UNIFORMLY DEFINING VALUATION RINGS IN HENSELIAN VALUED FIELDS WITH FINITE OR PSEUDO-FINITE RESIDUE FIELDS

RAF CLUCKERS, JAMSHID DERAKHSHAN, EVA LEENKNEGT,
AND ANGUS MACINTYRE

ABSTRACT. We give a 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 for all p and all finite field extensions of these fields, and in many other Henselian valued fields as well. The formula can be taken existential-universal in the ring language, and in fact existential in a modification of the language of Macintyre. Furthermore, we show the negative result that in the language of rings there does not exist a uniform definition by an existential formula and neither by a universal formula for the valuation rings of all the finite extensions of a given Henselian valued field. We also show that there is no existential formula of the ring language defining $\mathbb{Z}_p$ inside $\mathbb{Q}_p$ uniformly for all p. For any fixed finite extension of $\mathbb{Q}_p$, we give an existential formula and a universal formula in the ring language which define the valuation ring.

1. INTRODUCTION

Uniform definitions of valuation rings inside families of Henselian valued fields have played important roles in the work related to Hilbert's 10th problem by B. Poonen [11] and by J. Koenigsmann [8], especially uniformly in p-adic fields. We address this issue in a wider setting, using the ring language and Macintyre's language. Since the work [9], the Macintyre language has always been prominent in the study of p-adic fields.

Let $\mathcal{L}_{\text{ring}}$ be the ring language $(+, -, \cdot, 0, 1)$. Write $\mathcal{L}_{\text{Mac}}$ for the language of Macintyre, which is obtained from $\mathcal{L}_{\text{ring}}$ by adding for each integer $n > 0$ a predicate P_n for the set of nonzero n-th powers. We assume that the reader is familiar with pseudo-finite fields and Henselian valued fields. For more information we refer to [5], [10], [4], and [3].

The following notational conventions are followed in this paper. For a Henselian valued field K we will write $\mathcal{O}_K$ for its valuation ring. $\mathcal{O}_K$ is assumed nontrivial. $\mathcal{M}_K$ is the maximal ideal of $\mathcal{O}_K$, and $k = \mathcal{O}_K/\mathcal{M}_K$ is the residue field. We denote by res the natural map $\mathcal{O}_K \to k$.

Given a ring R and a formula φ in $\mathcal{L}_{\text{ring}}$ or $\mathcal{L}_{\text{Mac}}$ in $m \geq 0$ free variables, we write $\varphi(R)$ for the subset of R^m consisting of the elements that satisfy φ. In this paper we will always work without parameters, that is, with $\emptyset$-definability.

2000 *Mathematics Subject Classification.* Primary 11D88, 11U09; Secondary 11U05.
Key words and phrases. Definability, Diophantine sets, Hilbert's Tenth Problem.

1. **Theorem.** *There is an existential formula $\varphi(x)$ in $\mathcal{L}_{\text{ring}} \cup \{P_2, P_3\}$ such that*

$$\mathcal{O}_K = \varphi(K)$$

holds for any Henselian valued field K with finite or pseudo-finite residue field k provided that k contains non-cubes in case its characteristic is 2.

We are very grateful to an anonymous referee for pointing out to us that our argument in an earlier version failed when k has characteristic 2 and every element is a cube (i.e. $(k^*)^3 = k^*$). There are such k, finite ones and pseudo-finite ones (cf. Section 5).

Note that in such a case k has no primitive cube root of unity, and so its unique quadratic extension is cyclotomic. That extension is the Artin-Schreier extension, and (as the referee suggested) it is appropriate to adjust the Macintyre language by replacing P_2 by P_2^{AS}, where

$$P_2^{AS}(x) \Leftrightarrow \exists y(x = y^2 + y).$$

This has notable advantages, namely:

2. **Theorem.** *There is an existential formula $\varphi(x)$ in $\mathcal{L}_{\text{ring}} \cup \{P_2^{AS}\}$ such that*

$$\mathcal{O}_K = \varphi(K)$$

holds for all Henselian valued fields K with finite or pseudo-finite residue field.

Since in a field of characteristic not equal to 2, we have $P_2^{AS}(x) \Leftrightarrow P_2(1 + 4x)$, Theorem 2 implies the following.

3. **Theorem.** *There is an existential formula $\varphi(x)$ in $\mathcal{L}_{\text{ring}} \cup \{P_2\}$ such that*

$$\mathcal{O}_K = \varphi(K)$$

holds for all Henselian valued fields K with finite or pseudo-finite residue field of characteristic not equal to 2.

Before proving the above theorems, we state some other results. First some negative results.

4. **Theorem.** *Let K be any Henselian valued field. There does not exist an existential formula $\psi(x)$ in $\mathcal{L}_{\text{ring}}$ such that*

$$\mathcal{O}_L = \psi(L)$$

for all finite extensions L of K. Neither does there exist a universal formula $\eta(x)$ in $\mathcal{L}_{\text{ring}}$ such that

$$\mathcal{O}_L = \eta(L)$$

for all finite extensions L of K.

The following was noticed by the referee.

5. **Theorem.** *There is no existential or universal $\mathcal{L}_{\text{ring}}$-formula $\varphi(x)$ such that $\mathbb{Z}_p = \varphi(\mathbb{Q}_p)$ for all the primes p. More generally, given any $N > 0$, there is no such formula $\varphi(x)$ such that $\mathbb{Z}_p = \varphi(\mathbb{Q}_p)$ for all $p \geq N$.*

For a fixed local field of characteristic zero, we can give existential and universal definitions.

6. **Theorem.** *Let K be a finite extension of $\mathbb{Q}_p$. Then the valuation ring $\mathcal{O}_K$ of K is definable by an existential formula in $\mathcal{L}_{\text{ring}}$ and also by a universal formula in $\mathcal{L}_{\text{ring}}$.*

2. Negative results

2.1. **Proof of Theorem 4.** Suppose that there was such an existential formula $\psi(x)$. Let K^{alg} denote the algebraic closure of K. By [5, Lemma 4.1.1 and Theorem 4.1.3], there is a unique valuation on K^{alg} extending the valuation on K. The valuation ring $\mathcal{O}_K$ has a unique prolongation to every algebraic extension of K. The valuation ring $\mathcal{O}_{K^{alg}}$ of K^{alg} is the union of the valuation rings of the finite extensions L, and is thus contained in $\psi(K^{alg})$. On the other hand, if $a \in \psi(K^{alg})$, then $a \in \psi(L)$ for some finite extension L of K. Thus a lies in the valuation ring of L, and hence $a \in \mathcal{O}_{K^{alg}}$. So $\psi(K^{alg})$ coincides with the valuation ring of K^{alg} which implies that it must be finite or cofinite, contradiction.

We will now show that there is no existential formula $\theta(x)$ in the language of rings such that for all finite extensions L of K

$$\theta(L) = \mathcal{M}_L.$$

Suppose that there was such a formula $\theta(x)$. Then since the maximal ideal of $\mathcal{O}_{K^{alg}}$ is the union of the maximal ideals $\mathcal{M}_L$ over all finite extensions L of K, we see that if $a \in \mathcal{M}_{K^{alg}}$, then $a \in \mathcal{M}_L$ for some finite extension L of K, hence $\theta(a)$ holds in L, so $\theta(a)$ holds in K^{alg}. Conversely, if $K^{alg} \models \theta(a)$, where $a \in K^{alg}$, then $L \models \theta(a)$ for some finite extension L of K, hence $a \in \mathcal{M}_L$, thus $a \in \mathcal{M}_{K^{alg}}$. Therefore $\theta(K^{alg})$ coincides with the maximal ideal of the valuation ring of K^{alg} which implies that it must be finite or cofinite, contradiction.

If $\theta(x)$ is a formula defining $\mathcal{M}_L$, then the formula

$$\sigma(x) := \exists z(xz = 1 \wedge \theta(z))$$

defines the set $L \setminus \mathcal{O}_L$. We deduce that there does not exist an existential formula $\sigma(x)$ in the language of rings such that for all finite extensions L of K

$$\sigma(L) = L \setminus \mathcal{O}_L.$$

Thus there does not exist a universal formula $\eta(x)$ of the language of rings such that for all finite extensions L of K

$$\eta(L) = \mathcal{O}_L.$$

The proof of Theorem 4 is complete.

2.2. **Proof of Theorem 5.** Suppose there is such a formula $\varphi(x)$. By a result of Ax [2, Proposition 7, pp.260], there is an ultrafilter $\mathcal{U}$ on the set $\mathbf{P}$ of all primes such that the ultraproduct $k = (\prod_{p \in \mathbf{P}} \mathbb{F}_p)/\mathcal{U}$ satisfies

$$k \cap \mathbb{Q}^{alg} = \mathbb{Q}^{alg}.$$

The field $K = (\prod_{p\in\mathbf{P}} \mathbb{Q}_p)/\mathcal{U}$ is Henselian with residue field k, which is pseudo-finite of characteristic zero, and value group an ultrapower of $\mathbb{Z}$.

If L is a finite extension of K, the residue field k' of L is a finite extension of k, hence is pseudo-finite and has the same algebraic numbers as k. Since two pseudo-finite fields with isomorphic subfields of algebraic numbers are elementarily equivalent ([2, Theorem 4, pp.255]), $k' \equiv k$. Thus all residue fields of finite extensions of K are elementarily equivalent to k and all value groups are elementarily equivalent to $\mathbb{Z}$. So, by the theorem of Ax-Kochen [1, Theorem 3, pp.440], $L \equiv K$ for all finite extensions L of K, and so $\mathcal{O}_L = \varphi(L)$ uniformly, contradicting Theorem 4.

3. Proof of Theorem 6

Suppose K has degree n over $\mathbb{Q}_p$. We have $n = ef$, where f and e are respectively the residue field dimension and ramification index of K over $\mathbb{Q}_p$ (cf. [6]). Let L be the maximal unramified extension of $\mathbb{Q}_p$ inside K. L has residue field $\mathbb{F}_{p^f}$ and value group $\mathbb{Z}$ for the valuation extending the p-adic valuation v_p of $\mathbb{Q}_p$. K has value group $(1/e)\mathbb{Z}$ for the valuation v extending v_p.

Select (non-uniquely) a monic irreducible polynomial $G_0(x)$ over $\mathbb{F}_p$ of degree f such that $\mathbb{F}_{p^f}$ is the splitting field of $G_0(x)$. Consider a monic polynomial $G(x)$ over $\mathbb{Z}$ which reduces to $G_0(x)$ mod p. The polynomial $G_0(x)$ has a simple root in $\mathbb{F}_{p^f}$, so by Hensel's Lemma, $G(x)$ has a root γ in L.

1. **Claim.** $L = \mathbb{Q}_p(\gamma)$.

Proof of the claim. Clearly $\mathbb{Q}_p(\gamma) \subset L$. But the residue field of $\mathbb{Q}_p(\gamma)$ contains $\mathbb{F}_{p^f}$. So the dimension of $\mathbb{Q}_p(\gamma)$ over $\mathbb{Q}_p$ is at least f. So $L = \mathbb{Q}_p(\gamma)$. □

Note that $G(x)$ is irreducible over $\mathbb{Z}_p$ and so over $\mathbb{Q}_p$, and $G(x)$ splits in L. Thus all the roots of $G(x)$ are conjugate over $\mathbb{Q}_p$ by automorphisms of L. We can choose an Eisenstein polynomial over L of the form

$$x^e + H_{e-1}(\gamma)x^{e-1} + \cdots + H_0(\gamma) \in L[x],$$

where for $i \in \{0, \ldots, e-1\}$, $H_j(z)$ is a polynomial in the variable z over $\mathbb{Q}_p$. We aim to get an Eisenstein polynomial whose coefficients are in $\mathbb{Q}(\gamma)$. For any polynomials $H_0^*(z), \ldots, H_{e-1}^*(z)$ over $\mathbb{Q}$, we let

$$H_z^*(x) := x^e + H_{e-1}^*(z)x^{e-1} + \cdots + H_0^*(z) \in \mathbb{Q}(z)[x].$$

If $H_j^*(z)$ is such that $|H_j(z) - H_j^*(z)|$ is very small, then since $v(\gamma) \in \mathbb{Z}$, it follows that $|H_j(\gamma) - H_j^*(\gamma)|$ is also very small. Thus we can choose $H_j^*(z)$ over $\mathbb{Q}$ sufficiently close to $H_j(z)$ so that $H_\gamma^*(x) \in \mathbb{Q}(\gamma)[x]$ is Eisenstein. So $H_\gamma^*(x)$ is irreducible over L, and, by Krasner's Lemma, it has a root in K which generates K over L. For any other root γ' of $G(x)$, there is a $\mathbb{Q}_p$-automorphism σ of L such that $\sigma(\gamma) = \gamma'$, and thus $\sigma(H_j^*(\gamma)) = H_j^*(\gamma')$. Since L is unramified over $\mathbb{Q}_p$ and p is a uniformizer in L, the valuation ring of L is definable without parameters and σ preserves the valuation. Thus $H_{\gamma'}^*(x)$ is also an Eisenstein polynomial. By [6, Theorem 1, p.23], any root of an Eisenstein polynomial is a uniformizer. We have thus shown that for any root η

of $G(x)$, any root of $H^*_\eta(x)$ is a uniformizer. Indeed, $\{t : \exists\eta\ G(\eta) = 0 \wedge H^*_\eta(t) = 0\}$ is an existentially definable nonempty set of uniformizers. So using Hensel's Lemma, we can define $\mathcal{O}_K$ by

$$\exists z \exists y \exists w\ (G(z) = 0 \wedge H^*_z(y) = 0 \wedge 1 + yx^2 = w^2)$$

if $p \neq 2$, and

$$\exists z \exists y \exists w\ (G(z) = 0 \wedge H^*_z(y) = 0 \wedge 1 + yx^3 = w^3)$$

if $p \neq 3$.

This completes the proof of existential definability of $\mathcal{O}_K$. Note that combined with the remark about existential definition of a nonempty set of uniformizers, it gives existential definition of the set of uniformizers, and so of the maximal ideal $\mathcal{M}_K$ as the set of elements of K which are a product of a uniformizer and an element of $\mathcal{O}_K$. Thus the complement of $\mathcal{O}_K$ is existentially definable as the set of inverses of elements of $\mathcal{M}_K$. Hence $\mathcal{O}_K$ is universally definable.

4. Proof of Theorems 1 and 2

For any prime number p, let $T_p(x)$ be the condition about 1 free variable x expressing that

$$p^p + x \in P_p \wedge x \notin P_p.$$

Let $T(x)$ be the property about $x \in K$ saying that

$$T_2(x) \vee T_3(x).$$

Let $T^+(x)$ be the statement

$$x \neq 0 \wedge \neg P_2^{AS}(x) \wedge \neg P_2^{AS}(x^{-1}).$$

Recall that $\wedge$ stands for conjunction and $\vee$ for disjunction in first order languages.

1. **Lemma.** *Let k be a pseudo-finite field. If the characteristic of k is different from 2, then $T_2(k)$ is infinite. If the characteristic of k is 2 and k contains a non-cube, then $T_3(k)$ is infinite.*

Proof. Suppose the characteristic of k is different from 2. k is elementarily equivalent to an ultraproduct of finite fields $\mathbb{F}_q$ where q is a power of an odd prime. Thus $(q-1, 2) \neq 1$, hence $\mathbb{F}_q^\times$ contains a non-square (cf. Section 5, Proposition 5). Thus $k^\times$ contains a non-square a. Then $T_2(x)$ is equivalent with

$$\exists w, v (w^2 = 4 + x \wedge av^2 = x).$$

Now consider the curve C given by $w^2 = 4+x,\ av^2 = x$ in $\mathbf{A}^3$. Since this is an absolutely irreducible curve defined over k, it follows by the pseudo-algebraic closedness of k that $C(k)$ is infinite. Thus, $T_2(k)$ is infinite. The proof for characteristic 2 is similar. $\square$

2. **Lemma.** *$T^+(k)$ is infinite for every pseudo-finite field k.*

Proof. Given a pseudo-finite field k choose $a \in k \setminus P_2^{AS}(k)$ if k has characteristic 2 and $a \in k \setminus k^2$ if k has characteristic different from 2, and define the curve $\mathcal{C}_a$ by

$$w^2 + w = a - x$$
$$v^2 + v = a - x^{-1}$$

if k has characteristic 2; and

$$1 + 4x = aw^2$$
$$1 + 4x^{-1} = av^2$$

if k has characteristic different from 2. Then $\mathcal{C}_a$ is an absolutely irreducible curve in $\mathbf{A}^3$. Since k is pseudo-algebraically closed, $\mathcal{C}_a(k)$ is infinite. Note that

$$T^+(x) \Leftrightarrow \exists v \exists w\ (v, w, x) \in \mathcal{C}_a(k),$$

which completes the proof. □

3. **Lemma.** *Let K be any Henselian valued field with residue field k. Then, $T(K)$ is a subset of the valuation ring $\mathcal{O}_K$ and $T^+(K)$ is a subset of the units $\mathcal{O}_K^\times$. Moreover, $T(K)$ contains both the sets*

$$res^{-1}(T_2(k) \setminus \{0\}) \quad \text{and} \quad res^{-1}(T_3(k) \setminus \{0\}),$$

and $T^+(K)$ contains $res^{-1}(T^+(k))$.

Proof. We first show that $T_2(K) \subset \mathcal{O}_K$ for all Henselian valued fields K. It suffices to show for $x \in K \setminus \mathcal{O}_K$ that x is a square if and only if $x + 4$ is a square. Let $x \in K \setminus \mathcal{O}_K$. We show the left to right direction, the converse is similar. So assume x is a square. It suffices to show that $1 + 4/x$ is a square, for then $x + 4$ will be a product of two squares $1 + 4/x$ and x, hence a square.

Let $f(y) := y^2 - 1 - 4/x$. Since $|f'(1)| = |2|$ and $|x| > 1$, we have

$$|f(1)| = |4/x| < |4| = |2|^2 = |f'(1)|^2.$$

Thus by Hensel's Lemma, $f(y)$ has a root in $\mathcal{O}_K$. This shows that $T_2(K) \subset \mathcal{O}_K$. One proceeds similarly to show that $T_3(K) \subset \mathcal{O}_K$. It follows that $T(K) \subset \mathcal{O}_K$ for all Henselian valued fields K.

Now let $x \in T_2(k) \setminus \{0\}$. This implies that the characteristic of k is not 2. Thus if $\hat{x} \in \mathcal{O}_K$ is any lift of x, by Hensel's Lemma, $\hat{x} \in T_2(K)$, so $res^{-1}(T_2(k)) \subset T_2(K)$. Similarly $x \in T_3(k) \setminus \{0\}$ implies that the characteristic of k is not 3, and $res^{-1}(T_3(k)) \subset T_3(K)$. The other assertions concerning $T^+(K)$ and $T^+(k)$ are immediate. □

We will use the following theorem of Chatzidakis - van den Dries - Macintyre [4]. This result can be thought of as a definable version of the classical Cauchy - Davenport theorem.

7. **Theorem.** [4, Proposition 2.12] *Let K be a pseudo-finite field and S an infinite definable subset of K. Then every element of K can be written as $a + b + cd$, with $a, b, c, d \in S$.*

8. **Corollary.** *Let $\varphi(x)$ be an $\mathcal{L}_{\text{ring}}$-formula. Then there exists $N = N(\varphi)$ such that*
$$K = \{a + b + cd : a, b, c, d \in \varphi(K)\}.$$
for every finite field K of cardinality at least N.

Proof. Follows from Theorem 7 and a compactness argument. □

9. **Theorem.** *Let $\varphi(x)$ be an $\mathcal{L}_{\text{ring}}$-formula such that $\varphi(k)$ is infinite for every pseudo-finite field k and $\varphi(K) \subset \mathcal{O}_K$ and $res^{-1}(\varphi(k)) \subset \varphi(K)$ for every Henselian valued field K with pseudo-finite residue field k. Then there exists $N \geq 1$ such that*
$$\mathcal{O}_K = \{a + b + cd : \ a, b, c, d \in \varphi(K)\}$$
for every Henselian valued field K with finite or pseudo-finite residue field of cardinality at least N.

Proof. Let $\theta \in \mathcal{O}_K$. Then $res(\theta) = a + b + cd$ for $a, b, c, d \in \varphi(k)$. Let $\hat{b}, \hat{c}, \hat{d}$ denote lifts of b, c, d respectively. Then
$$res(\theta - (\hat{b} + \hat{c}\hat{d})) = a.$$
Thus $\theta - (\hat{b} + \hat{c}\hat{d}) \in \varphi(K)$, and we are done. □

10. **Corollary.** *There exists $N > 0$ such that*
$$\mathcal{O}_K = \{a + b + cd : \ a, b, c, d \in T(K)\}$$
for any Henselian valued field K with finite or pseudo-finite residue field k with cardinality at least N provided that k contains non-cubes in case its characteristic is 2.

Proof. Immediate. □

11. **Corollary.** *There exists $N > 0$ such that*
$$\mathcal{O}_K = \{a + b + cd : \ a, b, c, d \in T^{+}(K)\}$$
for any Henselian valued field K with finite or pseudo-finite residue field k with cardinality at least N.

Proof. Immediate. □

For any integer $\ell > 0$, K any field, and $X \subset K$ any set, let $S_\ell(X)$ be the set consisting of all $y \in K$ such that $y^\ell - 1 + x \in X$ for some $x \in X$.

4. **Proposition.** *Let K be a Henselian valued field with finite residue field k with q_K elements. Let ℓ be any positive integer multiple of $q_K(q_K - 1)$. Then one has*
$$\mathcal{O}_K = \{0, 1\} + S_\ell(T^{+}(K)),$$
where the sumset of two subsets A, B of K consists of the elements $a + b$ with $a \in A$ and $b \in B$. If k has a non-cube in case it has characteristic different from 3*, then one has*
$$\mathcal{O}_K = \{0, 1\} + S_\ell(T(K)).$$

Proof. Since $\mathcal{O}_K$ is integrally closed in K, for any $l > 0$ and any Henselian valued field K, one has by Lemma 3 that

$$S_l(T(K)) \subset \mathcal{O}_K$$

and

$$S_l(T^+(K)) \subset \mathcal{O}_K.$$

2. **Claim.** *For any unit $y \in \mathcal{O}_K$ there is a positive γ in the value group such that* $\mathrm{ord}(y^l - 1) > \gamma$.

Proof. There are two cases. Either the value group has a least positive element or it has arbitrarily small positive elements. Suppose the first case holds. Let π denote an element of least positive valuation.

We assume K has residue field $\mathbb{F}_q$, with $q = p^f$. Fix a unit y. Let a be a (not necessarily primitive) $(q-1)$-th root of unity such that

$$|y - a| < 1.$$

Note that a exists by Hensel's Lemma since y is a root of the polynomial $x^{q-1} - 1$ modulo the maximal ideal and is clearly non-singular.

Write y as $a + b\pi$, where $b \in \mathcal{O}_K$. Then

$$y^l = 1 + la^{l-1}b\pi + \cdots + b^l\pi^l.$$

Note that the Binomial coefficients are divisible by l, and hence by q and thus by π (as $\pi^e = p$ where e is ramification index), and $l \geq 2$; therefore

$$v(y^l - 1) \geq 2.$$

This proves the Claim in the first case. In the second case, there are arbitrarily small positive elements in the value group and $y^l - 1$ has some strictly positive valuation, hence γ exists in this case. □

3. **Claim.** *Given γ a positive element of the value group, there is $a \in T(K)$ and $b \in T^+(K)$ such that* $\mathrm{ord}(a) \leq \gamma$, $\mathrm{ord}(b) \leq \gamma$, *and*

$$a + a\mathcal{M}_K \subset T(K)$$

$$b + b\mathcal{M}_K \subset T^+(K).$$

Proof. Again, first assume that the value group has a least positive element π. Clearly π is a non-square and a non-cube, and by Hensel's Lemma $4 + \pi$ is a square if the residue characteristic is not equal to 2, and $27 + \pi$ is a cube if the residue characteristic is not equal to 3. So we can take $a = \pi$, and by Hensel's Lemma we have $a + a\mathcal{M}_K \subset T(K)$.

In the case that there are elements of arbitrarily small positive value, there exist non-squares and non-cubes of arbitrarily small positive value. Indeed, fix a non-square x. We can choose b such that its valuation is very close to half the valuation of $1/x$. Then b^2x has valuation very close to zero. A similar argument works for the non-cubes. Then Hensel's Lemma as above completes the proof in this case.

As for $T^+(K)$, given $\gamma > 0$, choose any $b \in T^+(K)$. We have that b is a unit and hence $\mathrm{ord}(b) = 0 < \gamma$. It follows from Hensel's Lemma that $b + b\mathcal{M}_K \subset T^+(K)$ since if $b + bm = y^2 + y$ for some y, where $m \in \mathcal{M}$, then $b - y^2 - y$ has a non-singular root modulo the maximal ideal $\mathcal{M}$; this contradicts $b \in T^+(K)$. This argument works for any value group. □

To complete the proof of the proposition take a unit $\alpha \in \mathcal{O}_K$. By Claim 2 there is $\gamma > 0$ with $\mathrm{ord}(\alpha^l - 1) > \gamma$. Choose elements $a \in T(K)$, and $b \in T^+(K)$ such that $\mathrm{ord}(a) \leq \gamma$ and $\mathrm{ord}(b) \leq \gamma$. Thus

$$(\alpha^l - 1)/a \in \mathcal{M}_K$$

and

$$(\alpha^l - 1)/b \in \mathcal{M}_K,$$

hence

$$\alpha^l - 1 + a \in a + a\mathcal{M}_K$$

and

$$\alpha^l - 1 + b \in b + b\mathcal{M}_K.$$

So by Claim 3, $\alpha \in S_l(T(K))$ and $\alpha \in S_l(T^+(K))$. This completes the proof. □

We can now give the proof of Theorems 1 and 2. By Lemma 3, for any $\ell > 0$ and any Henselian valued field K one has

$$S_\ell(T(K)) \subset \mathcal{O}_K.$$

and

$$S_\ell(T^+(K)) \subset \mathcal{O}_K.$$

From Proposition 4 and Corollaries 10 and 11 we deduce that there exists $\ell > 0$ such that for any Henselian valued field K we have

$$\mathcal{O}_K = (\{0,1\} + S_\ell(T(K))) \cup \{a + b + cd : \ a, b, c, d \in T(K)\} \tag{4.0.1}$$

provided that the residue field k contains a non-cube in case the characteristic of k is 2. From Proposition 4 and Corollaries 10 and 11 we also deduce that

$$\mathcal{O}_K = (\{0,1\} + S_\ell(T^+(K))) \cup \{a + b + cd : \ a, b, c, d \in T^+(K)\} \tag{4.0.2}$$

for any Henselian valued field K. Now Theorems 1 and Theorem 2 follow since the unions in 4.0.1 and 4.0.2 corresponds to existential formulas in $\mathcal{L}_{\text{ring}} \cup \{P_2, P_3\}$ and $\mathcal{L}_{\text{ring}} \cup \{P_2^{AS}\}$ respectively as desired.

5. Appendix: Powers in pseudo-finite fields

5. **Proposition.** *Let p be a prime, q a power of p, and $m \in \mathbb{N}$. The following are equivalent.*

- $\mathbb{F}_q^* = (\mathbb{F}_q^*)^m$.
- $(q - 1, m) = 1$.
- $\mathbb{F}_h^* = (\mathbb{F}_h^*)^m$ *for infinitely many powers h of p.*

Proof. To show the first and second statements are equivalent, let $K = \mathbb{F}_q$. The multiplicative group K^* is cyclic of order $q-1$. If $(m, q-1) = 1$ then the map $x \to x^m$ is an automorphism of K^*. Conversely, if the map $x \to x^m$ from K^* to K^* is surjective, then it is injective. Choose d with $d|m$ and $d|(q-1)$. There is y such that $y^d = 1$, so $y^m = (y^d)^{m/d} = 1$, thus $y^m = 1$, contradiction.

To prove the equivalence of the second and third statements, let h be the order of p in $(\mathbb{Z}/m\mathbb{Z})^*$. Assume that $(p^s - 1, m) = 1$, for some s. For any $a \in \mathbb{N}$, we have

$$p^{ah+s} \equiv \; p^s \pmod{m},$$

hence

$$p^{ah+s} - 1 \equiv \; p^s - 1 \pmod{m}.$$

Therefore $(p^{ah+s} - 1, m) = 1$. Conversely, the last congruence shows that $(p^{ah+s} - 1, m) = 1$ implies $(p^s - 1, m) = 1$. The proof is complete. $\square$

Corollary. *There are pseudo-finite fields of characteristic* 2 *which do not contain non-cubes, and pseudo-finite fields of characteristic* 3 *which do not contain non-squares. There are pseudo-finite fields* K *of characteristic zero such that* $K^* = (K^*)^n$ *for all odd* n.

Proof. The first two statements are immediate by Proposition 5. For the last statement use compactness to reduce to the case of finitely many n, therefore to one n by taking product, and then use Proposition 5. $\square$

Note that the restriction to odd n in the Corollary is necessary since for any finite field k of odd characteristic, $k^*/(k^*)^2$ has cardinality 2.

Acknowledgement. The idea for this paper originated through discussions with J. Koenigsmann, J Demeyer, and C. Degroote, to whom we are very grateful. We are also indebted to E. Hrushovski and Z. Chatzidakis for invaluable help on the results of [7]. We also thank I. Halupczok and D. R. Heath-Brown for interesting discussions, and the referee for very valuable ideas.

References

1. J. Ax and S. Kochen, *Diophantine problems over local fields:III. decidable fields*, Ann. of Math. (2) **83** (1966), 437–456.
2. James Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR 0229613 (37 #5187)
3. Z. Chatzidakis, *Notes on the model theory of finite and pseudo-finite fields*, http://www.logique.jussieu.fr/~zoe/index.html, Notes d'un mini-cours donné à lŠUniversité Autonome de Madrid en novembre 2005.
4. Z. Chatzidakis, L. van den Dries, and A. Macintyre, *Definable sets over finite fields*, J. Reine Angew. Math. **427** (1992), 107–135.
5. A.J. Engler and A. Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer-Verlag, 2005.
6. A. Fröhlich, *Local fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 1–41. MR 0236145 (38 #4443)
7. Ehud Hrushovski, *Pseudo-finite fields and related structures*, Model theory and applications, Quad. Mat., vol. 11, Aracne, Rome, 2002, pp. 151–212.

8. J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, to appear in Annals of Mathematics, arXiv:1011.3424.
9. A. Macintyre, *On definable subsets of p-adic fields*, Journal of Symbolic Logic **41** (1976), 605–610.
10. D. Marker, *Model theory: an introduction*, Graduate Texts in Mathematics, vol. 217, Springer-Verlag, 2002.
11. Bjorn Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682. MR 2530851 (2010h:11203)

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

University of Oxford, Mathematical Institute, 24-29 St Giles', Oxford OX1 3LB, UK
E-mail address: derakhsh@maths.ox.ac.uk

Purdue University, Department of Mathematics, 150 N. University Street, West Lafayette, IN 47907-2067, US
E-mail address: eleenkne@math.purdue.edu

Queen Mary, University of London, School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK
E-mail address: angus@eecs.qmul.ac.uk