数理解析研究所講究録
第 1888 巻 2014 年 17-22

Uncountable p-adically closed fields with arithmetic parts satisfying PA

Makoto Yanagawa
Graduate School of Pure and Applied Sciences
Tsukuba University

Abstract

We introduce the notion of arithmetic part. For a p-valued field (K, v), an arithmetic part N of K is a dense subsemiring of the valuation ring and the 2-ary relation $v(x) \leq v(y)$ on N is definable in N. We show that there is an $\aleph_1$-saturated p-adically closed field which has no arithmetic part satisfying PA.

1 Introduction

First of all, we recall some results in [1], where they gave a necessary and sufficient condition for the recursive saturation of real closed fields. A real closed field is a model of the theory of the field $\mathbb{R}$ of reals in the language $L_{or} = \{+, \times, 0, 1, <\}$ of ordered rings. For an ordered field R, an integer part is a subset of R such as the relationship between $\mathbb{Z}$ and $\mathbb{R}$. Suppose R is an ordered field and I is a unitary subring of R. We say that I is an *integer part* if there is no element between 0 and 1, and for each $x \in R$, there is some $i \in I$ such that $i \leq x < i + 1$. Mourges and Ressayre [2] proved that every real closed field has an integer part. D'Aquino, Knight, and Starchenko showed the following theorem.

Theorem 1.1 (D'Aquino, Knight, and Starchenko [1]). *Suppose R is a real closed field. If there is an integer part I of R which is a nonstandard model of PA, then R is recursively saturated. In addition if R is countable then the converse holds.*

In this theorem, the countable condition is necessarily. In fact, Marker and Steinhorn showed the following theorem.

Theorem 1.2 (Marker and Steinhorn [9]). *There is an $\aleph_1$-saturated real closed field which has no integer part satisfying PA.*

We consider a p-adic analogy of [1] and [9]. The author showed the following p-adic analogy of Theorem 1.1 (see, Theorem 2.3). In this paper, we show the p-adic analogy of Theorem 1.2, that is, there is an $\aleph_1$-saturated p-adically closed field which has no arithmetic part satisfying PA.

In the section 2, we recall definitions and facts necessary for understanding the statement of the main result (Theorem 2.3). In the section 3, we recall the definition of the ordinal Hahn fields, and in section 4, we mention a p-adic analogy of Hahn fields introduced by Poonen. In section 5, we prove the main theorem.

2 Preliminaries

An ordered group G is called a *$\mathbb{Z}$-group* if it is elementary equivalent to $\mathbb{Z}$ in the language $\{+, 0, 1, <\}$. There is a well-known fact.

Fact 2.1. *A unitary ordered group G is a $\mathbb{Z}$-group if and only if the unit is the least positive element and $G/\mathbb{Z}$ is divisible.*

This fact is proved using the method of quantifier elimination, for more detail see [7].

Suppose K is a field, G is an ordered abelian group and $v : K^\times \to G$ a surjective group homomorphism. We say that (K, v, G) is a *valued field* if all triples $x, y, x+y \in K^\times$ satisfy the strong triangle inequality

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

If G and v are obvious, we say simply that (K, v) or K is a valued field. For a valued field (K, v), we say that G is the *valued group* of K denoted by vK. The set $\{x \in K^\times : v(x) \geq 0\} \cup \{0\}$ of all positive value elements of K with 0 forms a subring of K. The subring is called the *valuation ring*, denoted by $\mathcal{O}_K$. The valuation ring of K is a local ring whose unique maximal ideal $\mathcal{M}_K = \{x \in K^\times : v(x) > 0\} \cup \{0\}$. The *residue field* of K is the residue field $\mathcal{O}_K/\mathcal{M}_K$ of $\mathcal{O}_K$, denoted by Kv. The *characteristic* of the valued field (K, v) is the pair $(\mathrm{ch}(K), \mathrm{ch}(Kv))$. The possibility of characteristic of valued fields is $(0,0)$, $(0,p)$, or (p,p). The case of $(0,0)$ or (p,p) is called *equi-characteristic* case, and otherwise *mixed characteristic*.

A valued field (K, v) is *p-valued* if characteristic of K is 0, $v(p)$ is the least positive element in the value group vK, and the residue field Kv is the finite field $\mathbb{F}_p$ of p elements. A p-valued field (K, v) is called *p-adically closed* if there is no proper algebraic p-valued extension. The language L_V of valued fields is the language $L_r = \{+, \times, 0, 1\}$ of rings with one unary predicate symbol V. For a valued field (K, v), we regard K as an L_V-structure as follows: for $a \in K$,

$$K \models V(a) \iff a \in \mathcal{O}_K.$$

Ax, Kochen, and Ershov have characterized p-adically closed fields from model theoretic point of view.

Fact 2.2 (AKE-principle, the proof see [4]). *For a valued field (K, v), the following are equivalent;*

1. *K is p-adically closed.*
2. *K is elementary equivalent to $\mathbb{Q}_p$ as L_V-structure.*
3. *the valuation ring $\mathcal{O}_K$ is henselian, the residue field Kv is $\mathbb{F}_p$, and the value group vK is elementary equivalent to $\mathbb{Z}$ as $\{+, 0, 1, <\}$-structure, that is vK is a $\mathbb{Z}$-group.*

We denote pCF the theory $\mathrm{Th}_{L_V}(\mathbb{Q}_p)$ of $\mathbb{Q}_p$ in the language L_V.

For a p-valued field K, we will define an arithmetic part of K which is an analogy of integer part. Our arithmetic part is something like in $\mathbb{Q}_p$, while the arithmetic part corresponds to $\mathbb{N}$ in the given field. Suppose (K, v) is a p-valued field and N is a subsemiring of K. We say that N is an *arithmetic part* if it is dense with respect to valuation topology in the valuation ring of K and the 2-ary relation $v(x) \leq v(y)$ on N is definable in N. There is the following theorem.

Theorem 2.3 ([10]). *Suppose K is a p-adically closed field. If there is an arithmetic part N of K which is a nonstandard model of PA, then K is recursively saturated. In addition if K is countable then the converse holds.*

The rest of this paper, we consider necessity of the countability condition in the theorem 2.3. In fact, we show the following theorem.

Theorem 2.4. *There is an $\aleph_1$-saturated p-adically closed field which has no arithmetic part satisfying PA.*

3 Mal'cev-Neuman rings and Hahn fields

Suppose k is a unitary ring and G is an ordered abelian group. The Mal'cev-Neumann ring $k((t^G))$ is the ring with the underlying set $\{\alpha : G \to k : \mathrm{supp}(\alpha) \text{ is well ordered}\}$, where

$\operatorname{supp}(\alpha) = \{g \in G : \alpha_g := \alpha(g) \neq 0\}$. We denote $f \in k((t^G))$ by a formal sum $\sum_{g\in G} \alpha_g t^g$ in an indeterminate t. If $\alpha = \sum_g \alpha_g t^g, \beta = \sum_g \beta_g t^g$ are elements of $k((t^G))$, then $\alpha + \beta$ is defined as $\sum_g (\alpha_g + \beta_g) t^g$, and $\alpha\beta = \sum_g (\sum_{i+j} \alpha_i \beta_j) t^g$. It is easy to see that $\alpha+\beta$ and $\alpha\beta$ are well-defined. Thus, they make $k((t^G))$ a ring.

Define $v : k((G))^\times \to G$ by $v(\alpha) = \min \operatorname{supp}(\alpha)$ for $\alpha \neq 0$. There is the fact that if k is a field then $(k((t^G)), v)$ is a valued field (see, [8]), so in the case we call $k((t^G))$ a Hahn field. Suppose $K = k((t^G))$ is a Hahn field, then the value group vK is G and the residue field Kv is k, so $\operatorname{ch}(K) = \operatorname{ch}(Kv)$. Thus, any Hahn fields have equi-characteristic. It is natural to ask whether we can construct a mixed characteristic valued field for given an ordered group G and a field k. We will answer to this question in the next section.

4 p-adic Hahn fields

The p-adic Hahn field are introduced by B.Poonen in [8]. To construct an analogy of mixed characteristic, it requires a more complicated construction. We recall a result about complete discrete valuation rings.

Fact 4.1. *If k is a perfect field of characteristic $p > 0$, then there exists a unique field $W(k)$ of characteristic 0 with a discrete valuation v' such that the residue field is k, $v(p) = 1 \in \mathbb{Z}$, and $W(k)$ is complete with respect to v'.*

For example, if $k = \mathbb{F}_p$, then $W(k) = \mathbb{Q}_p$ with the p-adic valuation. In fact, $W(k)$ is well known as the set of Witt vectors over k.

To construct p-adic analogy of Hahn field, at first, we consider the Mal'cev-Neuman ring $\mathcal{O}_{W(k)}((t^G))$. We want to replace t to p in $\mathcal{O}_{W(k)}((t^G))$, that is we want to consider something like the structure $\mathcal{O}_{W(k)}((t^G))/(t-p)$. Poonen defined the following set N which elements should be 0 in $\mathcal{O}_{W(k)}((t^G))$ throughout replacing t to p;

$$N = \{\alpha \in \mathcal{O}_{W(k)}((t^G)) : \forall g \in G; \sum_{n=-\infty}^{\infty} \alpha_{g+n} p^n = 0 \text{ in } W(k)\}.$$

And he show the following proposition.

Proposition 4.2 (Poonen, [8]). *1. N is a maximal ideal of $\mathcal{O}_{W(k)}((t^G))$.*

2. $\mathcal{O}_{W(k)}((t^G))/N$ is a valued field whose the value group is G and the residue field is k.

3. $\mathcal{O}_{W(k)}((t^G))/N$ is of the form

$$\left\{\alpha = \sum_{g\in G} \alpha_g p^g : \alpha_g \in k, \operatorname{supp}(\alpha) \textit{ is well-ordered}\right\}.$$

We write $k((p^G))$ for $\mathcal{O}_{W(k)}((t^G))/N$, and call $k((p^G))$ a p-adic Hahn field. For example, $\mathbb{F}_p((p^{\mathbb{Z}})) = \mathbb{Q}_p$. Moreover, he showed the maximal completeness of p-adic Hahn fields.

Proposition 4.3 (Poonen, [8]). *The p-adic Hahn fields are maximally complete. In particular, they are henselian valued fields.*

5 Proof of Theorem 2.3

The proof of Theorem 2.3 is divided three parts.

Proposition 5.1. *Let G be a $\mathbb{Z}$-group. Then the p-adic Hahn field $\mathbb{F}_p((p^G))$ is a p-adically closed field.*

Proof. It is clear, by Proposition 4.3 and AKE-principle (Fact 2.2). □

Proposition 5.2. *There is $\aleph_1$-saturated $\mathbb{Z}$-group such that there is no expansion to a model of PA.*

Proof. The following proof is the analogy of $\aleph_0$-saturated case in [7].

Let Z be an $\aleph_1$-saturated $\mathbb{Z}$-group of cardinality $> 2^{\aleph_0}$ and let Q be an $\aleph_1$-saturated model of $\mathrm{Th}(\mathbb{Q}, +, <)$ of cardinality $2^{\aleph_0}$. Let $G = Q \times Z$ with addition defined coordinatewise and with the lexicographic ordering $(q_1, z_1) < (q_2, z_2)$ if and only if $q_1 < q_2$ or $q_1 = q_2$ and $z_1 < z_2$. The integers $\mathbb{Z}$ are embedded in G as $\{0\} \times \mathbb{Z} \subset G$. Since $(0,1) \in G$ is the least positive element and $G/\mathbb{Z} = Q \times Z/\mathbb{Z}$ is divisible, G is a $\mathbb{Z}$-group. In order to prove the proposition, we shall show two claims.

Claim 5.3. *There is no multiplication $\times$ on G satisfying the rules $x < y \to xz < yz$, $(x \pm y)z = xz \pm yz$, and $1z = z$.*

Proof. Suppose that such a multiplication exists. Let $a = (q, 0)$, $q > 0$ $(q \in Q)$. Then $a > (0, z)$ for all $z \in Z$. Consider the map $G \to G/Z$ defined as $x \mapsto [xa]$. This is a one-to-one order preserving homomorphism of G into $G/Z \simeq Q$ since if $x > y$ then $(x-y)a > 1a = a > (0, z)$ for all $z \in Z$, and hense, $[xa] \neq [ya]$. But it is a contradiction because $|G| > 2^{\aleph_0}$ and $|Q| = 2^{\aleph_0}$. $\square$

Claim 5.4. *G is $\aleph_1$-saturated.*

Proof. Let $\Sigma(x)$ be a non-algebraic complete type over a countable $A \subset G$. Using the elimination of quantifiers for $\mathrm{Th}(\mathbb{Z}, 0, 1, +, <, \equiv_n)_{n \in \mathbb{N}}$, we can replace each formula of $\Sigma(x)$ by a disjunction of conjunctions of atomic formulas in $\{0, 1, +, <, \equiv_n\}_{n \in \mathbb{N}}$. Since $\Sigma(x)$ is maximal we have that $\Sigma(x)$ is equivalent to $\Sigma_1(x) \cup \Sigma_2(x) \cup \Sigma_3(x)$, where $\Sigma_1(x)$ is a set of formulas of the form $x \equiv_n i_n, i_n \in \mathbb{N}$ and $\Sigma_2(x)$ is a set of formulas of the form $j_n x \gtrless t_n(\overline{a}_n), \overline{a}_n \in A$ and $j_n \in \mathbb{N}$, where $t_n(\overline{y}_n)$ is a term whose variables are $\overline{y}_n$ and $\mathrm{ln}(\overline{y}_n) = \mathrm{ln}(\overline{a}_n)$, and $\Sigma_3(x)$ is a set of equalities. Since $\Sigma(x)$ is non-algebraic, $\Sigma_3(x)$ is empty. Let $t_n(\overline{a}_n) = j_n b_n + r_n, 0 \leq r_n < k_n$. Then $k_n x \gtrless t_n(\overline{a}_n)$ if and only if $x \gtrless b_n$. Let $\Sigma_2'(x)$ be the set of formulas of this form corresponding to the formula of $\Sigma_2(x)$. Then $\Sigma(x)$ is equivalent to $\Sigma_1(x) \cup \Sigma_2'(x)$. Let $\overline{\Sigma}_2(x) = \{x \gtrless [c] : x \gtrless c \in \Sigma_2'(x)\}$. Hence $\overline{\Sigma}_2(x)$ is a countable set of formulas in $G/Z \simeq Q$.

If $\overline{\Sigma}_2(x)$ is consistent then there is a realization $q_0 \in Q$ of $\overline{\Sigma}_2(x)$. Then all the inequalities in $\Sigma_2'(x)$ are satisfied by (q_0, a) for any $a \in Z$. Choose $z_0 \in Z$ satisfying $\Sigma_1(x)$. Then (q_0, z_0) satisfying $\Sigma(x)$.

If $\overline{\Sigma}_2(x)$ is inconsistent then there are two inequalities $b_1 < x < b_2$ in $\Sigma_2'(x)$ with $[b_1] = [b_2]$. Let $q_0 \in Q$ with $[(q_0, 0)] = [b_1] = [b_2]$. Let $\overline{\overline{\Sigma}}_2(x) = \{x \gtrless z : x \gtrless (q_0, z) \in \Sigma_2(x)\}$. Think of $\Sigma_1(x) \cup \overline{\overline{\Sigma}}_2(x)$ as a type in Z over some countable subset of Z. It is finitely satisfiable. Hence by the $\aleph_1$-saturation of Z we can choose $z_0 \in Z$ which satisfies it. Then (q_0, z_0) satisfies $\Sigma_1(x) \cup \Sigma_2'(x)$ in G. $\square$

By Claim 5.3. 5.4, G satisfies the required properties in the proposition. $\square$

Proposition 5.5. *Suppose K is a p-adically closed field and $N \subset K$ is an arithmetic part which is a model of PA. Then there is an isomorphism from $(vK_{\geq 0}, +, 0, 1, <)$ to $(N, +, 0, 1, <)$.*

Proof. First of all, we note that the exponential function p^x is definable function on N since N is a model of PA. We denote p^N is the set $\{p^a : a \in N\}$. First, we cheek the valuation map $v : (p^N, \times, 1, p) \to (vK_{\geq 0}, +, 0, 1)$ is an isomorphism. Indeed, since $N \subset \mathcal{O}_K$, $v(p^N) \subset v(N) \subset vK_{\geq 0}$. And, if $a \in N$ is non-zero, then there is $b \in N$ such that $a = b + 1$, hence $v(p^a) = v(p^{b+1}) = v(p^b) + 1 > 0$. This shows the injectivity of $v : (p^N, \times, 1, p) \to (vK_{\geq 0}, +, 0, 1)$. The subjectivity of $v : (p^N, \times, 1, p) \to (vK_{\geq 0}, +, 0, 1)$ is implied by the density of N. Indeed, for any $\gamma \in vK_{\geq 0}$, by density of N, there is $c \in N$ such that $v(c) = \gamma$. We write c as bp^a where $a, b \in N$ and $(b, p) = 1$.

Claim 5.6. *If $(b, p) = 1$ then $v(p) = 0$.*

Proof. We prove by induction on b. Since K is p-adically closed field, for b $(0 \leq b \leq p-1)$ $v(b) = 0$. So, we may assume that $b \geq p$. Suppose that $(b,p) = 1$ and for any $b' < b$ if $(b',p) = 1$ then $v(b') = 0$. Then $v(b-p) = 0$. By strong triangular inequality, $v(b) = \min\{v(b-p), v(p)\} = v(b-p) = 0$. □

Hence, $\gamma = v(c) = v(bp^a) = v(p^a)$. This shows the subjectivity of $v : (p^N, \times, 1, p) \to (vK_{\geq 0}, +, 0, 1)$, so it is an isomorphism.

We can check easily that the exponential map $p^x : (N, +, 0, 1) \to (p^N, \times, 1, p)$ is an isomorphism. Thus, there is an isomorphism $v \circ p^x : (N, +, 0, 1) \to (vK_{\geq 0}, +, 0, 1)$. Clearly, this isomorphism preserves both orders. □

Fact 5.7 ([6]). *In the theory pCF, the multiplicative subgroup of non-zero n-th powers has finite index with coset representatives among the λp^r, $0 \leq r < m$ and $v(\lambda) = 0$.*

Proposition 5.8. *Suppose G is an $\aleph_1$-saturated $\mathbb{Z}$-group. Then the p-adic Hahn field $\mathbb{F}_p((p^G))$ is $\aleph_1$-saturated.*

Proof. Suppose $\Sigma(x)$ is a non-algebraic complete type over a countable set $A \subset \mathbb{F}_p((p^G))$. Without loss of generality, $\Sigma(x)$ is of the form $\{\varphi_i(x) : i \in \mathbb{N}\}$, where $\varphi_i(x)$ is a $L_V(A)$-formula and $\mathbb{F}_p((p^G)) \models \forall x(\varphi_{i+1}(x) \to \varphi_i(x))$ for all $i \in \mathbb{N}$. By p-adic cell decomposition theorem (see, [5]) and the completeness of $\Sigma(x)$, we may assume that for all $i \in \mathbb{N}$, $\varphi_i(x)$ is a cell

$$\{x : g_i \leq v(x - t_i) \leq h_i,\ x - t_i \in d_i(\mathbb{F}_p((p^G))^\times)^{m_i}\},$$

where $g_i, h_i \in G \cup \{\infty, -\infty\}, t_i, d_i(\neq 0) \in \mathbb{F}_p((p^G)), m_i \in \mathbb{N}$.

Claim 5.9. *Suppose $C = \{x : g \leq v(x-t) \leq h,\ x - t \in d(\mathbb{F}_p((p^G))^\times)^m\}$ is a cell. Then for any $a \in \mathbb{F}_p((p^G))$, $a \in C$ if and only if there is $r \in \mathbb{N}$ with $0 \leq r < m$ and $\lambda, \mu \in \mathbb{F}_p((p^G))$ with $v(\lambda) = v(\mu) = 0$ such that $v(a - (t + p^{v(a-t)}\lambda\mu^m)) > v(a-t) + 2v(m)$ and $g \leq v(a-t) \leq h$, where $d(\mathbb{F}_p((p^G))^\times)^m = \lambda p^r(\mathbb{F}_p((p^G))^\times)^m$.*

Proof. Note that, by Hensel's Lemma, the following (a) and (b) are equivalent; for $x \in \mathbb{F}_p((p^G))$ with $v(x) = 0$, (a) x is a m-th power, (b) there is $\mu \in \mathbb{F}_p((p^G))$ with $v(\mu) = 0$ such that $v(x - \mu^m) > 2v(m)$.

Suppose $d(\mathbb{F}_p((p^G))^\times)^m = \lambda p^r(\mathbb{F}_p((p^G))^\times)^m$ as described in Fact 5.7. The condition $a - t \in \lambda p^r(\mathbb{F}_p((p^G))^\times)^m$ is equivalent to $(a-t)p^{-v(a-t)-r}\lambda^{-1} \in (\mathbb{F}_p((p^G))^\times)^m$. Since $v((a-t)p^{-v(a-t)}\lambda^{-1}) = 0$, there is $\mu \in \mathbb{F}_p((p^G))$ with $v(\mu) = 0$ such that $v((a-t)p^{-v(a-t)}\lambda^{-1} - \mu^m) > 2v(m)$. Hence, we have $v(a - (t + p^{v(a-t)}\lambda\mu^m)) > v(a-t) + 2v(m)$. □

By the above claim and our assumption, there are $\{s_i \in \mathbb{F}_p((p^G)) : i \in \mathbb{N}\}$ and $\{\gamma_i \in G : i \in \mathbb{N}\}$ such that, for all i, $s_i \in C_i$, $\max\operatorname{supp}(s_i) = \gamma_i + 2v(m_i)$, $\gamma_i + 2v(m_i) \leq \gamma_{i+1} + 2v(m_{i+1})$, and $v(s_{i+1} - s_i) > \gamma_i + 2v(m_i)$. Let $s \in \mathbb{F}_p((p^G))$ be the natural limit of $\{s_i : i \in \mathbb{N}\}$. Since G is $\aleph_1$-saturated, there is $\gamma \in G$ such that $\gamma_i + 2v(m_i) < \gamma$ for all $i \in \mathbb{N}$. Then, any $e \in B_\gamma(s)$ is a realization of $\Sigma(x)$. So $\mathbb{F}_p((p^G))$ is $\aleph_1$-saturated. □

Proof of Theorem 2.3. Suppose G is a $\aleph_1$-saturated $\mathbb{Z}$-group indicated by Proposition 5.2. By Proposition 5.8, the p-adic Hahn field $\mathbb{F}_p((p^G))$ is $\aleph_1$-saturated p-adically closed field. If $\mathbb{F}_p((p^G))$ has an arithmetic part N which is a model of PA, then, by Proposition 5.5, $(G, 0, 1, <)$ is isomorphic to $(N, 0, 1, <)$. It is a contradiction. □

References

[1] P.D'Aquino, J.K.Knight and S.Starchenko, *Real Closed Fields and Models of Peano Arithmetic*, The Journal of Symbolic Logic, vol.75, 2010.

[2] M.H.Mourgues and J.P.Ressayre, *Every real closed field has an integer part*, The Journal of Symbolic Logic, vol.58, 1993.

[3] W.Hodges, *Model Theory*, Encyclopedia of Mathematics and its Applications, vol.42, Cambridge University Press, 1993.

[4] J.Ax and S.Kochen, *Diophantine Problems Over Local Fields II*, American Journal of Mathematics, 1984.

[5] L.van den Dries, *Algebraic theories with definable Skolem functions*, The Journal of Symbolic Logic, vol.49, 1984.

[6] L. Bélair, *Panorama of p-adic Model Theory*, Annales des sciences mathématiques du Québec, vol.36, 2012.

[7] L.Lipshitz and M.Nadel, *The Additive Structure of Models of Arithmetic*, Proceedings of The American Mathmatical Society, Vol.68, No.3, 1978.

[8] B.Poonen, *Maximally Complete Fields*, preprint, 1992.

[9] D.Marker and C.Steinhorn, *Uncountable Real closed Fields with PA Integer Parts*, arXiv:1205.5156v1, 2012.

[10] M.Yanagawa, *p-adically closed fields and models of Peano arithmetic*, preprint, 2013.