A VERSION OF p-ADIC MINIMALITY

RAF CLUCKERS AND EVA LEENKNEGT

Abstract. We introduce a very weak language $\mathcal{L}_p$ on $\mathbb{Q}_p$, which is just rich enough to have the same definable subsets of the line $\mathbb{Q}_p$ than one has using the ring language. We prove that the only definable functions in the language $\mathcal{L}_p$ are trivial functions. We further give a definitional expansion $\mathcal{L}'_p$ of $\mathcal{L}_p$ in which $\mathbb{Q}_p$ has quantifier elimination and we obtain a weak cell decomposition. Our language $\mathcal{L}_p$ can serve as the p-adic analogue of the very weak language $(<)$ on the real numbers to define a notion of minimality on the p-adics. Finally we give a universal-existential definition, in the ring language, of $\mathbb{Z}_p$ inside $\mathbb{Q}_p$ and of $\mathbb{F}_p[[t]]$ inside $\mathbb{F}_p((t))$, which works uniformly in all p, and in all finite field extensions.

1. Introduction and main results

In nowadays common usage of terminology, for $\mathcal{L}$ an expansion of a first order language $\mathcal{L}_0$, an $\mathcal{L}$-structure K is called $\mathcal{L}_0$-minimal if and only if every $\mathcal{L}$-definable subset of the line K is already $\mathcal{L}_0$-definable, where definable means with parameters from the model K. When the property holds for all the models K of an $\mathcal{L}$-theory $\mathcal{T}$, then $\mathcal{T}$ is called $\mathcal{L}_0$-minimal. Famous examples of this kind are o-minimality, minimality, C-minimality, P-minimality, and so on. Note that among the existing notions of minimality that make sense on the p-adic number field, namely P-minimality [8] and b-minimality [4], only P-minimality follows the mentioned common usage of terminology.

We introduce here a very weak language $\mathcal{L}_p$ on $\mathbb{Q}_p$, which is just rich enough to have the same definable subsets of the line $\mathbb{Q}_p$ as with the ring language (the definable sets in the ring language are called semi-algebraic sets). It is thus a natural candidate for a notion of p-adic minimality for languages on $\mathbb{Q}_p$ expanding $\mathcal{L}_p$, where the advantage over P-minimality is that weaker languages than the ring language are allowed (whereas for P-minimality the basic language already contains the ring language). The language $\mathcal{L}_p$ is a very weak language in particular because the only definable functions in the language are trivial ones: we show that any $\mathcal{L}_p$-definable function $X \subset \mathbb{Q}_p^n \to \mathbb{Q}_p$ is piecewise a coordinate projection or a constant function, where the pieces can be taken $\mathcal{L}_p$-definable. The language $\mathcal{L}_p$ is a p-adic analogue of the very basic language $(<)$ of totally ordered structures which is used on the real numbers to define the general notion of o-minimal structures.

2010 *Mathematics Subject Classification.* Primary 03C10, 11U05, 03C07; Secondary 03C64.

Key words and phrases. p-adic numbers, quantifier elimination, cell decomposition, P-minimality, o-minimality, Hilbert's Tenth Problem, definability.

Further we give a definitial expansion $\mathcal{L}'_p$ of $\mathcal{L}_p$ in which $\mathbb{Q}_p$ has quantifier elimination and we prove a weak cell decomposition theorem. We also discuss Skolem functions, the definable sets up to definable bijection, and the dimension of definable sets.

Let us be more precise. Consider the following basic semi-algebraic sets, for all positive integers m and n

$$Q_{n,m} := \{x \in \mathbb{Q}_p \mid x = p^{an}(1 + p^m y) \text{ for some } a \in \mathbb{Z} \text{ and some } y \in \mathbb{Z}_p\}.$$

On the field $\mathbb{Q}_p$ of p-adic numbers consider for all positive integers m and n the predicates $R_{n,m}$ in three p-adic variables given by

$$R_{n,m}(x, y, z) \text{ if and only if } y - x \in zQ_{n,m}.$$

Let $\mathcal{L}_p$ be the first order language consisting of the predicates $R_{n,m}$ for all positive integers n and m. By definable we will always mean definable with parameters from the model.

Furthermore consider the language $\mathcal{L}'_p$ which is $\mathcal{L}_p$ together with for each integer k the predicate D_k in three p-adic variables given by

$$D_k(x, y, z) \text{ holds if and only if } z \neq y \text{ and } \operatorname{ord}(x - y) < \operatorname{ord}(z - y) + k.$$

1. **Proposition.** *The language $\mathcal{L}'_p$ is a definitional expansion of $\mathcal{L}_p$. Namely, each $\mathcal{L}'_p$-definable set is already $\mathcal{L}_p$-definable. Moreover, $\mathbb{Q}_p$ allows quantifier elimination in the language $\mathcal{L}'_p$.*

The following is a natural candidate definition for a minimality notion on $\mathbb{Q}_p$ (following the usual practice for notions of minimality), certainly in view of Proposition 2.

1.1. **Definition.** Let $\mathcal{L}$ be any language on $\mathbb{Q}_p$ expanding $\mathcal{L}_p$. Say that the $\mathcal{L}$-structure $\mathbb{Q}_p$ is $\mathcal{L}_p$-minimal if and only if all $\mathcal{L}$-definable subsets of $\mathbb{Q}_p$ are already $\mathcal{L}_p$-definable. Say that the theory of $(\mathbb{Q}_p, \mathcal{L})$ is $\mathcal{L}_p$-minimal if and only if all $\mathcal{L}$-definable subsets of K are already $\mathcal{L}_p$-definable, where K is any structure which is elementary equivalent to $(\mathbb{Q}_p, \mathcal{L})$.

By the cell decomposition result of [2] for subanalytic sets (or, alternatively, by the P-minimality result for the subanalytic structure on $\mathbb{Q}_p$ of [7] and the cell decomposition result of [5]), one finds the following.

2. **Proposition.** *The subanalytic structure on $\mathbb{Q}_p$ is $\mathcal{L}_p$-minimal and has $\mathcal{L}_p$-minimal theory. Hence, any intermediary structure between the structure $\mathcal{L}_p$ and the subanalytic structure on $\mathbb{Q}_p$ is $\mathcal{L}_p$-minimal and has $\mathcal{L}_p$-minimal theory.*

Further, all P-minimal structures on $\mathbb{Q}_p$ have $\mathcal{L}_p$-minimal theory (but not the other way around). Some of the intermediary structures between the structure $\mathcal{L}_p$ and the subanalytic structure on $\mathbb{Q}_p$ are known to have cell decomposition, for example, the semi-affine expansion of $\mathcal{L}_p$ by Liu [10], or any of the analytic structures of [3] on $\mathbb{Q}_p$.

We now turn our attention to cells in the language $\mathcal{L}'_p$.

1.2. **Definition.** An $\mathcal{L}'_p$-cell $A \subset \mathbb{Q}_p^k \times \mathbb{Q}_p$ is a set of the form

$$A = \{(x,t) \in D\times\mathbb{Q}_p \mid \operatorname{ord} p^{\ell_1}(a_1-c)\ \square_1\ \operatorname{ord}(t-c)\ \square_2\ \operatorname{ord} p^{\ell_2}(a_2-c),\ t-c \in \lambda Q_{n,m}\},$$

where $x = (x_1, \dots x_k)$, the ℓ_i are integers, the set D equals the image under the projection of A to $\mathbb{Q}_p^k$ and is a quantifier free $\mathcal{L}'_p$-definable subset of $\mathbb{Q}_p^k$, $\square_1$ and $\square_2$ denote '$<$' or 'no condition', $\lambda \in \mathbb{Q}_p$, the a_i and c are either one of the variables $x_1, \dots, x_k$ or a constant from $\mathbb{Q}_p$, and, the $a_i - c$ do not vanish on D. We call c the center of A, and D the base of A.

Clearly, any $\mathcal{L}'_p$-cell is an $\mathcal{L}'_p$-definable set. Note however that the above functions $p^{k_1}(a_1 - c)$ and $p^{k_2}(a_2 - c)$ are not necessarily $\mathcal{L}'_p$-definable functions in $x \in D$, see Proposition 4. For this reason, we will speak of weak cell decomposition (as opposed to cell decomposition).

The following is the main technical result of the paper.

3. **Proposition** (Weak Cell Decomposition)**.** *Every $\mathcal{L}'_p$-definable subset X of $\mathbb{Q}_p^k\times\mathbb{Q}_p$ can be partitioned into finitely many $\mathcal{L}'_p$-cells.*

Proposition 3 allows us to establish the triviality of $\mathcal{L}_p$-definable functions.

4. **Proposition.** *Any $\mathcal{L}_p$-definable function $f : X \subset \mathbb{Q}_p^k \to \mathbb{Q}_p$ is piecewise a coordinate projection or a constant function, where the pieces can be taken $\mathcal{L}_p$-definable.*

By providing two examples in Section 3 we show that $\mathcal{L}_p$ does not have definable Skolem functions, and that the classification of [2] for semi-algebraic and subanalytic sets does not analogously hold for $\mathcal{L}_p$-definable sets. Of course, all results in this paper could be formulated, with the necessary adaptations, for any finite field extension of $\mathbb{Q}_p$. However, to clarify the theory of $(\mathbb{Q}_p, \mathcal{L}_p)$ is a delicate matter and we leave this to the future. Remark 3.3 gives that structures with $\mathcal{L}_p$-minimal theory have a well-behaved dimension invariant.

In the final section we give a universal-existential definition, in the ring language, of $\mathbb{Z}_p$ inside $\mathbb{Q}_p$ and of $\mathbb{F}_p[[t]]$ inside $\mathbb{F}_p((t))$, which works uniformly in all p, and also uniformly in all finite field extensions. Previously, Poonen and Koenigsmann obtained and used an existential-universal definition [11], [9] of $\mathbb{Z}_p$ in $\mathbb{Q}_p$.

2. The proofs

The following is the main technical lemma.

2.1. **Lemma.** *Let C_1, C_2 be $\mathcal{L}'_p$-cells with centers c_1, resp. c_2. Then $C_1 \cap C_2$ can be partitioned into a finite union of $\mathcal{L}'_p$-cells A each of which has a center which is a restriction of either c_1 or of c_2.*

Proof. By partitioning C_1 and C_2 further if necessary, we may suppose that they both use $Q_{n,m}$ with the same positive integers m, n, that is, that C_i is of the form

$$\{(x,t) \in D_i\times\mathbb{Q}_p \mid \operatorname{ord} p^{k_{1i}}(a_{1i}-c_i)\ \square_{1i}\ \operatorname{ord}(t-c_i)\ \square_{2i}\ \operatorname{ord} p^{k_{2i}}(a_{2i}-c_i),\ t-c_i \in \lambda_i Q_{n,m}\}$$

for $i=1,2$, where the symbols have their meaning as in Definition 1.2. Up to a finite partition, we may suppose that on C_1 one of the following conditions holds for $k = 1+m+n+\sum_{i,j=1,2}|k_{ij}|$ and some integer ℓ_1 with $-k \le \ell_1 \le k$

$$\begin{array}{rcll} \operatorname{ord}(t-c_1) & > & \operatorname{ord}(c_2-c_1)+k, & (\mathrm{I})_k \\ \operatorname{ord}(t-c_1) & < & \operatorname{ord}(c_2-c_1)-k, & (\mathrm{II})_k \\ \operatorname{ord}(t-c_1)+\ell_1 & = & \operatorname{ord}(c_2-c_1). & (\mathrm{III})_{\ell_1} \end{array}$$

Note that $(\mathrm{I})_k$ and $(\mathrm{II})_k$ imply respectively

$$\begin{array}{rcccll} \operatorname{ord}(t-c_1) & > & \operatorname{ord}(c_2-c_1)+k & = & \operatorname{ord}(t-c_2)+k, & (\mathrm{i})_k \\ \operatorname{ord}(t-c_2) & = & \operatorname{ord}(t-c_1) & < & \operatorname{ord}(c_1-c_2)-k. & (\mathrm{ii})_k \end{array}$$

If $(\mathrm{I})_k$ holds on C_1, put

$$W = \{x \in D_2 \mid \operatorname{ord} p^{k_{12}}(a_{12}-c_2) \,\square_{12}\, \operatorname{ord}(c_1-c_2) \,\square_{22}\, \operatorname{ord} p^{k_{22}}(a_{22}-c_2)\}.$$

Then one has

$$C_1 \cap C_2 = \{(x,t) \in (W \times \mathbb{Q}_p) \cap C_1 \mid c_1 - c_2 \in \lambda_2 Q_{n,m}\},$$

which is easily seen to be a finite disjoint union of $\mathcal{L}'_p$-cells of the desired form. If $(\mathrm{II})_k$ holds on C_1, then we may suppose, up to partitioning C_2, that either $C_1 \cap C_2$ is empty, or, that $(\mathrm{ii})_k$ holds for all $(x,t) \in C_1$ and all $(x,t) \in C_2$. If now the intersection $C_1 \cap C_2$ is nonempty then $C_1 \cap C_2$ consists of all points $(x,t) \in (D_1 \cap D_2) \times \mathbb{Q}_p$ satisfying the conditions

$$\max_{i \in I}\{\operatorname{ord} p^{k_{1i}}(a_{1i}-c_i)\} < \operatorname{ord}(t-c_1) < \min_{i=1,2}\{\operatorname{ord} p^{k_{2i}}(a_{2i}-c_i)\},$$

and

$$t - c_1 \in \lambda_1 Q_{n,m},$$

where I consists of i such that $\square_{1i}$ is the condition $<$, and where the maximum over the emptyset is $-\infty$. If $\sharp I \ge 1$ we have to show that the function $x \mapsto \max_{i\in I}\{\operatorname{ord} p^{k_{1i}}(a_{1i}-c_i)\}$ is piecewise of the form $p^r(a-c_1)$, or of the form $p^r(a-c_2)$, for some integer r and some a being either a constant from $\mathbb{Q}_p$ or one of the variables x_i, and correspondingly for the minimum. If $\sharp I = 1$, this is easy, and if $\sharp I = 2$, then one has

$$\operatorname{ord}(a_{12}-c_2) = \operatorname{ord}(a_{12}-c_1),$$

by $(\mathrm{ii})_k$ and since $C_1 \cap C_2$ is nonempty. The minimum is treated likewise: one has, again by $(\mathrm{ii})_k$ and since $C_1 \cap C_2$ is nonempty, that

$$\operatorname{ord}(a_{22}-c_2) = \operatorname{ord}(a_{22}-c_1) \text{ and } \operatorname{ord}(a_{21}-c_2) = \operatorname{ord}(a_{21}-c_1),$$

which finishes the case $(\mathrm{II})_k$. We may suppose by symmetry (that is, up to reversing the role of C_1 and C_2) that, if $(\mathrm{III})_{\ell_1}$ holds on C_1, then also

$$\operatorname{ord}(t-c_1)+\ell_1 \;=\; \operatorname{ord}(c_2-c_1) \;=\; \operatorname{ord}(t-c_2)+\ell_2 \quad (\mathrm{iii})_\ell$$

holds with $\ell = (\ell_1, \ell_2)$ and $-k \le \ell_2 \le k$. Suppose again that $C_1 \cap C_2$ is nonempty. If one now fixes the residue classes of $c_2 - c_1$ and of $t - c_1$ modulo $Q_{2kn,2kn}$, then the conditions

$$\operatorname{ord}(c_2-c_1) = \operatorname{ord}(t-c_2)+\ell_2 \text{ and } t-c_2 \in \lambda_2 Q_{n,m}$$

follow automatically from $\operatorname{ord}(t-c_1)+\ell_1=\operatorname{ord}(c_2-c_1)$. Hence, one can easily partition $C_1\cap C_2$ into finitely many $\mathcal{L}'_p$-cells. $\square$

The previous lemma has the following consequence, which forms a part of Proposition 3.

2.2. **Lemma.** *Any quantifier-free $\mathcal{L}'_p$-definable subset of $\mathbb{Q}_p^{k+1}$ can be partitioned as a finite union of $\mathcal{L}'_p$-cells.*

Proof. By Lemma 2.1, it is enough to show that the sets (and complements of these sets)

$$\{x\in\mathbb{Q}_p^{k+1}\mid D_n(g_1,g_2,g_3)\}\quad\text{and}\quad\{x\in\mathbb{Q}_p^{k+1}\mid R_{n,m}(g_1,g_2,g_3)\},$$

with $g_i\in\{x_1,\dots,x_k,t\}\cup\mathbb{Q}_p$, can be partitioned as a finite union of $\mathcal{L}'_p$-cells, for integers $k,n\geq 0$ and $n,m\geq 1$. Since the $Q_{n,m}$ have finite index in $\mathbb{Q}_p^\times$, the situation for the relation $R_{n,m}$ is easy. To treat the relations D_n, it suffices to show that the set

$$A:=\{(x,t)\in\mathbb{Q}_p^{k+1}\mid \operatorname{ord}(t-c_1)<\operatorname{ord}p^n(t-c_2)\},$$

with $c_1,c_2\in\{x_1,\dots,x_k\}\cup\mathbb{Q}_p$, and $n\geq 0$, can be partitioned as a finite union of $\mathcal{L}'_p$-cells. We may suppose that $c_1\neq c_2$. Partition $\mathbb{Q}_p^{k+1}$ in the following way:

$$\begin{aligned}\mathbb{Q}_p^{k+1} &= \{(x,t)\in\mathbb{Q}_p^{k+1}\mid \operatorname{ord}(t-c_1)>\operatorname{ord}(c_1-c_2)\}\\ &\quad\cup\{(x,t)\in\mathbb{Q}_p^{k+1}\mid \operatorname{ord}(t-c_1)<\operatorname{ord}(c_1-c_2)\}\\ &\quad\cup\{(x,t)\in\mathbb{Q}_p^{k+1}\mid \operatorname{ord}(t-c_1)=\operatorname{ord}(c_1-c_2)\}.\end{aligned}\tag{2.2.1}$$

By working on these three parts separately, we can write A as a union of sets on which one of the conditions in (2.2.1) holds. For example, on

$$B:=A\cap\{(x,t)\in\mathbb{Q}_p^{k+1}\mid \operatorname{ord}(t-c_1)>\operatorname{ord}(c_1-c_2)\},$$

one has that $\operatorname{ord}(t-c_2)=\operatorname{ord}(c_1-c_2)$, and therefore B is equal to the set

$$B=\{(x,t)\in\mathbb{Q}_p^{k+1}\mid\operatorname{ord}(c_1-c_2)<\operatorname{ord}(t-c_1)<\operatorname{ord}p^n(c_1-c_2)\}$$

which is easily seen to be a finite disjoint union of $\mathcal{L}'_p$-cells. The other cases are similar. $\square$

Proof of Proposition 1. The quantifier elimination statement follows easily from Lemma 2.2 and the definition of $\mathcal{L}'_p$-cells. Indeed, by the cell decomposition theorem 3, it is sufficient to eliminate $\exists t$ from a condition $(x,t)\in A$, where $A\subset\mathbb{Q}_p^{k+1}$ is an $\mathcal{L}'_p$-cell. But the base of a cell is defined in a quantifier free way by Definition 1.2, and so we are done. It remains to show that $\mathcal{L}'_p$ is a definitional expansion of $\mathcal{L}_p$. Write $\lambda\sim_{3,1}\mu$ for $\lambda Q_{3,1}=\mu Q_{3,1}$. The relation $P(x,z)$ given by

$$(z-x)\sim_{3,1}z\not\sim_{3,1}x$$

is $\mathcal{L}_p$-definable and is equivalent with

$$\operatorname{ord}(z)<\operatorname{ord}(x)\wedge z\not\sim_{3,1}x.$$

Hence, the relation $\operatorname{ord}(x) \leq \operatorname{ord}(y)$ for x and y in $\mathbb{Q}_p$ is equivalent to

$$\forall z\big(P(x,z) \implies z-y \sim_{3,1} z\big).$$

Likewise, the relation $P(z-y, w-y)$ in y, z, w is $\mathcal{L}_p$-definable and is equivalent with

$$\operatorname{ord}(w-y) < \operatorname{ord}(z-y) \wedge w-y \not\sim_{3,1} z-y.$$

Hence, $\operatorname{ord}(z-y) < \operatorname{ord}(x-y)$ is equivalent with

$$\forall w\big(P(z-y, w-y) \implies w-x \sim_{3,1} w-y\big),$$

which is clearly $\mathcal{L}_p$-definable. Finally, for each integer k, $D_k(x,y,z)$ can easily be seen to be an $\mathcal{L}_p$-definable relation by using the above $\mathcal{L}_p$-definable relations and some quantifiers. □

Proof of Proposition 2. Follows immediately from the cell decomposition result of [2] for subanalytic sets, or, alternatively, from the P-minimality result for the subanalytic structure on $\mathbb{Q}_p$ of [7] together with the cell decomposition result of [5]. □

Proof of Proposition 3. By Proposition 1 and Lemma 2.2. □

Proof of Proposition 4. Partition the graph of the definable function f in finitely many $\mathcal{L}'_p$-cells G of the form

$$\{(x,t) \in D \times \mathbb{Q}_p \mid \operatorname{ord} p^{k_1}(a_1 - c) \ \square_1\ \operatorname{ord}(t-c) \ \square_2\ \operatorname{ord} p^{k_2}(a_2 - c),\ t - c \in \lambda Q_{n,m}\},$$

where the symbols have the same meaning as in Definition 1.2. For each $x \in D$ there is a unique t such that $(x,t) \in G$, since G is a part of the graph of f. This uniqueness condition implies that $\lambda = 0$, and thus G has the form

$$G = \{(x,t) \in D \times \mathbb{Q}_p \mid t = c\}$$

and we are done, by the form of the center as given by Definition 1.2. □

3. Some examples

The following lemma exhibits the fact that $\mathcal{L}_p$ does not have definable skolem functions.

3.1. **Lemma.** *Consider the $\mathcal{L}_p$-definable set*

$$A = \{(x,y) \in (\mathbb{Q}_p^\times)^2 \mid \operatorname{ord} y = 1 + \operatorname{ord} x\}.$$

Then there exists no $\mathcal{L}_p$-definable function $g : \mathbb{Q}_p^\times \to \mathbb{Q}_p$ such that the graph of g lies in A.

Proof. Follows directly from Proposition 4. □

Another natural question is whether it is possible to give a simple classification of definable sets up to definable bijections. For semi-algebraic sets, it is shown in [1] that there exists a semi-algebraic bijection between two infinite semi-algebraic sets if and only if they have the same dimension, and in [2] this is extended to the subanalytic setting. Such a classification no longer holds for $\mathcal{L}_p$-definable sets, by the following.

3.2. **Lemma.** *Consider $\mathcal{L}_p$-definable sets given by*

$$A_i := \{x \in \mathbb{Q}_p \mid \operatorname{ord}(x) = k_i\}$$

for $i = 1, 2$ and some integers $k_1 \neq k_2$. Then there does not exist an $\mathcal{L}_p$-definable bijection between A_1 and A_2.

Proof. After a finite partition of A_1 in $\mathcal{L}'_p$-cells, the bijection restricted to any of the parts should be of the form $x \mapsto x$ or $x \mapsto a$, for $a \in \mathbb{Q}_p$, by Propositions 3 and 4. But it is clear that none of these maps can have an image which is an infinite subset of A_2. Hence, such a bijection cannot exist. $\square$

3.3. *Remark.* Note that any structure $\mathcal{L}$ on $\mathbb{Q}_p$ with $\mathcal{L}_p$-minimal theory comes with a dimension invariant for its definable sets. This dimension invariant has nice properties, for example, one has $\dim(f(X)) \leq \dim(X)$ for any $\mathcal{L}$-definable function $f : X \to Y$. Indeed, the structure $\mathcal{L}$ on $\mathbb{Q}_p$ is always a reduct of a P-minimal structure on $\mathbb{Q}_p$ which comes with such a dimension invariant, see [8].

3.4. *Remark.* To generalize our setting to a finite field extension K of $\mathbb{Q}_p$, one should replace the prime number p by a fixed uniformizer π of the valuation ring of K. Then all results and definitions go through correspondingly, referring to [6] instead of [5] for the semi-algebraic cell decomposition result.

4. A uniform, universal-existential definition of $\mathbb{Z}_p$ inside $\mathbb{Q}_p$

Let P_3 stand for the nonzero cubes in $\mathbb{Q}_p$. Write $\lambda \equiv \mu \bmod P_3$ if and only if $\lambda P_3 = \mu P_3$, where $\lambda P_3 = \{\lambda t \mid t \in P_3\}$. Let $P'(z)$ be the property about $z \in \mathbb{Q}_p$ saying that

$$(z-1) \equiv z \not\equiv 1 \bmod P_3.$$

4.1. **Lemma.** *A p-adic number x lies in $\mathbb{Z}_p$ if and only if*

$$\forall z \big(P'(z) \implies z - x \equiv z \bmod P_3\big). \tag{4.1.1}$$

Instead of proving this lemma, we will prove the more general Lemma 4.2 below.

By Lemma 4.1, we can define $\mathbb{Z}_p$ inside $\mathbb{Q}_p$ in the ring language $(+, -, \cdot, 0, 1)$ by

$$\forall z_1 \big(\exists z_2 \forall y_2 (z_2^3(z_1 - 1) = z_1 \neq y_2^3) \implies \exists y_1 (z_1 - x = y_1^3 z_1)\big)$$

which is equivalent to

$$\forall z_1 \forall z_2 \exists y_1 \exists y_2 \big(z_2^3(z_1 - 1) = z_1 \neq y_2^3 \implies z_1 - x = y_1^3 z_1\big).$$

In fact, we obtain the following

4.2. **Lemma.** *Let K be a nonarchimedean local field. If K has characteristic different from 3, then an element x of K lies in the valuation ring of K if and only if*

$$\forall z_1 \forall z_2 \exists y_1 \exists y_2 \big(z_2^3(z_1 - 1) = z_1 \neq y_2^3 \implies z_1 - x = y_1^3 z_1 \big). \tag{4.2.1}$$

If K has characteristic 3, then an element x of K lies in the valuation ring of K if and only if

$$\forall z_1 \forall z_2 \exists y_1 \exists y_2 \big(z_2^4(z_1 - 1) = z_1 \neq y_2^4 \implies z_1 - x = y_1^4 z_1 \big).$$

Proof. Suppose first that K has characteristic different from 3. Clearly Condition (4.2.1) is equivalent to condition (4.1.1), interpreted in K. We will reason on (4.1.1), interpreted in K. Take $x \in K$ with x not in the valuation ring of K. Write π for a uniformizer and write $\mathrm{ord}(\pi) = 1$. First suppose that $\mathrm{ord}(3) = 0$ or $\mathrm{ord}(x) < -\mathrm{ord}(3) - 1$. In the case that $\mathrm{ord}(x) \not\equiv 0 \bmod 3$ then take $z = x + 1$ to violate (4.1.1). In the case that $\mathrm{ord}(x) \equiv 0 \bmod 3$ then take $z = \pi x$ to violate (4.1.1). In the remaining case that $\mathrm{ord}(x) \geq -\mathrm{ord}(3) - 1$ and that $\mathrm{ord}(3) > 0$, one can take $z = 3^{-1}\pi^{-1}u$, with u a well-chosen unit, to violate (4.1.1). The proof for K having characteristic equal to 3 is similar, where one replaces the exponent 3 by 4. $\square$

Acknowledgement. We would like to thank Annand Pillay for mentioning the search for basic minimality notions on the p-adic numbers, and Jochen Koenigsmann for discussing uniform definitions of p-adic valuation rings inside p-adic fields with us.

References

[1] R. Cluckers. Classification of semi-algebraic p-adic sets up to semi-algebraic bijection. *J. reine angew. Math.*, 540:105–114, 2001.

[2] R. Cluckers. Analytic p-adic cell decomposition and integrals. *Transactions of the American Mathematical Society*, 356(4):1489–1499, 2003.

[3] R. Cluckers and L. Lipshitz. Fields with analytic structure. *to appear in J. Eur. Math. Soc. (JEMS).* math.LO/0610666.

[4] Raf Cluckers and Francois Loeser. b-minimality. *Journal of mathematical logic*, 7(2):195–227, 2007.

[5] J. Denef. The rationality of the poincaré series associated to the p-adic points on a variety. *Invent. Math.*, 77:1–23, 1984.

[6] J. Denef. p-adic semi-algebraic sets and cell decomposition. *J. reine angew. Math.*, 369:154–166, 1986.

[7] L. van den Dries, D. Haskell, and D. Macpherson. One-dimensional p-adic subanalytic sets. *Journal of the London Mathematical Society*, 59(1):1–20, 1999.

[8] D. Haskell and D. Macpherson. A version of o-minimality for the p-adics. *Journal of Symbolic Logic*, 62(4):1075–1092, 1997.

[9] J. Koenigsmann. Defining $\mathbb{Z}$ in $\mathbb{Q}$. *preprint*, 2010.

[10] Nianzheng Liu. Semilinear cell decomposition. *Journal of Symbolic Logic*, 59(1):199–208, March 1994.

[11] B. Poonen. Characterizing integers among rational numbers with a universal-existential formula. *Amer. J. Math.*, 131(3):675–682, 2009.

Université Lille 1, Laboratoire Painlevé, CNRS - UMR 8524, Cité Scientifique, 59655 Villeneuve d'Ascq Cedex, France, and, Katholieke Universiteit Leuven, Department of Mathematics, Celestijnenlaan 200B, B-3001 Leuven, Belgium,
E-mail address: Raf.Cluckers@math.univ-lille1.fr
URL: http://math.univ-lille1.fr/∼cluckers

Katholieke Universiteit Leuven, Department of Mathematics, Celestijnenlaan 200B, B-3001 Leuven, Belgium,
E-mail address: Eva.Leenknegt@wis.kuleuven.be
URL: http://perswww.kuleuven.be/∼u0050316/About_me.html