of $\mathbb{Q}(G')$ and thus K' and $\mathbb{Q}(G)$ are linearly disjoint over $\mathbb{Q}(G')$. By linear disjointness, we can extend $\imath$ to an isomorphism $\imath' : (K'', G') \longrightarrow (L'', H') : \alpha \longmapsto \beta$. The freeness of K'' and $\mathbb{Q}(G)$ over $\mathbb{Q}(G')$ follows from the assumption that $\alpha \notin K'(G)^h$. $\dashv$

Let us note that the above theorem can be adapted for any $n \in \mathbb{Z}$:

If $n = 1 + x$ where $v_p(x) > 0$. Then this is immediate: we can define the valuation $V(g)$ by $v_p(g - 1) - v_p(x)$ as $v_p((1 + x)^n) - 1) = v_p(\log(1 + x)) + v_p(n)$. Then one can adapt the axiomatization $pCF(1 + x)$ in a obvious way and prove an equivalent to the above theorem.

If $n = i + x$ where $1 < i < p$ and $v_p(x) > 0$ then there is $k \in \mathbb{N}$ such that $(i + x)^k = 1 + y$ with $v(y) > 0$ (take k minimal for this property). So, (K, G) is a model of $Th(\mathbb{Q}_p, (1 + x)^{\mathbb{Z}})$ iff (K, G^k) is a model of $pCF(1 + y)$.

If $p = 2$, for $n = 1 + p^2$, we have that $v_p((1 + p^2)^n - 1) = v_p(exp(\log(1 + p^2)n) - 1) = v_p(n) + 2$. So one can proceed like for the case $n = (1 + p)$, $p \neq 2$: define $pCF(1 + p^2)$ using the same set of axioms and prove the above theorem in the same way. Similarly, if $n = (1 + x)$ where $v_2(x) > 1$. For $n = (1 + x)$ with $v_2(x) = 1$, let us remark that $n^2 = (1 + 2x + x^2)$ and $v_p(2x + x^2) = 2$. So, (K, G) is a model of $Th(\mathbb{Q}_2, (1 + x)^{\mathbb{Z}})$ iff (K, G^2) is a model of $pCF(1 + 2x + x^2)$.

§4. Definable sets. In the case $v_p(n) > 0$, we can use the result of quantifier elimination to describe definable sets. In particular,

PROPOSITION 4.1. *The $\mathcal{L}_p$-definable sets in $\mathbb{Q}_p$ are boolean combinations of open sets and discrete countable sets.*

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

In the case $v_p(n) = 0$, we don't have a result of quantifier elimination but it is straightforward to adapt the description from [4]:

Let (K, G) be a model of $pCF(1+p)$. Let $\mathcal{L}_{pV}(\Sigma)$ be the expansion of $\mathcal{L}_{pV}$ (see Section 2) by predicates $\Sigma_{\overline{k}}$ for all $\overline{k} \subset \mathbb{Z}$ interpreted in G by: for all $\overline{g} \subset G$

$$\Sigma_{\overline{k}}(\overline{g}) \leftrightarrow k_1 g_1 + \cdots + k_n g_n = 0.$$

Let $\mathcal{L}_{1+p}(\Sigma) = (+, -, \cdot, 0, 1, P_n, U, \equiv_n \ (n \in \mathbb{N}), \Sigma_{\overline{k}}(\overline{k} \subset \mathbb{Z}))$. Note that $\mathcal{L}_{pV}(\Sigma)$ is not a sublanguage of $\mathcal{L}_{1+p}(\Sigma)$ but any symbol of the language $\mathcal{L}_{pV}(\Sigma)$ is quantifier-free definable in $\mathcal{L}_{1+p}(\Sigma)$. Let Φ be a $\mathcal{L}_{pV}(\Sigma)$-formula. Then the U-restriction Φ_U is:

- If Φ is atomic, $\Phi_U = \Phi$;
- If $\Phi = \neg\Phi'$, $\Phi_U = \neg\Phi'_U$;
- If $\Phi = \Phi' \vee \Phi''$ (resp. $\Phi = \Phi' \wedge \Phi'$), $\Phi_U = \Phi'_U \vee \Phi''_U$ (resp. $\Phi_U = \Phi'_U \wedge \Phi''_U$);
- If $\Phi = \exists x \Phi'$ (resp. $\Phi = \forall x \Phi'$), $\Phi_U = \exists x U(x) \wedge \Phi'_U$ (resp. $\Phi_U = \forall x U(x) \wedge \Phi'_U$).

In other words, for all $\overline{g}$ in G,

$$G(\Sigma) \vDash \Phi(\overline{g}) \text{ iff } (K, G) \vDash \Phi_U(\overline{g}),$$

where $G(\Sigma)$ is the $\mathcal{L}_{1+p}(\Sigma)$-expansion of the $\mathcal{L}_{1+p}$-structure G. A special formula in $\overline{x}$ is a $\mathcal{L}_{1+p}(\Sigma)$-formula of the type

$$\exists \overline{y}\, U(\overline{y}) \wedge \Phi_U(\overline{y}) \wedge \theta(\overline{x}, \overline{y}),$$

where Φ is a $\mathcal{L}_{pV}(\Sigma)$-formula and θ is a $\mathcal{L}_{1+p}$-formula.

Lemma 4.2. *Each $\mathcal{L}_{1+p}(\Sigma)$-formula $\Psi(\overline{x})$ is equivalent in $pCF(1+p, \Sigma)$ to a boolean combination of special formulas in $\overline{x}$.*

The proof is word for word the same as Lemma 7.6 in [4].

Proof. Let (K, G) and (L, H) be two $\aleph_1$-saturated models of $pCF(1+p, \Sigma)$. Let $\overline{\alpha} \in K^n$ and $\overline{\beta} \in L^n$ satisfying the same special formulas in $\overline{x}$. Then, it is sufficient to prove that $tp_{(K,G)}(\overline{\alpha}) = tp_{(L,H)}(\overline{\beta})$. Let Γ be the back-and-forth system of Theorem 3.3. We have to find $\imath \in \Gamma$ such that $\imath(\overline{\alpha}) = \overline{\beta}$.

Assume that $\mathbb{Q}(G)(\alpha)$ has transcendence degree r over $\mathbb{Q}(G)$.

Then $\mathbb{Q}(H)(\beta)$ has transcendence degree r over $\mathbb{Q}(H)$. Indeed, suppose this is not the case. Then without loss of generality we can assume that $\alpha_1, \dots, \alpha_r$ are algebraically independent over $\mathbb{Q}(G)$ and $\beta_1, \dots, \beta_r$ are algebraically dependent over $\mathbb{Q}(H)$. Say $\beta_r \in \mathbb{Q}(H)(\beta_1, \dots, \beta_{r-1})^{alg}$. Then there is a formula $\varphi(\overline{x}, \overline{y})$ and $\overline{h}$ in H such that

$$(L, H) \vDash \varphi(\overline{h}, \beta_1, \dots, \beta_r) \wedge \exists^{\leq n} x_r \varphi(\overline{h}, \beta_1, \dots, \beta_{r-1}, x_r),$$

i.e.,

$$(L, H) \vDash \exists \overline{y}\, U(\overline{y}) \wedge \varphi(\overline{y}, \beta_1, \dots, \beta_r) \wedge \exists^{\leq n} x_r \varphi(\overline{y}, \beta_1, \dots, \beta_{r-1}, x_r).$$

So (the last formula is a special formula),

$$(K, G) \vDash \exists \overline{y}\, U(\overline{y}) \wedge \varphi(\overline{y}, \alpha_1, \dots, \alpha_r) \wedge \exists^{\leq n} x_r \varphi(\overline{y}, \alpha_1, \dots, \alpha_{r-1}, x_r).$$

This is a contradiction.

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

Let $G' = \{g_1, g_2, \dots\}$ be a countable subgroup of G such that $G'(\Sigma) \preceq G(\Sigma)$ and α has transcendence degree r over $\mathbb{Q}(G')$.
Let $\theta_1, \dots, \theta_n$ be $\mathcal{L}_{pV}(\Sigma)$-formulas and $\Phi_1, \dots, \Phi_k$ be $\mathcal{L}$-formulas such that

$$G(\Sigma) \vDash \theta_i(\overline{g}) \text{ and } K \vDash \Phi_j(\overline{\alpha}, \overline{g}), \quad (*)$$

i.e.,

$$(K, G) \vDash \exists \overline{y}\, U(\overline{y}) \wedge \theta_U(\overline{y}) \wedge \Phi(\overline{\alpha}, \overline{y}),$$

where $\theta = \wedge_i \theta_i$ and $\Phi = \wedge_i \Phi_i$. So,

$$(L, H) \vDash \exists \overline{y}\, U(\overline{y}) \wedge \theta_U(\overline{y}) \wedge \Phi(\overline{\beta}, \overline{y}).$$

Then,

$$\{U(\overline{y})\} \cup \{\theta_U(\overline{y})\} \cup \{\Phi(\overline{\beta}, \overline{y})\}$$

(where we take all formulas θ_U and Φ that satisfy $(*)$) forms a partial type over $\overline{\beta}$. Let $\overline{h} = (h_1, h_2, \dots)$ be a realization of this type in (L, H). Then there is a partial elementary map between $G(\Sigma)$ and $H(\Sigma)$ sending g_i to h_i. Let $H' = \{h_i\}$. Then H' is a subgroup of H such that $H'(\Sigma) \preceq H(\Sigma)$ and β has transcendence degree r over $\mathbb{Q}(H')$. And we have an isomorphism $\imath$ between $\mathbb{Q}(G')(\overline{\alpha})$ and $\mathbb{Q}(H')(\overline{\beta})$ sending α_i to β_i and g_i to h_i. Let $K' = \mathbb{Q}(G')(\overline{\alpha})^h$ and $L' = \mathbb{Q}(H')(\overline{\beta})^h$. Then $(K', G') \in Sub(K, G)$, $(L', H') \in Sub(L, H)$ and $\imath \in \Gamma$. This concludes the proof of the lemma. ⊣

Theorem 4.3. *Every definable subset of (K, G) is a boolean combination of subsets of K^n defined by formulas $\exists \overline{y}\, U(\overline{u}) \wedge \Phi(\overline{x}, \overline{y})$ where $\Phi(\overline{x}, \overline{y})$ is quantifier-free in the language of p-adically closed fields.*

Again the proof is similar to the Theorem 7.5 in [4].

Proof. We know by the last lemma that any formula is equivalent to a special formula in $\overline{x}$ i.e., formula of the type

$$\Psi(\overline{x}) \equiv \exists \overline{y}\, U(\overline{y}) \wedge \theta_U(\overline{y}) \wedge \Phi(\overline{x}, \overline{y}).$$

By quantifier elimination for p-valued $\mathbb{Z}$-groups

$$\{\overline{g} \in G^n \mid G \vDash \theta(\overline{g})\}$$

is equivalent to a boolean combination of

(1) $\{\overline{g} \mid \xi_{\overline{k}}(\overline{g}) := g_1^{k_1} \cdots g_n^{k_n} = 1\}$;
(2) $\{\overline{g} \mid V(\xi_{\overline{k}}(\overline{g})) + r \,\square\, V(\xi_{\overline{k'}}(\overline{g})) + s\}$;
(3) $\{\overline{g} \mid \xi_{\overline{k}} \in (1 + p)^i G^n\}$.

As any of these $\mathcal{L}_{pV}$-definable set is definable using a quantifier-free $\mathcal{L}$-formula and existential quantifiers over G and by quantifier elimination for p-adically closed field, Ψ is equivalent to

$$\Psi'(\overline{x}) \equiv \exists \overline{z}\, U(\overline{z}) \wedge \Phi'(\overline{x}, \overline{z}),$$

where Φ' is a quantifier-free $\mathcal{L}$-formula. ⊣

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press

§5. Acknowledgements. During the preparation of this paper the author was supported by the grant *Italian FIRB 2010, Nuovi sviluppi nella Teoria dei Modelli dellesponenziazione.*

REFERENCES

[1] O. Belegradek and B. Zilber, *The model theory of the field of reals with a subgroup of the unit circle*. ***Journal of the London Mathematical Society***, vol. 78 (2008), no. 3, pp. 563–579.

[2] J. H. Evertse, *On sums of S-units and linear recurrences*. ***Composition Mathematica***, vol. 53 (1984), no. 2, pp. 225–244.

[3] F. Guignot, *Théorie des modèles du groupe valué* $(\mathbb{Z}, +, v_p)$, ***Séminaires de structures algébriques ordonnées***, no. 89 (2014), preprint.

[4] A. Günaydin and L. van den Dries, *The fields of real and complex numbers with a small multiplicative group*. ***Proceedings of the London Mathematical Society***, vol. 93 (2006), no. 1, pp. 43–81.

[5] S. Lang, ***Algebra***, third ed., Springer, Berlin, 2002.

[6] M. Laurent, *Équations diophantiennes exponentielles*. ***Inventiones Mathematicae***, vol. 78 (1984), pp. 299–327.

[7] H. Mann, *On linear relations between roots of unity*. ***Mathematika***, vol. 12 (1965), pp. 101–117.

[8] A. Prestel and P. Roquette, ***Formally p-adic fields***, Springer, Berlin, 1984.

[9] A. Robinson and E. Zakon, *Elementary properties of ordered abelian groups*. ***Transactions of the American Mathematical Society***, vol. 96 (1960), pp. 222–236.

[10] L. van den Dries, *The field of reals with a predicate for the powers of two*. ***Manuscripta mathematica***, vol. 54 (1985), pp. 187–195.

[11] A. J. van der Poorten and H.P. Schlickewei, *Additive relations in fields*. ***Journal of the Australian Mathematical Society***, vol. 51 (1991), pp. 154–170.

[12] E. Zakon, *Generalized archimedean groups*. ***Transactions of the American Mathematical Society***, vol. 99 (1961), pp. 21–40.

[13] B. Zilber, *A note on the model theory of the complex field with roots of unity*, available at www.maths.ox.ac.uk/∼zilber, 1990.

[14] ———, *Complex roots of unity on the real plane*, available at www.maths.ox.ac.uk/∼zilber, 2003.

INSTITUT DE MATHÉMATIQUES DE JUSSIEU - PARIS RIVE GAUCHE
UNIVERSITÉ PARIS DIDEROT
75205 PARIS CEDEX 13, FRANCE
E-mail: nathanael.mariaule@imj-prg.fr

https://doi.org/10.1017/jsl.2016.22 Published online by Cambridge University Press