P-CONVEXLY VALUED RINGS

NICOLAS GUZY

Abstract. In [3], L. Bélair developed a theory analogous to the theory of real closed rings in the p-adic context, namely the theory of p-adically closed integral rings. Firstly we use the property proved in Lemma (2.4) in [4] to express this theory in a language including a p-adic divisibility relation and we show that this theory admits definable Skolem functions in this language (in the sense of [17]). Secondly, we are interested in dealing with some questions similar to that of [1]; e.g. results about integral-definite polynomials over a p-adically closed integral ring A and a kind of "Nullstellensatz" using the notion of $\mathcal{M}_A$-radical.

Keywords: p-adically closed fields, model-completeness, definable Skolem functions, Nullstellensatz.
Mathematics Subject Classification: 03C10; 12J12.

1. Introduction

First we recall some notions, model-theoretic results and notations. Let $\mathcal{L}_{\text{rings}}$ be the usual language of rings and let $\mathcal{L}_{\text{fields}}$ be the language of fields, i.e. $\mathcal{L}_{\text{rings}} \cup \{^{-1}\}$. Let $\mathcal{L}_{\mathcal{D}}$ be an expansion of the language of rings with a two-ary predicate $\mathcal{D}(\cdot,\cdot)$. Let A be an unitary commutative domain with a valuation v on its fraction field, denoted by $Q(A)$. Suppose that A is the valuation ring of $\langle Q(A), v\rangle$. Then we define a binary relation (which will be interpreted by the set of 2-tuples such that $v(a) \leqslant v(b)$) as follows:

$\mathcal{D}$ is transitive, $\neg\mathcal{D}(0,1)$, compatible with $+$ and $.$ and either $\mathcal{D}(a,b)$ or $\mathcal{D}(b,a)$. We can extend $\mathcal{D}$ to the fraction field of A as follows:

$$\mathcal{D}(\frac{a}{b},\frac{c}{d}) \iff \mathcal{D}(ad,bc).$$

So the divisibility relation on $Q(A)$ induces the initial valuation v by defining $v(a) \leqslant v(b)$ if $\mathcal{D}(a,b)$. In the sequel, if $\langle K, v\rangle$ is a valued field then the valuation ring, the valuation ideal, the residue field and the value group of $\langle K, v\rangle$ are respectively denoted by $\mathcal{O}_K$, $\mathcal{M}_K$, k_K and $v(K^\times)$, and if A is a valuation ring then we denote the maximal ideal and the residue field of A, by $\mathcal{M}_A$ and k_A, respectively. We denote the canonical residue map $A \longmapsto k_A$ by $\bar{\cdot}$. In order to specify the valuation v for which we consider these objects, we put a subscript v. For any ring A, we denote the set $A \setminus \{0\}$ by $A^\bullet$ and the set of its units by $A^\times$. For any elements a, b in A, $a|b$ means that there exists c in A such that $ac = b$. For any subsets B, C of a valued field $\langle K, v\rangle$, we say that $v(B) < v(C)$ if for any $b \in B$, $c \in C$ we have $v(b) < v(c)$.

Date: October 11, 2004.

[1] "Aspirant" at the "Fonds National de la Recherche Scientifique".

[2] Partially supported by a grant of the National Bank of Belgium and by INTAS contract 2000-447.

Recall that a p-valued field $\langle K, v\rangle$ of p-rank d, with p a prime number, is a valued field of characteristic 0, residue field of characteristic p and the dimension of $\mathcal{O}_K/(p)$ over the prime field $\mathbb{F}_p$ is equal to d (v is called a p-valuation of p-rank d on K). An element of a p-valued field is called prime if its value is the least positive value of $v(K^\times)$.

Let K be a p-valued field of p-rank d. We say that a valued field extension L of K is a p-valued extension of p-rank d if the valuation of L is a p-valuation of p-rank d on L which extends the valuation of K (i.e. $\mathcal{O}_K \subseteq \mathcal{O}_L$ and $\mathcal{M}_L \cap K = \mathcal{M}_K$). We say that K is a p-adically closed field of p-rank d if K does not admit any proper p-valued algebraic extension with the same p-rank d. In Theorems (3.1) and (3.2) of [12], a characterization of the p-adically closed fields of p-rank d is given and the notion of a p-adic closure is established with a criterion for uniqueness : K is p-adically closed if and only if K is henselian and, moreover its value group is a $\mathbb{Z}$-group; the necessary and sufficient condition for K to admit an unique p-adic closure up to K-isomorphism (i.e. an algebraic p-valued extension which is a p-adically closed field of p-rank d) is that its value group is a $\mathbb{Z}$-group. For the notion of henselian valued fields and Henselization of a valued field, we can refer to [14] or [15]. In this paper, we restrict ourselves with p-valuations of p-rank 1 (i.e. $v(p)$ is a prime element and the residue field is equal to $\mathbb{F}_p$) like in the papers of [3] and [4]. However, many of our results remain valid for p-valued fields with fixed p-rank d ($d \in \mathbb{N}$) after adequate enrichment of the language as the reader can easily check.

Let $\mathcal{L}_{\mathcal{D}}^{P_\omega}$ be the language $\mathcal{L}_{\text{fields}} \cup \{\mathcal{D}\} \cup \{P_n; n \in \omega \setminus \{0,1\}\} \cup \{c_2, \cdots, c_d\}$; this language is known as Macintyre's language (see [9]). In Theorem (5.6) of [12], Prestel and Roquette show that the $\mathcal{L}_{\mathcal{D}}^{P_\omega}$-theory pCF_d of p-adically closed fields of p-rank d admits quantifier elimination. In [2] L. Bélair gave an explicit axiomatization of the universal part of pCF_d in the language $\mathcal{L}_{\mathcal{D}}^{P_\omega}$.

In the table below we summarize the analogies between "p-adic" and "real"; the first two items have been object of study for several decades, the last one is the main topic of this paper.

p-adically closed field (pCF)	$\Longleftrightarrow$	real closed field
p-adically closed integral ring (Bélair)	$\Longleftrightarrow$	real closed (valuation) ring (Cherlin-Dickmann)
p-convexly valued ring (pCVR)	$\Longleftrightarrow$	convexly ordered valuation ring (Becker).

Indeed, in Section (2), we introduce a notion of p-convexly valued domain which is the p-adic counterpart of Becker's convexly ordered valuation rings and give a set of axioms in a suitable language. We prove some analogues of results in [2]. We also give a variant of Bélair's set of axioms for the first-order theory of p-adically closed integral rings which are the p-adic counterpart of real closed valuation rings. By using a criterion due to van den Dries [17], we show that the first-order theory of p-adically closed integral rings has definable Skolem functions in a suitable extension of Macintyre's language for p-adic fields. In Section (3), we settle the analogue of Hilbert's seventeenth problem for p-adically closed integral rings by using a relative form of Kochen's operator. In Section (4), we prove a Nullstellensatz for p-adically closed integral rings by using the notions of $\mathcal{M}$-radical of an ideal and of p-adic ideal (introduced by Srhir [16], this notion corresponds to that of real ideal). We close this paper by investigating the generalized notion of model-theoretic radical of an ideal in the context of p-adically closed integral rings similarly to [7].

2. Preliminaries

In the sequel, we work with unitary commutative rings of characteristic zero. First we introduce the notion of p-convexity for domains with p-valued fraction fields. *Let us recall that we consider only p-valued fields of p-rank* 1 *throughout this paper.* We begin with a definition.

Definition 2.1. Let A be a domain containing $\mathbb{Q}$. We say that A is a p-valued domain if A is not a field and its fraction field $Q(A)$ is p-valued.

Definition 2.2. Let F be a p-valued field, with its p-valuation denoted by v_p, and let $A \subseteq B$ be two subsets of F. We say that A is p-convex in B if for all $a \in A$ and $b \in B$, $v_p(a) \leqslant v_p(b)$ implies $b \in A$.

From now on, we prove some elementary results for p-valued domains in the style of [1].

Lemma 2.3. *Let $\langle F, v_p\rangle$ be a p-valued field and let A be a p-valued domain which is p-convex in F. Then A is a valuation ring and $F = Q(A)$.*

Proof. Let f be in F. Then we have $v_p(1) \leqslant v_p(f)$ or $v_p(f) \leqslant v_p(1)$; this means f or $f^{-1} \in A$ by p-convexity of A in F. This clearly shows that A is a valuation ring of F. □

Notation 2.4. The previous lemma shows that any p-convex subdomain A of a p-valued field F supports a valuation v which corresponds to a divisibility relation $\mathcal{D}$ on the domain A. In the sequel the notation $\mathcal{M}_A$ and k_A are relative to the valuation v.

Lemma 2.5. *Let A be a p-valued domain. Then the following are equivalent:*

(1) *A is p-convex in $Q(A)$;*
(2) *A is a valuation ring and $\mathcal{M}_A$ is p-convex in A;*
(3) *A is a valuation ring and $\mathcal{M}_A$ is p-convex in $Q(A)$;*
(4) *A is a valuation ring and for every $a \in \mathcal{M}_A$, $v_p(a)$ is larger than the value of any rational number in $Q(A)$;*
(5) *A is a valuation ring and for every $a \in \mathcal{M}_A$, $v_p(a) > 0$;*
(6) *$A \models \forall x, y \left(v_p(x) \leqslant v_p(y) \rightarrow \exists z(xz = y)\right)$.*

Proof. (1)→(2): Suppose A is p-convex in $Q(A)$. By Lemma (2.3), A is a valuation ring. Let x in $\mathcal{M}_A$ and y in A be such that $v_p(x) \leqslant v_p(y)$ (we may assume x and y different from 0); hence $v_p(1) = 0 \leqslant v_p(y/x)$ ($y/x \in Q(A)$). Since A is p-convex in $Q(A)$, we have $y/x \in A$ and so, $y = x \cdot y/x \in \mathcal{M}_A$.

(2)→(3): Let x in $\mathcal{M}_A$ and u, v in $A^\bullet$ be such that $v_p(x) \leqslant v_p(u/v)$. If $u/v \in A$ then by p-convexity of $\mathcal{M}_A$ in A, $u/v \in \mathcal{M}_A$. Suppose $u/v \notin A$. Since A is a valuation ring, we have $v/u \in \mathcal{M}_A$. So, $x \cdot v/u \in \mathcal{M}_A$ and $v_p(x \cdot v/u) \leqslant v_p(1) = 0$ implies $1 \in \mathcal{M}_A$, this is a contradiction.

(3)→(4): Suppose $a \in \mathcal{M}_A$ such that $v_p(a) \leqslant v_p(q)$ for some $q \in \mathbb{Q}$; so $q \in \mathcal{M}_A$, hence $\frac{1}{q} \notin A$, contradicting that A contains $\mathbb{Q}$.

(4)→(5): Trivial since $v_p(p) = 1$.

(5)→(6): Let x, y in $A^\bullet$ be such that $v_p(x) \leqslant v_p(y)$. We have to show that $y/x \in A$. Otherwise $x/y \in \mathcal{M}_A$ and, by (5), $v_p(x/y) > 0$, which contradicts the assumption.

(6)→(1): Suppose $x, y, z \in A$, $z \neq 0$ and $v_p(x) \leqslant v_p(y/z)$. Then $v_p(xz) \leqslant v_p(y)$ implies $xz|y$, i.e. there exists c in A such that $xzc = y$ and so, $y/z = xc \in A$. □

Definition 2.6. A p-convexly valued domain A is a p-valued domain which satisfies one of the previous equivalent properties.

Let $\mathcal{L}$ be the following expansion of the language of rings, $\mathcal{L}_\mathcal{D} \cup \{\mathcal{D}_p(\cdot,\cdot)\}$. It is easy to see from the previous lemmas that, with $\mathcal{D}$ interpreted as divisibility and $\mathcal{D}_p(x, y)$ as $v_p(x) \leqslant v_p(y)$, any p-convexly valued domain satisfies the following set of $\mathcal{L}$-axioms:

(1) Axioms for a $\mathbb{Q}$-algebra;
(2) $\forall x, y\,[(xy = 0) \Rightarrow (x = 0) \vee (y = 0)]$;
(3) $\forall x, y\,[\mathcal{D}_p(x, y) \vee \mathcal{D}_p(y, x)]$;
(4) $\forall x, y, z\,[\mathcal{D}_p(x, y) \wedge \mathcal{D}_p(y, z) \Rightarrow \mathcal{D}_p(x, z)]$;
(5) $\forall x, y, x', y'\,[\mathcal{D}_p(x, y) \wedge \mathcal{D}_p(x', y') \Rightarrow \mathcal{D}_p(xx', yy')]$;
(6) $\forall x, y, y'\,[\mathcal{D}_p(x, y) \wedge \mathcal{D}_p(x, y') \Rightarrow \mathcal{D}_p(x, y + y')]$;
(7) $\neg\mathcal{D}_p(p, 1)$;
(8) $\forall x\,[\mathcal{D}_p(1, x) \Rightarrow \bigvee\{\mathcal{D}_p(p, x - i) : 0 \leqslant i < p\}]$;
(9) $\forall x\,[\mathcal{D}_p(x, 1) \vee \mathcal{D}_p(p, x)]$;
(10) $\forall x, y\,[\mathcal{D}(x, y) \iff \exists z(x \cdot z = y)]$;
(11) $\exists z\,[\neg(\mathcal{D}(z, 1)) \wedge \neg(z = 0)]$;
(12) the condition of divisibility compatibility for the p-valuation and the divisibility:
$$\forall x, y\,[\mathcal{D}_p(x, y) \Rightarrow \mathcal{D}(x, y)].$$

It is not difficult to show that any model A of the previous set of axioms is a p-convexly valued domain: the first part of the list says that $Q(A)$ is a p-valued field of p-rank 1 and the last three axioms enforce that A is p-convex in $Q(A)$ (by using (6) of Lemma (2.5)). So this list is an axiomatization of the theory of p-convexly valued domains. This $\mathcal{L}$-theory is denoted by $pCVR$ (this means $\underline{p}$-$\underline{c}$onvexly $\underline{v}$alued $\underline{r}$ings).

Remark 2.7. If A is a p-convexly valued domain then by definition, its fraction field $Q(A)$ is a p-valued field. So we can interpret the two-ary predicate $\mathcal{D}_p$ as the restriction of the p-divisibility relation with respect to the p-valuation on $Q(A)$. The condition of divisibility compatibility for p-convexly valued domains implies that it is a valuation ring and that the valuation is induced by divisibility in the domain. Note that the axioms which express that $\mathcal{D}$ is a divisibility relation are included in the universal part of $pCVR$, and by Axiom (11), the divisibility relation on a model of $pCVR$ is never trivial.

Notation 2.8. In the sequel, if A is a p-convexly valued domain then we denote by v_p the corresponding p-valuation on $Q(A)$ and by v, the valuation corresponding to divisibility in the domain A. We sometimes use the same v_p for an extension of the p-valuation.

We continue in the style of [1] in order to find conditions to determine when a p-convexly valued domain A is a $\mathcal{L}$-substructure of a p-convexly valued domain B. The next lemma yields such a criterion.

Lemma 2.9. *Let $\mathcal{A}$, $\mathcal{B}$ be two $\mathcal{L}$-structures which are models of $pCVR$ and B is a p-convexly valued domain extension of A (i.e. $\langle A, \mathcal{D}_p\rangle \subseteq \langle B, \mathcal{D}_p\rangle$ or $Q(A) \subseteq Q(B)$ as p-valued fields). Then the following are equivalent:*

1. $\mathcal{A} \subseteq_{\mathcal{L}} \mathcal{B}$;
2. $A \cap \mathcal{M}_B = \mathcal{M}_A$;
3. $Q(A) \cap B = A$;
4. *for all* $a \in Q(A) \setminus A$ *and* $b \in B$, $v_p(b) > v_p(a)$.

Proof. (1)→(2): Clearly we have $A \cap \mathcal{M}_B \subseteq \mathcal{M}_A$. Let a in A be such that $B \models \neg\mathcal{D}(a, 1)$. Since $\mathcal{A} \subseteq_{\mathcal{L}} \mathcal{B}$, we have $A \models \neg\mathcal{D}(a, 1)$ and we get $A \cap \mathcal{M}_B \supseteq \mathcal{M}_A$.

(2)→(3): Let a, b in $A^\bullet$ be such that $a/b \in B$. If $a/b \notin A$ then $b/a \in \mathcal{M}_A$. Since $\mathcal{M}_A = \mathcal{M}_B \cap A$, we have $b/a \in \mathcal{M}_B$ and $1 = b/a \cdot a/b \in \mathcal{M}_B$, this is a contradiction.

(3)→(4): Let a be in $Q(A) \setminus A$ and $b \in B$. Since $Q(A) \cap B = A$, we have $a \notin B$ and so, $a^{-1} \in \mathcal{M}_B$, i.e. $v_p(a^{-1}) > 0$. Hence if $v_p(b) \leqslant v_p(a)$ then we have $v_p(b \cdot a^{-1}) \leqslant v_p(1)$ where $b \cdot a^{-1} \in \mathcal{M}_B$. Since B is a p-convexly valued domain, we get $1 \in \mathcal{M}_B$, this is a contradiction.

(4)→(1): Let a, b in $A^\bullet$ be such that there exists $c \in B$ satisfying $ac = b$. So $c \in Q(A)$. If $c \notin A$ then $c \in Q(A) \setminus A$ and so, we have $v_p(c) > v_p(c)$ by (4). □

Lemma 2.10. *Let A be a p-convexly valued domain A. Then $v_p(A^\times)$ is a p-convex subgroup of $v_p(Q(A)^\times)$.*

Proof. Let x, y in $A^\times$ and u, v in A be such that $v \neq 0$ and $v_p(x) \leqslant v_p(u/v) \leqslant v_p(y)$. So we have that $v_p(x \cdot v) \leqslant v_p(u)$. By the condition of divisibility compatibility, there exists an element c of A such that $x \cdot v \cdot c = u$. Hence we obtain $u/v = x \cdot c \in A$ and again by the condition of compatibility, there exists an element d of A such that $y = d \cdot u/v$. We conclude that u/v belongs to $A^\times$ since $y \in A^\times$. □

Remark 2.11. If A is a p-convexly valued domain then by p-convexity of $\mathcal{M}_A$ in A, we have $v_p(A^\times) < v_p(\mathcal{M}_A)$.

So we can define a p-valuation on the residue field k_A of A, denoted by $\widetilde{v}_p$, as follows: if $x = 0$ in k_A then $\widetilde{v}_p(x) = \infty$; otherwise if $x \neq 0$ in k_A, we take $y \in A^\times$ such that $\overline{y} = x$ and define $\widetilde{v}_p(x)$ as $v_p(y)$. By Remark (2.11), $\widetilde{v}_p$ is well-defined and k_A is a p-valued field by the axiom-schemes $pCVR$.

In the next paragraph we give a new axiomatization of p-adically closed integral rings which were introduced in [3]. Our candidate for such an axiomatization is the following list which will denote by $pCIR$.

Definition 2.12. *pCIR* is the following set of $\mathcal{L}$-sentences:

1. the set of axioms for the $\mathcal{L}$-theory of p-convexly valued rings;
2. for each integer $n > 0$, $\forall x\, \exists y\, [\mathcal{D}(x, y^n) \wedge \mathcal{D}(y^n, x)]$;
3. for each integer $n > 0$,
$$\forall a_0, \cdots, a_{n-1}\, [\mathcal{D}(a_{n-1}, 1) \wedge \textstyle\bigwedge_{i=0}^{n-2} \neg\mathcal{D}(a_i, 1)] \Rightarrow \\ \exists x\, [x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \wedge \mathcal{D}(x, 1)];$$
4. for each integer $n > 0$,
$$\forall x\, \exists y\, [\mathcal{D}(x, 1)] \Rightarrow \bigvee_{0 \leqslant r < n} \{\mathcal{D}_p(y^n p^r, x) \wedge \mathcal{D}_p(x, y^n p^r)\};$$
5. for each integer $n > 0$,
$$\forall a_0, \cdots, a_{n-1}\, [\mathcal{D}_p(1, a_{n-1}) \wedge \mathcal{D}_p(a_{n-1}, 1) \wedge \textstyle\bigwedge_{i=0}^{n-2} \mathcal{D}_p(p, a_i)] \Rightarrow \\ \exists x\, [\neg\mathcal{D}(x^n + a_{n-1}x^{n-1} + \cdots + a_0, 1) \wedge \mathcal{D}_p(1, x) \wedge \mathcal{D}_p(x, 1)].$$

We now show that the models of *pCIR* are exactly the p-adically closed integral rings introduced in [3]. In order to prove it, we reformulate Proposition (2.2) and Corollary (2.3) of [3] in our terminology.

Lemma 2.13. *The models of the $\mathcal{L}$-theory of p-adically closed integral rings correspond to henselian p-convexly valued rings with p-adically closed residue field and divisible ordered value group. Moreover, the $\mathcal{L}$-theory of p-adically closed integral rings is complete and model-complete; it has elimination of quantifiers in the language $\mathcal{L}_{rings}$ equipped with predicates P_n for the n-th powers (we replace in the $\mathcal{L}$-theory pCIR the predicate of p-divisibility relation by: $\mathcal{D}_p(x, y) \iff P_\epsilon(x^\epsilon + py^\epsilon)$; $\epsilon = 3$ if $p = 2$, otherwise $\epsilon = 2$ $\quad(*)$.).*

Proof. First we note that in the p-adically closed case membership to the valuation ring is definable by (*)[2]. Let A be a model of the $\mathcal{L}$-theory *pCIR*. Then A is a valuation ring with respect to the divisibility predicate $\mathcal{D}$ and is p-convex in its fraction field. The axioms (2) express that the value group is divisible and the axioms (3) say A is henselian (it is one of the equivalent forms of Hensel's Lemma, see [14]). The axiom-schemes (4) and (5) imply that the p-valued field $\langle k_A, \widetilde{v_p} \rangle$ is p-adically closed where $\widetilde{v_p}$ is the valuation defined as in Remark (2.11). The rest of the proof follows the lines of Corollary (2.3) in [3]. □

We need the next two lemmas to extend p-convexly valued domains in the most natural way possible, i.e. we will use the previous characterization of p-convexly valued domains. Moreover, Lemma (2.9) will help us to build extensions of $\mathcal{L}$-structures.

Lemma 2.14. *Let A be a p-valued domain and let $\langle K, v_p \rangle$ be a p-valued field extension of $Q(A)$ such that there exists an element of K of value lower than $v_p(A^\bullet)$. Then there exists a minimal p-convexly valued domain containing A whose fraction field is K. We will denote this minimal p-convexly valued domain extending A by $pcH(A, K)$. Furthermore, if A is a p-convexly valued domain then $A \subseteq_{\mathcal{L}} pcH(A, K)$.*

Proof. Let $pcH(A,K)$ be the following set $\{k \in K \mid \exists c \in A,\ K \models v_p(c) \leqslant v_p(k)\}$ which is different from K by hypothesis. Clearly it is a p-valued domain and it is p-convex in K. The minimality is deduced from the definition of $pcH(A,K)$. Let us denote $pcH(A,K)$ by $\widetilde{A}$. Lemma (2.3) implies that K is the fraction field of $pcH(A,K)$. For the second part, we have to show that $A \cap \mathcal{M}_{\widetilde{A}} = \mathcal{M}_A$ by Lemma (2.9). Suppose $a \in \mathcal{M}_A$. So, $a^{-1} \notin A$ because A is a valuation ring. If $a^{-1} \notin \widetilde{A}$ then $a \in \mathcal{M}_{\widetilde{A}}$ and the proof is finished. So, suppose $a^{-1} \in \widetilde{A}$. By definition, there exists $b \in A$ such that $v_p(b) \leqslant v_p(a^{-1})$. Hence, $v_p(b \cdot a) = v_p(b) + v_p(a) \leqslant v_p(a^{-1}) + v_p(a) = v_p(1)$. Sice $\mathcal{M}_A$ is p-convex in A, we get $1 \in \mathcal{M}_A$, this is a contradiction. □

In the previous lemma, if A is already a p-convexly valued domain then the hypothesis of having an element of K of value lower than $v_p(A^\bullet)$ is directly satisfied.

Lemma 2.15. *Let A be a p-convexly valued domain and let $\widetilde{Q(A)}$ be a p-adic closure of $Q(A)$ for the p-valuation v_p on $Q(A)$. Then there exists a model $\widetilde{A}$ of pCIR such that $A \subseteq_{\mathcal{L}} \widetilde{A}$. In addition, if the value group of $Q(A)$ is a $\mathbb{Z}$-group then $pcH(A, Q(A)^h)$ is a model of pCIR where $Q(A)^h$ is the Henselization of $Q(A)$ for the p-valuation v_p.*

Proof. Let H be the convex hull of the group $v_p(A^\times)$ in $v_p(\widetilde{Q(A)}^\times)$. Then we consider the set $\widetilde{A} = \{x \in \widetilde{Q(A)} \mid \exists h \in H,\ \widetilde{Q(A)} \models v_p(x) \geqslant h\}$. As in the proof of Proposition (2.5) in [3], we have that $\widetilde{A}$ is a model of $pCIR$. It remains to show that $A \subseteq_{\mathcal{L}} \widetilde{A}$. By Lemma (2.9), it suffices to prove that $A \cap \mathcal{M}_{\widetilde{A}} = \mathcal{M}_A$. Suppose $a \in \mathcal{M}_A$, so $a^{-1} \notin A$. If $a^{-1} \notin \widetilde{A}$ then $a \in \mathcal{M}_{\widetilde{A}}$ and the proof is finished. So we suppose $a^{-1} \in \widetilde{A}$. By definition of $\widetilde{A}$ and H, there exists an element b of $A^\times$ such that $v_p(b) \leqslant v_p(a^{-1})$. We conclude as in the proof of Lemma (2.14). For the second part, since $Q(A)^h$ is an immediate extension of $Q(A)$ for the valuation v_p, the value group of $Q(A)^h$ is a $\mathbb{Z}$-group and so $Q(A)^h$ is p-adically closed. By Remark (2.11) and Lemma (2.14), we have $pcH(A, Q(A)^h) = \{x \in Q(A)^h \mid \exists h \in H,\ Q(A)^h \models v_p(x) \geqslant h\}$ where H is the convex hull of the group $v_p(A^\times)$ in $v_p({Q(A)^h}^\times)$, i.e. it is $v_p(A^\times)$. The rest of the proof is the same as that of Proposition (2.5) in [3]. □

Lemma 2.16. *Let A be a model of the $\mathcal{L}$-theory of p-adically closed integral rings. Then its fraction field $Q(A)$ is p-adically closed.*

Proof. Owing to the p-divisibility on A, we can define the p-valuation v_p of $Q(A)$ as follows:

$$\forall a,b \in A \quad \forall c,d \in A^\bullet, \quad v_p(a/c) \leqslant v_p(b/d) \iff \mathcal{D}_p(ad,bc).$$

Clearly by the axioms of $pCIR$, the fraction field $Q(A)$ is a p-valued field. It remains to show that its value group is a $\mathbb{Z}$-group and that it is henselian with respect to v_p. Since A is a p-convexly valued domain, it is p-convex in $Q(A)$ and so, A contains the valuation ring $\mathcal{O}_{Q(A)}$ of $Q(A)$. To prove that $v_p(Q(A)^\times)$ is a $\mathbb{Z}$-group, it suffices to show that for any integer $n > 0$ and any element x of $Q(A)$ such that $v_p(x) \geqslant 0$ (so $x \in A$), there exists an element y of A and a positive integer r such that $0 \leqslant r \leqslant n-1$ and $v_p(x) = n \cdot v_p(y) + r$ (because p is a prime element of $Q(A)$). Indeed, let x be in $Q(A)$. If $v_p(x) < 0$ then $v_p(x^{-1}) > 0$ implies $x^{-1} \in A$. Hence, by the axiom-scheme

(4) of $pCIR$, there exists an element y of A such that $v_p(x^{-(n-1)}) = n \cdot v_p(y) + r$. We conclude that $v_p(x) = n \cdot (v_p(y) + v_p(x)) + r$ where $0 \leqslant r \leqslant n-1$.

Let x in A be such that $v_p(x) \geqslant 0$ then there exists an element z of A such that $v(x) = v(z^n)$ by the axiom-scheme (2). So $xz^{-n} \in A$ with $v(xz^{-n}) = 0$ where v is the valuation determined by the divisibility predicate $\mathcal{D}$. We apply the axiom-scheme (4) of $pCIR$ and we obtain the requirement. Now we show that $Q(A)$ is henselian. Let $Q(A)^h$ be the Henselization of $Q(A)$ for the p-valuation v_p. By Lemma (2.15), we can consider the minimal p-convexly valued domain $pcH(A, Q(A)^h)$ with fraction field $Q(A)^h$, denoted by $\widetilde{A}$. By Lemma (2.14), $\widetilde{A}$ is a model of $pCIR$ such that $A \subseteq_{\mathcal{L}} \widetilde{A}$. Since the $\mathcal{L}$-theory $pCIR$ is modele-complete and $\widetilde{A}$ is p-convex in $Q(\widetilde{A})$, $Q(A)$ satisfies Hensel's Lemma with respect to v_p on $Q(A)$. Let us check it.
Let $a_0, \ldots, a_{n-1}$ in $Q(A)$ be such that $v_p(a_{n-1}) = 0$ and $v_p(a_i) \geqslant 1$ for all $i \in \{0, \ldots, n-2\}$. Then each a_i belongs to A by p-convexity of A in $Q(A)$. Since $Q(A)^h$ is henselian for the p-valuation v_p, there exists an element b in $Q(A)^h$ such that $b^n + a_{n-1} \cdot b^{n-1} + \cdots + a_0 = 0$ and $v_p(b) = 0$. We have that $b \in pcH(A, Q(A)^h)$ which is a model of $pCIR$.

Thus $\widetilde{A} \models \exists y\, [(y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0) \wedge \mathcal{D}_p(1, y) \wedge \mathcal{D}_p(y, 1)]$. By model-completeness of $pCIR$, we get that

$$A \models \exists y\, [(y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0) \wedge \mathcal{D}_p(1, y) \wedge \mathcal{D}_p(y, 1)]$$

and so, $Q(A)$ is henselian with respect to v_p. □

Now we are interested in the existence of definable Skolem functions in the $\mathcal{L}$-theory of p-adically closed integral rings.

First recall a definition.

Definition 2.17. Let L be a first-order language. Let $\mathcal{A} \subseteq \mathcal{B}$ be two L-structures. We say that $\mathcal{B}$ is rigid over $\mathcal{A}$ if and only if $\mathrm{Aut}(\mathcal{B}/\mathcal{A}) = \{\mathrm{id}\}$ where id is the identity automorphism.

Secondly let us recall a theorem of L. van den Dries which gives a criterion for rigidity.

Theorem 2.18. *(see Theorem (2.1) in* [17]*) Let L be a first-order language and let T be a L-theory which admits quantifier elimination. Then the following are equivalent:*

- *T has definable Skolem functions;*
- *each model $\mathcal{A}$ of $T_\forall$ has an extension $\overline{\mathcal{A}} \models T$ which is algebraic over $\mathcal{A}$ (in the model-theoretic sense) and rigid over $\mathcal{A}$.*

Let $\mathcal{L}_{\mathcal{D},P_\omega}$ be an expansion of the language $\mathcal{L}_{\mathcal{D}}$ by predicates P_n for the n-th powers and a constant $\underline{c}$. We can reformulate the $\mathcal{L}$-theory $pCIR$ in the language $\mathcal{L}_{\mathcal{D},P_\omega}$. For example, the $\mathcal{L}_{\mathcal{D},P_\omega}$-theory $pCIR$ contains axioms which express that the models are not fields, i.e. $\neg\mathcal{D}(c, 1)$ (this assures that the valuation on a $\mathcal{L}_{\mathcal{D},P_\omega}$-substructure of a model of $pCIR$ is never trivial), $\forall x\, (P_n(x) \iff \exists y\, (y^n = x))$ and the p-divisibility relation $\mathcal{D}_p$ is defined as in the statement of Lemma (2.13).

Let A be a model of $pCIR$, i.e. a p-adically closed integral ring. We can define a basis of a Hausdorff topology by:

$$\{D_{(a,b)} \mid a, b \in A,\ b \neq 0\} \text{ where } D_{(a,b)} \text{ is the set}$$
$$\{x \in A \mid A \models \mathcal{D}_p(b, x-a) \wedge \neg\mathcal{D}_p(x-a, b)\}.$$

It is called the p-valuation topology on A. So, $\langle A, D_{(x,y)}\rangle$ is a first-order topological structure in the sense of [11, p. 765, example (e)].

Let us show topological results on the sets defined by the previous predicates.

Lemma 2.19. *Let A be a model of $pCIR$. Then the sets ${P_n}^A = \{a \in A^\bullet \mid A \models P_n(a)\}$, are clopen for the p-valuation topology on A, for each integer $n > 0$.*

Proof. Let $Q(A)$ be the fraction field of A which is a p-adically closed field. Let us consider the set of n-th powers $\overline{P_n}$ in $Q(A)$ which extends the set P_n in A (i.e. if $Q(A) \models \exists b\,(b^n = a)$ where $a \in A$ then $b \in A$ because A is integrally closed). It is well-known that the set $\overline{P_n}$ in $Q(A)^\bullet$ is clopen for the p-valuation topology on $Q(A)$. So, since A is a clopen set in $Q(A)$, ${P_n}^A$ is clopen for the topology on A induced by the p-valuation topology on $Q(A)$. It remains to show that ${P_n}^A$ is clopen for the p-valuation topology on A. The fact that it is closed is clear by definition of topologies. Suppose $a \in A$ is such that ${P_n}^A(a)$. By Lemma (2.3) of [8], we have that $a \in \mathcal{D}_{(a,an^2)} \subseteq {P_n}^A$ and the proof is finished. □

The following lemma corresponds to Proposition (1.9) in [6].

Lemma 2.20. *Let A be a p-adically closed integral ring. Then:*

1. *The following subsets of A are open for the p-valuation topology:* $\{x \in A \mid A \models \mathcal{D}(a, x)\}$ *for all* $a \in A^\bullet$, $\{x \in A \mid A \not\models \mathcal{D}(x, a)\}$, $\{x \in A \mid A \not\models \mathcal{D}(a, x)\}$, $\{x \in A \mid A \models \mathcal{D}(x, a)\}$ *for all* $a \in A$.
2. *The following subsets of A^2 are open (when A^2 is endowed with the product topology):* $\{(x, y) \in A^2 \mid A \models \mathcal{D}(x, y)\} \setminus \{(0, 0)\}$, $\{(x, y) \in A^2 \mid A \not\models \mathcal{D}(x, y)\}$.

Proof. (1) Let X_a be one of the two first sets. Let b be an element of X_a. Then the axiom of divisibility compatibility implies that $D_{(0,b)} \subseteq X_a$. Therefore X_a is open. Let us consider the two last sets. Let Y_a be one of these sets and $b \in Y_a$. Then the set $\{x \in A \mid \mathcal{D}_p(x, b)\}$ is included in Y_a which is clearly an open neighborhood of b for the p-valuation topology on A.

(2) Let D be the set $\{(x, y) \in A^2 \mid A \models \mathcal{D}(x, y)\} \setminus \{(0, 0)\}$ and let (x_0, y_0) be in D. Suppose $v_p(x_0) \leqslant v_p(y_0)$ and $y_0 \neq 0$. By the axiom of divisibility compatibility, we get $D_{(x_0,x_0)} \times D_{(y_0,y_0)} \subseteq D$. It is the same argument as above for the case $v_p(x_0) > v_p(y_0)$. So suppose that $y_0 = 0$ and $x_0 \neq 0$. Hence $D_{(x_0,x_0)} \times D_{(0,x_0)} \subseteq D$, again by using the axiom of divisibility compatibility.

Let $D' = \{(x, y) \in A^2 \mid A \not\models \mathcal{D}(x, y)\}$. If $(x_0, y_0) \in D'$ then $y_0 \neq 0$. Assume $x_0 \neq 0$. So $\neg\mathcal{D}(x_0, y_0)$ implies $v_p(x_0) > v_p(y_0)$. It suffices to apply the arguments of (1) to show that there exists an open neighborhood U of (x_0, y_0) contained in D' for the p-valuation topology on A. If $x_0 = 0$ then we choose an element $\epsilon \in \mathcal{M}_A^\bullet$. Hence, the axiom of divisibility compatibility implies $D_{(x_0,\epsilon y_0)} \times D_{(y_0,y_0)} \subseteq D'$, which proves that D' is an open set of A^2. □

The above properties imply that the models of the $\mathcal{L}_{\mathcal{D},P_\omega}$-theory $pCIR$ are proper first-order topological structures (see Definition (2.2) in [10]). So this $\mathcal{L}_{\mathcal{D},P_\omega}$-theory is unstable and has the strict order property (see [11]). Moreover, the models of $pCIR$ are topological systems (see Definition (4.1) in [10]) and we can apply some results of [10] to our setting. For example, by Theorem (4.4) of [10], $pCIR$ is model-theoretically bounded; let A be a model of $pCIR$, if B a subset of A then $\mathrm{acl}_A(B)$ is the field-theoretic algebraic closure of B in A; moreover A is t-minimal (i.e. for every definable $X \subseteq A$, the set $bd(X)$ of boundary points of X in A is finite).

Now we prove the existence of definable Skolem functions for the $\mathcal{L}_{\mathcal{D},P_\omega}$-theory $pCIR$.

Theorem 2.21. *The $\mathcal{L}_{\mathcal{D},P_\omega}$-theory of p-adically closed integral rings has definable Skolem functions.*

Proof. The proof follows the lines of Proposition (3.4) in [17]. By Theorem (2.18), it suffices to prove that each model $\mathcal{A}$ of $(pCIR)_\forall$ has an extension $\overline{\mathcal{A}} \models pCIR$ which is algebraic and rigid over $\mathcal{A}$. Let $\mathcal{A} \subseteq \mathcal{A}^* \models pCIR$ and define $\overline{\mathcal{A}}$ as the substructure of $\mathcal{A}^*$ whose members are the elements of A^* algebraic over the domain A. Write $\overline{\mathcal{A}} = \langle \overline{A}, \overline{\mathcal{D}}(\cdot,\cdot), \underline{c}, \overline{P_2}, \overline{P_3}, \cdots \rangle$. We claim that

$$\overline{\mathcal{A}} \models pCIR. \tag{1}$$

The underlying domain $\overline{A}$ of $\overline{\mathcal{A}}$ is integrally closed in A^*. Since A^* is henselian, $\overline{\mathcal{A}}$ endowed with the restriction of the valuation of A^* is also henselian (let us remark that this restriction corresponds to $\overline{\mathcal{D}}$).

Since $\mathcal{A}$ is a $\mathcal{L}_{\mathcal{D},P_\omega}$-substructure of $\mathcal{A}^*$, the valuation on $\mathcal{A}^*$ is an extension of the valuation on $\mathcal{A}$ and so, on $\overline{\mathcal{A}}$ also. Since $\overline{A}$ is integrally closed in the underlying ring of $\mathcal{A}^*$, it follows that $\overline{P_n}$ is the set of n-th powers of $\overline{A}$. Let x be in $\overline{A}$. Then there exists $e \in \mathbb{N}$ such that $\mathcal{A}^* \models \exists y(y^n = ex)$: indeed, since $Q(A^*)$ is a p-adically closed field, we know that $Q(A^*) \models \exists y(y^n = ex)$ and since A^* is integrally closed in its fraction field, this property holds in A^*. Since $\overline{A}$ is integrally closed in A^* and is a $\mathbb{Q}$-algebra, the value group of $\overline{A}$ is divisible. Since A is a model of $(pCIR)_\forall$, the p-divisibility $\mathcal{D}_p$ on A is defined as in (2.13) with universal axioms of $pCVR$ and the condition of compatibility between $\mathcal{D}_p$ and $\mathcal{D}$ is satisfied in A. The same holds for A^* and $\overline{A}$ which are p-convexly valued domains. Since $\overline{\mathcal{A}} \subseteq_{\mathcal{L}_{\mathcal{D},P_\omega}} \mathcal{A}^*$, the p-divisibility in A^* respects the p-divisibility in $\overline{A}$ and so, we have $\langle k_{\overline{A}}, \widetilde{v}_p\rangle \subseteq \langle k_{A^*}, \widetilde{v}_p\rangle$ (see Remark (2.11)). Let $a_0, \cdots, a_{n-1}$ in $\overline{A}$ be such that $\widetilde{v}_p(\overline{a}_{n-1}) = 0$ and $\widetilde{v}_p(\overline{a}_i) \geqslant 1$ for all $0 \leqslant i \leqslant n-2$. We know that k_{A^*} is henselian with respect to $\widetilde{v}_p$. So there exists b in A^* such that $b^n + a_{n-1}b^{n-1} + \cdots + a_0 \in \mathcal{M}_{A^*}$ and $b \notin \mathcal{M}_{A^*}$. Thus $b \in \mathrm{acl}_{A^*}(a_0, \cdots, a_{n-1})$ and we get $b \in \overline{A}$ which implies that $k_{\overline{A}}$ is henselian (because $\mathcal{M}_{A^*} \cap \overline{A} = \mathcal{M}_{\overline{A}}$).

Let us prove that the value group of the p-valuation $\widetilde{v}_p$ of $k_{\overline{A}}$ is a $\mathbb{Z}$-group. Let x be in $k_{\overline{A}}$. Choose an element y in $\overline{A}$ such that $\overline{y} = x$. Since $\mathcal{A}^*$ is a p-adically closed integral ring, there exists an element z of A^* such that $z^n = ey$ for some $e \in \mathbb{N}$ (as above). So there exists an element z' of $\overline{A}$ such that $z'^n = ey$ and we obtain $\overline{z'}^n = \overline{e}x$

($\overline{e} \neq 0$ because $k_{\overline{A}}$ is of characteristic zero). We conclude that $[\widetilde{v}_p(k_{\overline{A}}^{\times}) : n\widetilde{v}_p(k_{\overline{A}}^{\times})] = n$. So, (1) is proved.

It remains to prove that $\overline{\mathcal{A}}$ is rigid over $\mathcal{A}$. Suppose σ is a $\mathcal{A}$-automorphism of $\overline{\mathcal{A}}$. Take the substructure of $\overline{\mathcal{A}}$ pointwise fixed by σ. Let us write it as $\mathcal{A}^1 = \langle A^1, \mathcal{D}^1, \underline{c}, P_2^1, P_3^1, \cdots \rangle$. Then, for all $n \geqslant 2$, we have that $P_n{}^1 = \{a^n \mid a \in A^1\}$. First, $\langle A^1, \mathcal{D}_p^1, \mathcal{D}^1 \rangle$ is a p-convexly valued domain where $\mathcal{D}_p^1$ and $\mathcal{D}^1$ are restrictions to A^1 of divisibility relations $\mathcal{D}_p$ and $\mathcal{D}$ on $\overline{A}$. We consider the fraction field $Q(\overline{A})$ of $\overline{A}$ and extend the relations in a natural way: for every integer $n \geqslant 2$ and for all $a, b \in Q(\overline{A})^{\bullet}$, $Q(\overline{A}) \models P_n(a/b)$ iff $\overline{A} \models \exists z(z^n = ab^{n-1})$ (because $\overline{A}$ is integrally closed in A^*) and for all $u, v \in A$ and $s, t \in A^{\bullet}$, $Q(\overline{A}) \models \mathcal{D}(u/v, s/t)$ iff $\overline{A} \models \mathcal{D}(ut, sv)$. We extend the automorphism σ of $\overline{A}$ to an automorphism $Q(\sigma)$ of $Q(\overline{A})$. For suppose $a \in P_n{}^1$, $a \neq 0$. Let b be an n-th root of a in $\overline{A}$. Take an integer $m \geqslant 2$. As in the proof of (1), we find a rational $q \neq 0$ with $qb \in \overline{P}_m$; so in $Q(\overline{A})$, we have that $\sigma(qb) \cdot (qb)^{-1} = \sigma(b) \cdot b^{-1} \in P_m(Q(\overline{A}))$. Since $Q(\overline{A})$ is a p-adically closed field and $\sigma(b) \cdot b^{-1}$, an n-th root of unity, is an m-th power in $Q(\overline{A})$ for all m, we obtain $\sigma(b) \cdot b^{-1} = 1$, i.e. $b \in A^1$. By Lemma (2.16), $Q(\overline{A})$ is a p-adically closed field and $Q(A^1)$ is a p-valued field such that its value group is a $\mathbb{Z}$-group (by a previous argument and the form of P_n^1). So, we can extend the A-automorphism σ of $\overline{A}$ to a $Q(A)$-automorphism $Q(\sigma)$ of $Q(\overline{A})$ which has $Q(A^1)$ as pointwise fixed subfield (because A^1 is a valuation ring). As $\langle Q(\overline{A}), \overline{v}_p \rangle$ is henselian for its p-valuation $\overline{v}_p$ (which corresponds to the p-divisibility $\overline{\mathcal{D}}_p$), it contains an Henselization of $\langle Q(A), v_p \rangle$ and the universal property of the Henselization implies that it is fixed by $Q(\sigma)$, hence it is contained in $\langle Q(A^1), v_p^1 \rangle$. Therefore, $\langle Q(A^1), v_p^1 \rangle$ is henselian. So, $Q(A^1)$ is a p-adically closed field. As in the proof of Lemma (2.15), A^1 is a p-adically closed integral ring with respect to $\mathcal{D}_p^1$ and $\mathcal{D}^1$. By Lemma (2.3) of [17], $\overline{\mathcal{A}}$ is a minimal prime model extension of $\mathcal{A}$, as it is algebraic over $\mathcal{A}$. Therefore we have $\mathcal{A}^1 = \overline{\mathcal{A}}$, i.e. σ is the identity automorphism. □

Let A be a p-adically closed integral domain. Since A is clopen for the p-valuation topology of its fraction field and A is a p-convexly valued domain, a corollary of the previous theorem is that the models of $pCIR$ satisfy the property of Local Continuity as defined in [10]. Hence all required properties to guarantee the existence of a Cell decomposition in the sense of [10] are checked in the $L_{\mathcal{D},P_\omega}$-theory of p-adically closed integral rings. In a subsequent paper we explore a more adequate Cell decomposition for this class of p-convexly valued rings.

3. Hilbert's seventeenth problem for p-convexly valued domains

In this section we determine the form of polynomials over a p-adically closed ring A which are integral-definite on A (see Definition (3.12)). It is the analogue of Theorem 2 in [7] for the p-adic case by using the same techniques as in [1], e.g. the model-completeness of $pCIR$. First we provide the tools needed to settle this.

In the whole section, A will be assumed a p-convexly valued domain. Then $Q(A)$ is a p-valued field and $\mathcal{O}_{Q(A)}$ denotes the valuation ring of $Q(A)$ for the p-valuation v_p.

Definition 3.1. Let A be a p-valued domain and let B be a domain extension of A equipped with a valuation v. We say that B is a p-valued domain extension if v is a p-valuation on $Q(B)$ over $Q(A)$ (i.e v is a p-valuation on $Q(B)$ which extends the p-valuation of $Q(A)$).

Remark 3.2. For all $a \in A$, we have $\gamma_p(a) \in A$ where $\gamma_p(X)$ is the Kochen's operator defined by:

$$\gamma_p(X) = \frac{1}{p}\left[\frac{X^p - X}{(X^p - X)^2 - 1}\right]$$

(where $\gamma_p(a)$ is an element of $Q(A)$). This is an immediate consequence of the next lemma. We will denote by ∞ the value of $\gamma_p(b)$ when this value does not exist at b in $Q(A)$.

Let us recall Lemma (6.2) of [12].

Lemma 3.3. *Let k be a p-valued field, let K be a field extension of k and let v be a valuation of K extending the given p-valuation of k. A necessary and sufficient condition for v to be a p-valuation over k (i.e.* $\dim_{\mathbb{F}_p}(\mathcal{O}_K/(p)) = 1$*) is that* $v(\gamma_p(K)) \geqslant 0$.

Theorem 3.4. *Let B be a domain extension, which is not a field, of the p-valued domain A. Let M be a subset of B such that $v_p(M \cap A) \geqslant 0$. A necessary and sufficient condition for B to be a p-valued domain extension of A such that $v_p(M) \geqslant 0$ is that*

$$\frac{1}{p} \notin \mathcal{O}_{Q(A)}[\gamma_p(Q(A)), M]$$

where $\mathcal{O}_{Q(A)}[\gamma_p(Q(A)), M]$ denotes the subring of $Q(B)$ generated by $\gamma_p(Q(A)) \setminus \{\infty\}$ and M over the ring $\mathcal{O}_{Q(A)}$.

Proof. It suffices to adapt the proof of [12, p. 100]. For necessity, we use in addition that $v(M) \geqslant 0$ and the previous lemma. For sufficiency, we use the fact that the ideal generated by p in $\mathcal{O}_{Q(A)}[\gamma_p(Q(A)), M]$ is proper and so, we can invoke the general existence theorem for valuations [13, p. 43]. The hypothesis $v(M \cap A) \geqslant 0$ yields that it is an extension of the p-valuation. ☐

Corollary 3.5. *In the situation of the previous theorem, let v be a valuation of $Q(B)$. A necessary and sufficient condition for v to be a p-valuation over $Q(A)$ such that $v(M) \geqslant 0$ is that v lies above $\mathcal{O}_{Q(A)}[\gamma_p(Q(A)), M]$ and is centered over p.*

Proof. It is just a reformulation of the previous theorem, it suffices to examine its proof. ☐

Now we introduce a particular ring which plays an important role in the extension of a p-valuation, namely to a valued domain extension of the p-valued domain A. It is an adaptation of the classical Kochen ring and of its role in the p-adically closed field case (see Section (6.2) of [12]).

Definition 3.6. For any domain extension B of A which is not a field and M a subset of B, the M-Kochen ring $R^M_{\gamma_p}(B)$ is defined as the subring of $Q(B)$ consisting of quotients of the form

$$a = \frac{b}{1+pd} \text{ with } b, d \in \mathcal{O}_{Q(A)}[\gamma_p(Q(B)), M] \text{ and } 1 + pd \neq 0.$$

Lemma 3.7. *Let A be a model of $pCIR$ and let a be an element of A. Then $\mathcal{D}_p(1,a)$ if and only if there exists an element b in A such that $a = \gamma_p(b)$. Moreover, an element a of A satisfies $\mathcal{D}_p(1,a)$ if and only if $\exists y\,(y^\epsilon = 1 + pa^\epsilon)$; $\epsilon = 3$ if $p = 2$, otherwise $\epsilon = 2$.*

Proof. Clearly, since $Q(A)$ is a p-valued field, if there exists an element b in A such that $a = \gamma_p(b)$ then $v_p(a) \geqslant 0$, i.e. $A \models \mathcal{D}_p(1,a)$. On the other hand, if we consider the polynomial $f(X) = ap[(X^p - X)^2 - 1] - (X^p - X)$ then $f(X)$ admits 1 as a simple zero in the residue field of $Q(A)$. By Hensel's lemma, $f(X)$ has a zero b in A, whence $a = \gamma_p(b)$. For the second part of the statement, it is satisfied in the p-valued fraction field $Q(A)$ and it holds in A because A is an integrally closed ring (see Lemma (2.13)). ☐

So by the preceding result, the elements of the M-Kochen ring $R^M_{\gamma_p}(B)$ of B over the p-adically closed integral domain A have the following form:

$$a = \frac{b}{1+pd} \text{ with } b, d \in \mathbb{Z}[\gamma_p(Q(B)), M] \text{ and } 1 + pd \neq 0.$$

The fraction field of the M-Kochen ring $R^M_{\gamma_p}(B)$ is $Q(B)$ by Merckel's Lemma (see Appendix in [12]).

Theorem 3.8. *Suppose that p is not a unit in $\mathcal{O}_{Q(A)}[\gamma_p(Q(B)), M]$, in view of Theorem (3.4) this is equivalent to saying that $Q(B)$ is a p-valued field over $Q(A)$ such that $v_p(M) \geqslant 0$. Then*

1. *p is not a unit in $R^M_{\gamma_p}(B)$. Every maximal ideal of $R^M_{\gamma_p}(B)$ contains p and every prime ideal of $R^M_{\gamma_p}(B)$ containing p is maximal.*
2. *The p-valuations of $Q(B)$ over $Q(A)$ such that M belongs to the corresponding valuation ring can be characterized as being those valuations of $Q(B)$ which lie above $R^M_{\gamma_p}(B)$ and are centered at some maximal ideal of $R^M_{\gamma_p}(B)$.*

Proof. It is an easy adaptation of the proof of Theorem (6.8) in [12], it suffices to replace R by $R^M_{\gamma_p}(B)$ and to use the corresponding previous results. ☐

Definition 3.9. For any non empty set S of valuations of $Q(B)$, we denote by $\mathcal{O}_S$ the intersection of their valuation rings:

$$\mathcal{O}_S = \bigcap_{v \in S} \mathcal{O}_v \text{ where } \mathcal{O}_v \text{ is the valuation ring corresponding to } v.$$

$\mathcal{O}_S$ is called the holomorphy ring of S in $Q(B)$. Every such holomorphy ring is integrally closed in $Q(B)$.

Lemma 3.10. *Let P be a maximal ideal of the M-Kochen ring $R^M_{\gamma_p}(B)$ of B over A and let v be a valuation of $Q(B)$ lying above $R^M_{\gamma_p}(B)$ and centered at P. Then v is the only valuation of $Q(B)$ which lies over $R^M_{\gamma_p}(B)$ and is centered at P. Further, $R^M_{\gamma_p}(B)/P$ is the residue field of $Q(B)$ with respect to v and $\mathcal{O}_v = R^M_{\gamma_p}(B)_P$ where $R^M_{\gamma_p}(B)_P$ is the localization of the M-Kochen ring over B at the maximal ideal P.*

Proof. By the previous theorem, v is a p-valuation over $Q(A)$ such that $v(M) \geqslant 0$, the results are just now a transposition of Corollary (6.9), Lemma (6.10), Lemma (6.12) and Lemma (6.13) of [12]. $\square$

Theorem 3.11. *Under the hypothesis of Lemma (3.10), the subring $R^M_{\gamma_p}(B)$ of $Q(B)$ is the intersection of the valuation rings $\mathcal{O}_v$ where v ranges over the p-valuations of $Q(B)$ which extend the p-valuation of $Q(A)$ such that M belongs to $\mathcal{O}_v$.*

Now we define the notion of integral-definite polynomial over a p-convexly valued domain A and so, we can prove the following theorem, which provides a solution to the analogue Hilbert's seventeenth problem for p-adically closed integral rings.

Definition 3.12. Let A be a p-convexly valued domain and let $F(X_1, \cdots, X_n)$ be an element of $A[X_1, \cdots, X_n]$, the ring of polynomials in n indeterminates over A. Then F is called integral-definite on A if and only if for all $\bar{a} \in A^n$, we have $A \models \mathcal{D}_p(1, F(\bar{a}))$, i.e. $F(\bar{a})$ is in the range of γ_p on A.

From now on, we will denote the polynomial ring in n indeterminates over A by $A[\underline{X}]$ and its fraction field by $Q(A)(\underline{X})$.

Theorem 3.13. *Let A be a model of the $\mathcal{L}$-theory $pCIR$ and let F be an element of $A[\underline{X}]$. Then F is integral-definite on A if and only if F belongs to the M-Kochen ring $R^M_{\gamma_p}(A[\underline{X}])$ of $A[\underline{X}]$ over A where M is the ideal $\mathcal{M}_A \cdot A[\underline{X}]$ of $A[\underline{X}]$ and the elements of $R^M_{\gamma_p}(A[\underline{X}])$ have the following form:*

$$\frac{b}{1+pd} \text{ with } b, d \in \mathbb{Z}[\gamma(Q(A)), \mathcal{M}_A \cdot A[\underline{X}]] \text{ and } 1+pd \neq 0. \tag{2}$$

Proof. Let $\langle A, \mathcal{D}_p, \mathcal{D}\rangle \models pCIR$ and $F \in A[\underline{X}]$, where F is not of the form given by (2). By Theorem (3.11), there exists a p-valuation, denoted by v_p, on $Q(A)(\underline{X})$ which extends the p-valuation on the p-valued field $Q(A)$ such that $v_p(F) < 0$ and $v_p(m) > 0$ for all $m \in \mathcal{M}_A \cdot A[\underline{X}]$. We denote by A' the ring $A[\underline{X}]$. Let $B = pcH(A', Q(A'))$ (see Lemma (2.14)). Then, for every $a \in A'$ and for every $m \in \mathcal{M}_A$, we have $\mathcal{D}_p(m^{-1}, p{\cdot}a)$. Hence, B is not a field and by definition, B is a p-convexly valued domain (see Lemma (2.5)). By Lemma (2.9), $A \subseteq_{\mathcal{L}} B$. Let $\widetilde{B} = pcH(B, K)$ where K is a p-adic closure of $Q(B) = Q(A)(\underline{X})$. It is a model of $pCIR$ by Lemma (2.15). Since $pCIR$ is model-complete, we get that $A \prec \widetilde{B}$. Now $A \subseteq_{\mathcal{L}} \widetilde{B}$ and $\widetilde{B} \models \exists \bar{x}(\neg(\mathcal{D}_p(1, F(\bar{x}))))$. By model-completeness, $A \models \exists \bar{x}(\neg(\mathcal{D}_p(1, F(\bar{x}))))$. Hence F is not integral-definite on A, which contradicts our hypothesis. $\square$

Remark 3.14.
- In the previous proof, we have used the following fact: if A is a p-valued domain then $A[\underline{X}]$ can be considered as a p-valued domain; it

suffices to consider the natural p-valuation w_p of $Q(A)(\underline{X})$ which extends the p-valuation of $Q(A)$ (see Example (1.2) in [16]). Moreover we have $w_p(\mathcal{M}_A \cdot A[\underline{X}]) \geqslant 0$.

- In the previous proof, $A \subseteq_{\mathcal{L}} B$ is justified by the following statement of Lemma (2.9): $\mathcal{M}_B \cap A = \mathcal{M}_A$. Indeed, we get:
  - ($\subseteq$) is trivial.
  - ($\supseteq$): we know B satisfies $\mathcal{D}_p(m^{-1}, pa)$ for all $m \in \mathcal{M}_A$ and $a \in A[\underline{X}]$. By definition, it implies $m^{-1} \notin pcH(A', Q(A')) = B$ and the conclusion follows.

Now we prove an analogue of Theorem (3) in [1].

Theorem 3.15. *Let A be a model of the $\mathcal{L}$-theory pCIR and let $F_1, \cdots, F_r, G$ be in $A[\underline{X}]$. Then the following statements are equivalent:*

(1) $A \models \forall \bar{x} \, [\bigwedge_{i=1}^{r} \mathcal{D}_p(1, F_i(\bar{x})) \; \Rightarrow \; \mathcal{D}_p(1, G(\bar{x}))]$;

(2) *G belongs to the M-Kochen ring $R^{M}_{\gamma_p}(A[\underline{X}])$ of $A[\underline{X}]$ where M is the ideal of $A[\underline{X}]$ generated by $\mathcal{M}_A$ and the polynomials $F_1, \ldots, F_r$.*

Proof. The proof is similar to the one of Theorem (3.13). It suffices to modify the M of Theorem (3.13) such that M becomes (in this case) the ideal generated by $\mathcal{M}_A$ and the polynomials $F_1, \cdots, F_r$. □

4. Nullsetllensatz for p-adically closed integral rings

In this last section, we consider the question to establish a Nullstellensatz-type result for p-adically closed integral rings A, similar to the Nullstellensatz provided by Theorem (2) of [1]. To this effect, we introduce the notion of $\mathcal{M}_A$-radical of a polynomial ideal over A motivated by the notion of p-adic ideal as defined in [16, Definition (3.1)] thanks to which A. Srhir reproves the Nullstellensatz for p-adically closed fields.

In the sequel we denote by $R^{\mathcal{M}_A \cdot A[\underline{X}]}_{\gamma_p}(A[\underline{X}]) \cdot A[\underline{X}]$ the subring of $Q(A)(\underline{X})$ generated by $A[\underline{X}]$ and the $(\mathcal{M}_A \cdot A[\underline{X}])$-Kochen ring of $A[\underline{X}]$.

Definition 4.1. Let A be a p-convexly valued domain and let J be an ideal of the polynomial ring $A[\underline{X}]$ over A.

(1) The ideal J is called a p-adic ideal of $A[\underline{X}]$ if for any integer $s \geqslant 1$, for any elements $g_1, \cdots, g_s$ in J, any elements $\lambda_1, \cdots, \lambda_s$ of $R^{\mathcal{M}_A \cdot A[\underline{X}]}_{\gamma_p}(A[\underline{X}])$ and any $h \in A[\underline{X}]$ such that $h = \sum_{i=1}^{s} \lambda_i \cdot g_i$, we have $h \in J$.

(2) The $\mathcal{M}_A$-radical of an ideal J of $A[\underline{X}]$ is defined as the set of elements h of $A[\underline{X}]$ verifying the condition:

$$a^* h^l = \sum_{i=1}^{s} \lambda_i g_i$$

for some $a^* \in \mathcal{M}_A^{\bullet} \cup \{1\}$, some positive integers s, l, some elements $g_1, \cdots, g_s \in J$ and some elements $\lambda_1, \cdots, \lambda_s \in R^{\mathcal{M}_A \cdot A[\underline{X}]}_{\gamma_p}(A[\underline{X}])$.

We denote this set by $\sqrt[\mathcal{M}_A]{J}$.

Now we prove some properties of the $\mathcal{M}_A$-radical of an ideal J in $A[\underline{X}]$.

Lemma 4.2. *Let A be a p-convexly valued domain and let $\mathcal{M}_A$ be its maximal ideal. Let I be an ideal of $A[\underline{X}]$. Then we have the following properties:*

1. *$\sqrt[\mathcal{M}_A]{I}$ is an ideal containing I.*
2. *if J is an ideal containing I then $\sqrt[\mathcal{M}_A]{J}$ contains $\sqrt[\mathcal{M}_A]{I}$.*
3. *$\sqrt[\mathcal{M}_A]{\sqrt[\mathcal{M}_A]{I}} = \sqrt[\mathcal{M}_A]{I}$.*

Proof. Easy calculations. □

So the $\mathcal{M}_A$-radical of an ideal is also an ideal and we can define a notion of radical ideal.

Definition 4.3. We say that an ideal J of $A[\underline{X}]$ is $\mathcal{M}_A$-radical if $\sqrt[\mathcal{M}_A]{J} = J$.

So, if J is a $\mathcal{M}_A$-radical ideal containing an ideal I then we get $J \supseteq \sqrt[\mathcal{M}_A]{I}$. With this terminology, we prove the main result of this section.

Theorem 4.4. *Let A be a p-adically closed integral ring and let $f_1, \ldots, f_r, q$ be elements of $A[\underline{X}]$. Then q vanishes at every common zero of $f_1, \cdots, f_r$ in A^n if and only if there exists a positive integer l, an element a^* of $\mathcal{M}_A^\bullet \cup \{1\}$ and r elements $\lambda_1, \cdots, \lambda_r$ of the subring $R_{\gamma_p}^{M_A \cdot A[\underline{X}]}(A[\underline{X}]) \cdot A[\underline{X}]$ of $Q(A)(\underline{X})$ such that*

$$a^* \cdot q^l = \sum_{i=1}^{r} \lambda_i \cdot f_i; \tag{3}$$

i.e. q belongs to the $\mathcal{M}_A$-radical ideal of the ideal generated by $f_1, \cdots, f_r$ in $A[\underline{X}]$.

Proof. ($\Leftarrow$): This direction is a trivial consequence of the definition of the λ_i and Theorem (3.4) which asserts that in this case $\frac{1}{p} \notin \mathbb{Z}[\gamma_p(Q(A)), M]$ (the same kind of argument is given in more details in the proof of (5.5)).

($\Rightarrow$): We proceed ab absurdo. Suppose that there is no positive integer l and elements $a \in \mathcal{M}_A^\bullet \cup \{1\}$ so that $a \cdot q^l$ is of the form (3). Let S be the following multiplicative subset of $A[\underline{X}]$: $\{aq^l \mid l \in \mathbb{N}^\bullet,\ a \in (\mathcal{M}_A^\bullet) \cup \{1\}\}$. Let I be the ideal of $A[\underline{X}]$ generated by the polynomials $f_1, \cdots, f_r$. We can suppose $I \cap A = (0)$, otherwise $I = (1)$ or $I \cap \mathcal{M}_A \neq \emptyset$ and $aq \in I$ for some $a \in \mathcal{M}_A^\bullet$, and in both cases the theorem is proved. Let us consider the following set $\mathcal{J}$ of ideals of $A[\underline{X}]$

$$\mathcal{J} = \{I' \text{ proper } \mathcal{M}_A\text{-radical ideal of } A[\underline{X}] \text{ containing } I \text{ and disjoint from } S\}.$$

Since q does not satisfy the equation (3) and $\sqrt[\mathcal{M}_A]{I}$ is proper (otherwise the theorem is trivially satisfied), $\mathcal{J}$ is a non-empty set. By Zorn's Lemma, the set $\mathcal{J}$ contains a maximal element denoted by J. So J is a proper $\mathcal{M}_A$-radical ideal of $A[\underline{X}]$ containing I. Let us show that J is a prime ideal of $A[\underline{X}]$. So we assume that $f \cdot h \in J$ for some $f, h \in A[\underline{X}] \setminus J$. By maximality of the element J in $\mathcal{J}$, we get that $\sqrt[\mathcal{M}_A]{\langle f, J\rangle} \cap S \neq \emptyset$

and ${}^{\mathcal{M}_A}\!\sqrt{\langle h, J\rangle} \cap S \neq \emptyset$. So we have that

$$\begin{aligned} a_1 \cdot q^{k_1} &= \lambda \cdot f + \sum_{i=1}^{n_1} \lambda_i \cdot g_i \\ a_2 \cdot q^{k_2} &= \lambda' \cdot h + \sum_{j=1}^{n_2} \lambda'_j \cdot g'_j \end{aligned}$$

for some $a_1, a_2 \in \mathcal{M}_A^\bullet \cup \{1\}$, $g_i, g'_j \in J$, λ, λ', $\lambda_i, \lambda'_j \in R_{\gamma_p}^{M_A \cdot A[\underline{X}]}(A[\underline{X}])$ and some positive integers k_1, k_2, n_1, n_2.

Hence we obtain

$$a_1 \cdot a_2 \cdot q^{k_1+k_2} = \lambda \cdot \lambda' \cdot (fh) + \sum_{i=1}^{N} {\lambda^*}_i \cdot g^*_i$$

for some $g^*_i \in J$, $\lambda^*_i \in R_{\gamma_p}^{M_A \cdot A[\underline{X}]}(A[\underline{X}])$ and some positive integer N. Since $g^*_i \in J$ and J is a $\mathcal{M}_A$-radical ideal of $A[\underline{X}]$, we get that $S \cap J \neq \emptyset$, this is a contradiction. So $A[\underline{X}]/J$ is a domain which is not a field and we are going to show that we can extend the p-valuation of $Q(A)$ to a p-valuation, denoted by v_p, of $Q(A[\underline{X}]/J)$ such that $v_p(\mathcal{M}_A \cdot A[\underline{X}]/J) \geqslant 0$. Let us denote $Q(A[\underline{X}]/J)$ by $Q(A)(J)$. As in the proof of (3.8), it is sufficient to show that $\frac{1}{p} \notin R_{\gamma_p}^{\mathcal{M}_A \cdot A[\underline{X}]/J}(A[\underline{X}]/J)$. We know $A \hookrightarrow_{\mathcal{L}_{\text{rings}}} A[\underline{X}]/J$. Let us denote by $\bar{\cdot}$ the residue map : $A[\underline{X}] \longmapsto A[\underline{X}]/J$. Suppose $\frac{1}{p} \in R_{\gamma_p}^{\mathcal{M}_A \cdot A[\underline{X}]/J}(A[\underline{X}]/J)$, i.e. there exists $\frac{\bar{f}}{\bar{g}}$, $\frac{\bar{h}}{\bar{l}} \in \mathbb{Z}[\gamma_p(Q(A)(J)), \mathcal{M}_A \cdot A[\underline{X}]/J]$ such that

$$\frac{1}{p} = \frac{\frac{\bar{f}}{\bar{g}}}{1 + p \cdot \frac{\bar{h}}{\bar{l}}} \text{ for some elements } f, g, h, l \in Q(A)(\underline{X}).$$

So, $\frac{f}{g}$ and $\frac{h}{l}$ can be chosen such that $\frac{f}{g}$, $\frac{h}{l} \in \mathbb{Z}[\gamma_p(Q(A)(\underline{X})), \mathcal{M}_A \cdot A[\underline{X}]]$ and we obtain the equality

$$\overline{gl + p \cdot (gh - fl)} = 0.$$

This implies $gl + p \cdot (gh - fl) \in J$. We know that $Q(A)(\underline{X})$ is formally p-adic over $Q(A)$ with respect to $\mathcal{M}_A \cdot A[\underline{X}]$ (i.e. we can extend the p-valuation of $Q(A)$ to a p-valuation v_p of $Q(A)(\underline{X})$ such that $v_p(\mathcal{M}_A \cdot A[\underline{X}]) \geqslant 0$). Hence $1 + p \cdot (\frac{h}{l} - \frac{f}{g}) \neq 0$. So, we can write

$$gl = \frac{1}{1 + p \cdot (\frac{h}{l} - \frac{f}{g})} \cdot j \text{ where } j \in J.$$

We have that $\lambda = \frac{1}{1+p\cdot(\frac{h}{l} - \frac{f}{g})} \in R_{\gamma_p}^{\mathcal{M}_A \cdot A[\underline{X}]}(A[\underline{X}])$. Hence $g \cdot l = \lambda \cdot j$. Since J is a p-adic ideal (because J is a $\mathcal{M}_A$-radical ideal), we have $g \cdot l \in J$. But J is prime and so, $g \in J$ or $l \in J$ which gives a contradiction. So, we have a p-valuation v_p on $A[\underline{X}]/J$ which extends the p-valuation on A such that $v_p(\mathcal{M}_A \cdot A[\underline{X}]/J) > 0$. Up to now we have built a p-valued domain $A[\underline{X}]/J$ which is a p-valued extension of A. Moreover it contains a common zero of $f_1, \cdots, f_r$ which is not a zero of q. We repeat the same proof as for Theorem (3.13) by building a p-adically closed integral ring extending $A[\underline{X}]/J$. We have the final contradiction by model-completness of $pCIR$. □

5. Model-theoretic radical ideal

Throughout this section, A will stand for an arbitrary model of $pCIR$. All embeddings of rings extending A will be A-embeddings, i.e. embeddings leaving A pointwise fixed.

The $pCIR$-radical of an ideal $I \subseteq A[\underline{X}]$ is defined as follows:

$$pCIR - rad(I) = \bigcap \{J | J \text{ is an ideal of } A[\underline{X}],\ I \subseteq J,\ J \cap A = \{0\} \text{ and } A[\underline{X}]/J \text{ is } A\text{-embeddable in a model } B \text{ of the } \mathcal{L}\text{-theory } pCIR\}.$$

Remark 5.1. An ideal J satisfying the requirements of the preceding definition is necessarily prime since $A[\underline{X}]/J \subseteq B$ and B is an integral domain. Moreover, if J is prime, $J \cap A = \{0\}$ is equivalent to the following condition: for every $Q \in A[\underline{X}]$ and $b \in \mathcal{M}_A$, $b \neq 0$, we have: $bQ \in J \Rightarrow Q \in J$.

In the sequel, for any set I of polynomials in $A[\underline{X}]$, we denote by $V_A(I)$ the set of elements of A^n which are common zeroes of I.

Proposition 5.2. *For a finitely generated ideal $I \subseteq A[\underline{X}]$ and $P \in A[\underline{X}]$, the following are equivalent:*

- $V_A(I) \subseteq V_A(P)$;
- $P \in pCIR - rad(I)$.

Proof. It is an easy transposition of Proposition (2.2) in [7] using the model-completeness of the $\mathcal{L}$-theory $pCIR$. □

Now we study more closely the condition:

$$(*) \quad A[\underline{X}]/J \text{ is } A\text{-embeddable in a model } B \text{ of } pCIR \text{ such that } A \prec_{\mathcal{L}} B, \text{ where } J \supseteq I,\ J \cap A = \{0\}.$$

Proposition 5.3. *Condition (*) is equivalent to*

(**) *$A[\underline{X}]/J$ admits a p-divisibility relation $\mathcal{D}_p$ which extends the p-divisibility relation of A and such that $\mathcal{D}_p(1, aP/J)$ for all $a \in \mathcal{M}_A$, $P \in A[\underline{X}]$.*

Proof. (*)⇒(**): Let $C = A[\underline{X}]/J$. If $B \models pCIR$, $C \subseteq_{\mathcal{L}} B$, $A \prec_{\mathcal{L}} B$, then, in the p-divisibility relation that B induces on C, we have $\mathcal{D}_p(1, aP/J)$ since this holds for all $x \in \mathcal{M}_B$ and $a \in \mathcal{M}_A \subseteq \mathcal{M}_B$ implies $aP/J \in \mathcal{M}_B$.

(**)⇒(*): Endow C with a p-divisibility relation $\mathcal{D}_p$ as in (**). Let K be the fraction field of C endowed with the p-valuation induced by the p-divisibility of C. Let $\widetilde{K}$ be a p-adic closure of K and let $\widetilde{B} = pcH(B, \widetilde{K})$. As in the proof of Theorem (3.13), we conclude that $\widetilde{B} \models pCIR$ and so, $A \prec_{\mathcal{L}} \widetilde{B}$. □

Now we give an algebraic characterization of the $pCIR$-radical of an ideal I of the integral domain $A[\underline{X}]$ where A is a model of $pCIR$. In particular we get

Proposition 5.4. *For a finitely generated ideal $I \subseteq A[\underline{X}]$, the following equality holds:*

$$pCIR - rad(I) = \sqrt[\mathcal{M}_A]{I}.$$

Proof. By Theorem (4.4) and Proposition (5.2), we obtain our requirement. ☐

Proposition 5.5. *If $I \subseteq A[\underline{X}]$ is a $\mathcal{M}_A$-radical then $I = pCIR - rad(I)$.*

Proof. If I is finitely generated then the result is trivial by using the definition of $\mathcal{M}_A$-radical ideal and Proposition (5.4). In the general case, Proposition (5.3) and Remark (5.1) prove that $pCIR - rad(I)$ is the intersection of all prime ideals J containing I such that $J \cap A = \{0\}$ and $A[\underline{X}]/J$ admits a p-divisibility relation $\mathcal{D}_p$ such that $\mathcal{D}_p(1, \mathcal{M}_A \cdot A[\underline{X}]/J)$. If $A[\underline{X}]/J$ admits a p-divisibility relation $\mathcal{D}_p$ such that $\mathcal{D}_p(1, \mathcal{M}_A \cdot A[\underline{X}]/J)$ where $J \cap A = \{0\}$ and J is a proper prime ideal containing I then J is a $\mathcal{M}_A$-radical ideal. Indeed, assume that we have the following equation

$$a^* \cdot F = \sum_{i=1}^{n} \lambda_i \cdot j_i \tag{4}$$

where $j_i \in J$, $a^* \in \mathcal{M}_A^\bullet \cup \{1\}$, $\lambda_i \in R_{\gamma_p}^{\mathcal{M}_A \cdot A[\underline{X}]}(A[\underline{X}])$, $F \in A[\underline{X}] \setminus J$ and n is a positive integer.

In $Q(A)(J)$, we can consider the equation (4) because the λ_i's have the form $\frac{a_i}{1+p \cdot b_i}$ where a_i, b_i are elements of $\mathbb{Z}[\gamma_p(Q(A)(\underline{X})), \mathcal{M}_A \cdot A[\underline{X}]]$ and $1 + p \cdot b_i$ is different from zero modulo J by Theorem (3.4) (since $A[\underline{X}]/J$ admits a p-divisibility relation with the required properties). So we get that $a^* \cdot F \equiv 0 \bmod J$ in $A[\underline{X}]/J$ and $J \cap A = \{0\}$ implies that $F \equiv 0 \bmod J$. So $pCIR - rad(I)$ is a $\mathcal{M}_A$-radical containing I and thus $I = \sqrt[\mathcal{M}_A]{I} \subseteq pCIR - rad(I)$. Let us assume that $P \notin \sqrt[\mathcal{M}_A]{I}$. We have to show that there exists a proper prime ideal J of $A[\underline{X}]$ such that $A \cap J = \{0\}$, $J \not\ni P$ and $A[\underline{X}]/J$ admits a p-divisibility relation $\mathcal{D}_p$ so that we have $\mathcal{D}_p(1, \mathcal{M}_A \cdot A[\underline{X}]/J)$. To this effect we proceed as in the first step of the proof of Theorem (4.4). ☐

6. ACKNOWLEDGMENT

This work is part of the current Ph. D. thesis project of the author under the supervision of F. Point and C. Michaux. I thank the referee for detailed and constructive suggestions for improvements of the paper.

REFERENCES

[1] Becker T., Real closed rings and ordered valuation rings, Z. Math. Logik Grundlag. Math. 29 (1983), no. 5, pp. 417–425.

[2] Bélair L., Substructures and uniform elimination for p-adic fields, Annals of Pure and Applied Logic 39 (1988), pp. 1–17.

[3] Bélair L., Anneaux p-adiquement clos et anneaux de fonctions continues, Journal of Symbolic Logic 56 (1991), no. 2, pp. 539–553.

[4] Bélair L., Anneaux de fonctions p-adiques, Journal of Symbolic Logic 60 (1995), no. 2, pp. 484–497.

[5] Cherlin G., Dickmann M., Real closed rings. II. Model theory. Annals of Pure and Applied Logic 25 (1983), no. 3, pp. 213–231.

[6] Dickmann M., Quantifier elimination for ordered valuation rings, Journal of Symbolic Logic 52 (1987), no. 1, pp. 116-128.

[7] Dickmann M., On polynomials over real closed rings, *Model theory of algebra and arithmetic* (Proc.Conf., Karpacz, 1979), Lecture Notes in Mathematics 834, Springer, Berlin-New-York, 1980, pp. 117–135.

[8] Haskell D., MacPherson D., A version of o-minimality for the p-adics, Journal of Symbolic Logic 62 (1997), no. 4, pp. 1075–1092.
[9] Macintyre A., On definable subsets of p-adic fields, Journal of Symbolic Logic 41 (1976), no. 3, pp. 605–610.
[10] Mathews L., Cell decomposition and dimension functions in first-order topological structures, Proceedings of the London Mathematical Society (3) 70, 1995, no. 1, pp. 1–32.
[11] Pillay A., First-order topological structures and theories, Journal of Symbolic Logic 52 (1987), pp. 763–778.
[12] Prestel A., Roquette R., *Formally p-adic fields*, Lecture Notes in Mathematics 1050, 1984.
[13] Ribenboim P., Théorie des valuations, Les presses de l'Universitde Montréal, 1969.
[14] Ribenboim P., Equivalent forms of Hensel's lemma, Expositiones Mathematicae 3 (1985), pp. 3–24.
[15] Ribenboim P., The theory of classical valuations, Springer monographs in mathematics, Springer, 1999.
[16] Srhir A., p-adic ideals of p-rank d and the p-adic Nullstellensatz, Journal of Pure and Applied Algebra 180 (2003), pp. 299-311.
[17] van den Dries L., Algebraic theories with definable Skolem functions, Journal of Symbolic Logic 49 (1984), pp. 625–629.

Nicolas Guzy, Institut de Mathématique et Informatique, Université de Mons-Hainaut, Le Pentagone, 6, avenue du Champ de Mars, B-7000 Mons, Belgium
E-mail address: `Nicolas.Guzy@umh.ac.be`