On the $p$-adic Algebra and its Applications

Azzeddine Fekak

École Royale Navale, Boulevard Sour Jdid, Casablanca, Maroc
fekak.azed@hotmail.com

Ahmed Srhir

Département de Mathématiques, Faculté Polydisciplinaire
B.P. 4162, Safi, Maroc
ahmedsrhir@hotmail.com

Abstract

In this paper we introduce and study the notion of $p$-adic ring by a complete analogy of that of real ring (see [6]). Then, using this new notion we generalize the concept of $p$-adic ideal and that of $p$-adic radical of an ideal (see [17]) to any commutative ring with unit. Afterwards, we illustrate those notions by giving a new characterization of the $p$-adic spectrum of a ring. Finally, we state and prove an abstract Nullstellensatz of this spectrum.

Mathematics Subject Classification: 12J12, 14P10, 03C10, 13F20

Keywords: $p$-adic closed field, $p$-adic ideal, $p$-adic spectrum

0 Introduction

It is well-known that the real number field $\mathbb{R}$ is the completion of the rational number field $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$ defined by

$$ |x| = \begin{cases} 
  x & \text{if } 0 \leq x \\
  -x & \text{if } x \leq 0.
\end{cases} $$

Let $p$ be a fixed prime number from $\mathbb{N}$. Let us recall that the $p$-adic valuation of a nonzero rational $x$ is the unique integer $v_p(x) \in \mathbb{Z}$ given by

$$ x = \frac{n}{m} \cdot p^{v_p(x)}, \quad \text{where } n \in \mathbb{N}^* \text{ and } m \in \mathbb{Z}^* \text{ are prime to } p. $$
The $p$-adic absolute value $|\cdot|_p$ over $\mathbb{Q}$ is defined by

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

According to Ostrowski’s theorem (c.f. [10]) every non trivial absolute value over $\mathbb{Q}$ is equivalent to the usual absolute value or to one $p$-adic absolute value. This classical result was enabled Hensel to introduce the $p$-adic number field $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the $p$-adic absolute value. This precise resemblance between the construction of $\mathbb{R}$ and $\mathbb{Q}_p$ was motivated many mathematicians to translate known results and proofs from the real case to the $p$-adic one. However, the process of this transposition is nontrivial; although the deep structure of proofs may remain the same, the details are often different. For instance, the notion of a $p$-adically closed field was introduced by Kochen [11] as the $p$-adic counterpart of that of real closed field; and the $p$-adic spectrum of a ring was introduced by Robinson [16] to give a $p$-adic analogue of the real spectrum of a ring of Coste-Roy [7].

In the same way, we are interested here in $p$-adic algebra. More precisely, we will introduce a notion which will play a similar role in the $p$-adic case as the notion of real ring does in the real case. Let us first recall the definition of the latter notion (see also [6]):

**Definition 0.1** Let $A$ be an integral domain. We say that $A$ is a real ring if the quotient field of $A$ is formally real field.

The concept of real ring provides in real algebraic and analytic geometry an appropriate framework to describe and formulate many situations with a very concise way. We refer the reader to [6] for elementary properties of this notion and its applications in real geometry. The work in this paper has been motivated by the strong analogy between the real case and the $p$-adic case, and also by the lack of a Nullstellensatz for the ring of formal and convergent power series over the $p$-adic number field $\mathbb{Q}_p$. Our approach is inspired by [6], where Colliot-Thelene has used similar methods and arguments to deal with the real case. Finally, we note that all the notions and results given here can be extended to the class of $p$-adically closed fields of some $p$-rank.

The contents of this paper are organized as follows. In section 1 we recall briefly some basic facts about $p$-adic algebra and model theory of $p$-adically closed fields used later. In section 2 we introduce the notion of $p$-adic ring by analogy of the real case; and then we use this new notion to generalize the notion $p$-adic ideal and that of $p$-adic radical of an ideal to any commutative ring with unit. Section 3 is devoted to the $p$-adic spectrum; first we recall briefly the construction of the $p$-adic spectrum and then we provide a new characterization of the $p$-adic spectrum of a ring. Finally, in section 4 we give a
Nullstellensatz for the $p$-adic spectrum of a ring; and we state some conjectures concerning the Nullstellensatz for the rings of formal and convergent power series over the $p$-adic number field $\mathbb{Q}_p$.

1 Preliminaries and notations

Let us first fix some notations and terminologies. Throughout this paper, a ring means a commutative ring with unit. We shall write $x := (x_1, \ldots, x_m)$, where $m \in \mathbb{N}^*$. For an ideal $I$ of a ring $A$, we will denote by $\sqrt{I}$ the radical of $I$, that is,

$$\sqrt{I} = \{x \in A \mid \exists r \in \mathbb{N}^* \text{ such that } x^r \in I\}.$$ 

If in addition $I$ is a prime ideal of $A$, $k(I)$ will denote the residue field of $I$, that is, the quotient field of the integral domain $A/I$. For each integer $n \in \mathbb{N}^*$, we will denote by $P_n$ the unary predicate defined by

$$\forall x, \ (P_n(x) \iff \exists y : x = y^n).$$

Now let $K$ be a field. We will denote by $K^{(n)}$ the subset of $n$-th powers in $K$, that is,

$$K^{(n)} = \{x \in K \mid P_n(x) \text{ holds in } K\}.$$ 

We denote by $K[X] = K[X_1, \ldots, X_m]$ the ring of polynomials in indeterminates $X_1, \ldots, X_m$ over $K$, and by $K(X)$ the quotient field of $K[X]$.

Let $v$ be a valuation of $K$. We denote by $V_K$ the valuation ring of $K$ associated to $v$, that is,

$$V_K = \{x \in K \mid v(x) \geq 0\},$$

and by $\mathcal{M}_K$ the unique maximal ideal of $V_K$ defined by

$$\mathcal{M}_K = \{x \in K \mid v(x) > 0\}.$$ 

We let $K_v = V_K/\mathcal{M}_K$ to denote the residue field of $V_K$. Let us recall that a valuation $v$ is called $p$-valuation if $v$ satisfies the following conditions:

- $v(p) = \min \{v(x) > 0 \mid x \in K \setminus \{0\}\}$
- $K_v \simeq \mathbb{Z}/p\mathbb{Z}$.

Note that what we call here $p$-valuation is a $p$-valuation of $p$-rank 1 in the sense of [14]. A field of characteristic 0 together with a $p$-valuation is called $p$-valued field. For example, $\mathbb{Q}_p$ and $\mathbb{Q}$ with their $p$-adic valuations are both $p$-valued fields. Let $K$ be a $p$-valued field, and $L$ a valued extension field of $K$. The $p$-adic Kochen operator of $L$ over $K$ is defined by

$$\gamma(X) = \frac{1}{p} \cdot \frac{X^p - X}{(X^p - X)^2 - 1}.$$
We denote by $V_K[\gamma(L)]$ the subring of $L$ generated by $\gamma(L) \cup V_K$. The $p$-adic Kochen ring of $L$ over $K$ is the subring of $L$ defined by

$$\Lambda_L = \left\{ \frac{t}{1 - ps} \middle| t, s \in V_K[\gamma(L)] \text{ and } 1 - ps \neq 0 \right\}.$$ 

If $L = K(X)$, we will denote $\Lambda_{K(X)}$ by $\Lambda$. We shall denote by $K[X, \gamma(K(X))]$ the subring of $K(X)$ generated by $(X_1, \ldots, X_m)$ and $\gamma(K(X))$ over $K$. Finally, we denote by $\Lambda \cdot K[X]$ the subring of $K(X)$ generated by $\Lambda$ and $K[X]$. Then it is easy to see that

$$\Lambda \cdot K[X] = \left\{ \frac{t}{1 - ps} \middle| t \in K[X, \gamma(K(X))] \text{ and } s \in V_K[\gamma(K(X))] \right\}.$$ 

Let us recall that the valued field $L$ is called formally $p$-adic field over $K$ if $L$ admits a $p$-valuation extending the given $p$-valuation of $K$. If $K = \mathbb{Q}_p$, we say formally $p$-adic field instead of formally $p$-adic field over $\mathbb{Q}_p$. Formally $p$-adic fields are also characterized by

**Proposition 1.1** (c.f. [14]) Let $K$ be a $p$-valued field, and $L$ a valued extension field of $K$. Then $L$ is a formally $p$-adic field over $K$ if and only if $\frac{1}{p} \notin V_K[\gamma(L)]$.

**Example 1.2** Let $K$ be a $p$-valued field. The rational function field $K(X)$ is formally $p$-adic over $K$.

Let $P \in K[X]$ be a polynomial such that

$$P = a_kX^k + a_{k+1}X^{k+1} + \cdots + a_mX^m,$$

with $a_k \neq 0$ and $k \leq m$.

We put $w_0(P) = (k, v(a_k))$, where $v$ denotes the given $p$-valuation of $K$. Now if $f/g$ is an element of $K(X)$, we put

$$w \left( \frac{f}{g} \right) = w_0(f) - w_0(g).$$

Then $w$ is a $p$-valuation of $K(X)$ extending the $p$-valuation $v$.

Let us recall briefly that a $p$-valued field $L$ is called $p$-adically closed if $L$ does not admit any proper $p$-valued algebraic extension. Note that $p$-adically closed fields play the same role in the $p$-adic case as real closed fields do in the real case. The $p$-adic closure of a $p$-valued field is a $p$-adically closed algebraic extension of this $p$-valued field.

We will need later some facts from model theory of $p$-adically closed fields. For the convenience of the reader we will discuss those facts here. We will
denote by $\mathcal{L} = (+, -, \times, 0, 1)$ the first order language of rings. A first order formula in the language $\mathcal{L}$ with parameters in a ring $A$ is obtained by taking a finite number of conjunctions, disjunctions, negations and existential or universal quantifiers over variables from atomic formulas of type $f(x) = 0$, where $f$ is polynomial from $A[X]$.

If $A = \mathbb{Z}$, we simply say a first order formula in $\mathcal{L}$. A first order sentence in the language $\mathcal{L}$ is a formula without any free (i.e. non quantified) variables. We will denote by $\text{Th}(\mathbb{Q}_p)$ the set of all first order sentences in $\mathcal{L}$ which are true in $\mathbb{Q}_p$. We refer the reader to [14] for more details about model theory of $p$-adically closed fields. The following result states that the theory of $p$-adically closed fields is model complete in the language $\mathcal{L}$:

**Theorem 1.3 (c.f. [14])** Let $K$ and $L$ be two $p$-adically closed fields such that $K \subset L$. Let $\varphi$ be a first order formula in $\mathcal{L}$. Then $\varphi$ holds in $L$ if and only if $\varphi$ holds in $K$.

In particular, a formula holds in a $p$-adically closed field $K$ if and only if it holds in $\mathbb{Q}_p$. For this reason, we will denote $K \models \text{Th}(\mathbb{Q}_p)$. Let us recall that two $p$-adically closed extension fields of a $p$-valued field $K$ are called elementary equivalent over $K$ if a formula (with parameters in $K$) holds in $L$ if and only if it holds in $M$. From Theorem 1.3, we deduce the following result:

**Corollary 1.4** Let $K$ be a $p$-valued field. Let $L$ and $M$ be $p$-adically closed extension fields of $K$. Then $L$ and $M$ are elementary equivalent over $K$ if and only if $K \cap L^{(n)} = K \cap M^{(n)}$ for all $n \geq 1$.

The following result is an other consequence of theorem 1.3 which may be considered as Artin-Lang’s homomorphism theorem in the real case:

**Corollary 1.5 (c.f. [17])** Let $K$ and $L$ be two $p$-adically closed fields such that $K \subset L$, and let $I$ be an ideal of $K[X]$. If $\Phi : K[X]/I \longrightarrow L$ is a $K$-homomorphism then there exists a $K$-homomorphism $\Psi : K[X]/I \longrightarrow K$.

The other notion from model theory used here is that of elimination of quantifiers. The theory $\text{Th}(\mathbb{Q}_p)$ does not admit elimination of quantifiers in the language $\mathcal{L}$. But if we consider the extending language $\mathcal{L}(P_\omega)$ of $\mathcal{L}$ given by

$\mathcal{L}(P_\omega) = (+, -, \times, 0, 1, (P_n)_{n \geq 1})$,

and we define a first order formula in $\mathcal{L}(P_\omega)$ with parameters in a ring $A$ as obtained by taking a finite number of conjunctions, disjunctions, negations

On the $p$-adic algebra and its applications
and existential or universal quantifiers over variables from atomic formulas of type
\[ f(x) = 0 \text{ and } P_n(g(x)), \quad \text{with } f, g \in A[X]. \]

Then Macintyre [12] has showed that \( \text{Th}(\mathbb{Q}_p) \) admits elimination of quantifiers in the language \( \mathcal{L}(\mathcal{P}_\omega) \). More precisely, we have the following result:

**Theorem 1.6 (Macintyre’s theorem [12])** Let \( K \) be a \( p \)-adically closed field and \( \Phi \) a first order formula in \( \mathcal{L}(\mathcal{P}_\omega) \). Then there exists a quantifier free formula \( \Psi \) in \( \mathcal{L}(\mathcal{P}_\omega) \) such that \( \Phi \) holds in \( K \) if and only if \( \Psi \) holds in \( K \).

Macintyre’s theorem is the \( p \)-adic analogue of the well-known Tarski-Seidenberg’s theorem in the real case, which states that the theory of real closed fields admits elimination of quantifiers in the first order language of ordered fields.

## 2 \( p \)-adic ring and generalization of \( p \)-adic ideals

In this section, we will introduce the notion of \( p \)-adic ring; and we establish some elementary properties of this notion. Using this new notion we are able to generalize the notion of \( p \)-adic ideal and that of \( p \)-adic radical of an ideal to any ring. Throughout this section, unless otherwise specified, \( K \) will denote a fixed \( p \)-adically closed field. We are inspired by Definition 0.1 to introduce:

**Definition 2.1** Let \( A \) be an integral domain. We say that \( A \) is a \( p \)-adic ring if the quotient field of \( A \) is formally \( p \)-adic field.

**Remark 2.2** A field \( A \) is \( p \)-adic ring if and only if \( A \) is formally \( p \)-adic field.

**Examples.** 1) The ring \( K[X] \) of polynomials over \( K \) is a \( p \)-adic ring.
2) The ring \( K[[X]] \) of formal power series over \( K \) is a \( p \)-adic ring.
3) The ring \( \mathbb{Q}_p\{X\} \) of convergent power series over \( \mathbb{Q}_p \) is a \( p \)-adic ring.

In [17] we have introduced the notion of \( p \)-adic ideal by analogy with the real case but for the rings of polynomials over \( p \)-adically closed fields. Let us recall here the definition of this notion:

**Definition 2.3** Let \( I \) be an ideal of \( K[X] \) generated by \( f_1, \ldots, f_r \). We call that \( I \) is \( p \)-adic ideal if for all \( g \in K[X] \), \( m \in \mathbb{N}^* \) and \( \lambda_1, \ldots, \lambda_r \in \Lambda \cdot K[X] \) such that \( g^m = \lambda_1 f_1 + \cdots + \lambda_r f_r \) then \( g \in I \).

Using the notion of \( p \)-adic ring, we have also the following characterization of \( p \)-adic prime ideals:

**Proposition 2.4** A prime ideal \( I \) of \( K[X] \) is a \( p \)-adic ideal if and only if \( K[X]/I \) is a \( p \)-adic ring.
**Proof.** Let \(I\) be a \(p\)-adic prime ideal of \(K[X]\). According to Proposition 3.6 of [17], the residue field \(k(I)\) of \(I\) is formally \(p\)-adic field. Thus the integral domain \(K[X]/I\) is a \(p\)-adic ring.

Inversely, assume that the integral domain \(K[X]/I\) is \(p\)-adic ring. Therefore the residue field \(k(I)\) of \(I\) is formally \(p\)-adic field. Then by Proposition 3.6 of [17], the ideal \(I\) is a \(p\)-adic ideal. \(\square\)

This latter proposition and the strong ressemblance between the real case and the \(p\)-adic one suggest us to generalize the notion of \(p\)-adic ideal of an arbitrary ring in the following way:

**Definition 2.5** Let \(A\) be a ring. A prime ideal \(I\) of \(A\) is called a \(p\)-adic ideal if the integral domain \(A/I\) is a \(p\)-adic ring.

**Examples.** 1) Let \((X_1, \ldots, X_i)\) be the ideal of \(K[X]\) generated by \(X_1, \ldots, X_i\) for \(1 \leq i \leq m\). Since

\[K[X]/(X_1, \ldots, X_i) \simeq K[X_{i+1}, \ldots, X_m].\]

We deduce that \((X_1, \ldots, X_i)\) is a \(p\)-adic ideal of \(K[X]\).

2) Let \((X_1, \ldots, X_m)\) be the ideal of the ring of formal power series \(K[[X]]\) generated by \(X_1, \ldots, X_m\). Since

\[K[[X_1, \ldots, X_m]]/(X_1, \ldots, X_m) \simeq K.\]

Then \((X_1, \ldots, X_m)\) is a \(p\)-adic ideal of \(K[[X]]\).

3) Let \((X_1, \ldots, X_m)\) be the prime ideal of the ring of convergent power series \(Q_p\{X\}\) generated by \(X_1, \ldots, X_m\). Since

\[Q_p\{X_1, \ldots, X_m\}/(X_1, \ldots, X_m) \simeq Q_p.\]

Then \((X_1, \ldots, X_m)\) is a \(p\)-adic ideal of \(Q_p\{X\}\).

The notion of \(p\)-adic radical of an ideal was introduced in [17] but only for rings of polynomials over \(p\)-adically closed fields. Now we are able to generalize this notion for an arbitrary ring:

**Definition 2.6** Let \(A\) be a ring and \(I\) an ideal of \(A\). The \(p\)-adic radical of \(I\), denoted by \(\sqrt[n]{I}\), is the subset of \(A\) defined by

\[\sqrt[n]{I} = \bigcap \{\mathcal{I} \mid \mathcal{I} \text{ is a } p\text{-adic prime ideal of } A \text{ such that } I \subset \mathcal{I}\}.

**Proposition 2.7** Let \(I\) and \(J\) be two ideals of a ring \(A\). Then we have:

i) \(I \subset \sqrt[n]{I}\).
ii) $\sqrt{I} \subset \mathfrak{p} I$.

iii) $I \subset J \implies \sqrt{I} \subset \mathfrak{p} J$.

**Proof.** i) It is clear that $I \subset \sqrt{I}$.

ii) Let $x \in \sqrt{I}$. There is $n \in \mathbb{N}^*$ such that $x^n \in I$. If $\mathcal{I}$ is a $p$-adic prime ideal of $A$ such that $I \subset \mathcal{I}$, then $x^n \in \mathcal{I}$. Since $\mathcal{I}$ is a prime ideal, we have $x \in \mathcal{I}$. It follows that $x \in \sqrt{\mathcal{I}}$. Hence $\sqrt{I} \subset \sqrt{\mathcal{I}}$.

iii) Assume that $I \subset J$. Let $x \in \sqrt{\mathcal{I}}$. If $\mathcal{J}$ is a $p$-adic prime ideal of $A$ such that $J \subset \mathcal{J}$. Then we have $I \subset \mathcal{J}$. It follows that $x \in \mathcal{J}$. Hence $x \in \sqrt{\mathcal{J}}$. □

**Definition 2.8** Let $A$ be a ring and $I$ an ideal of $A$. We say that $I$ is a $p$-adic ideal if $I = \sqrt{\mathfrak{p} I}$.

**Remark 2.9** Let $A$ be a ring and $I$ an ideal of $A$. If $I$ is a $p$-adic ideal then we have $I = \sqrt{\mathfrak{p} I}$.

**Theorem 2.10** Let $A$ be a ring and $I$ an ideal of $A$. Then the $p$-adic radical $\sqrt{\mathcal{I}}$ of $I$ is the smallest $p$-adic ideal of $A$ containing $I$.

**Proof.** By definition $\sqrt{\mathcal{I}}$ is an ideal of $A$. We have to show that $\sqrt{\mathcal{I}} = \sqrt{\sqrt{\mathfrak{p} I}}$.

From Proposition 2.7 we deduce that $\sqrt{I} \subset \sqrt{\sqrt{\mathfrak{p} I}}$. Let $x \in \sqrt{\sqrt{\mathfrak{p} I}}$. Let $\mathcal{I}$ be a $p$-adic prime ideal of $A$ such that $I \subset \mathcal{I}$. Since $\mathcal{I}$ is a $p$-adic ideal of $A$, we have $\sqrt{\mathcal{I}} \subset \mathcal{I}$. Therefore $x \in \mathcal{I}$. Thus $x \in \sqrt{\mathcal{I}}$. It follows that $\sqrt{\mathcal{I}}$ is a $p$-adic ideal of $A$. If $J$ is a $p$-adic ideal of $A$ containing $I$. Then we have $\sqrt{\mathcal{I}} \subset J$. We conclude that $\sqrt{\mathcal{I}}$ is the smallest $p$-adic ideal of $A$ containing $I$. □

**Theorem 2.11** Let $A$ be a Noetherian ring and $I$ an ideal of $A$. If $I$ is a $p$-adic ideal. Then all the minimal prime ideals of $I$ are also $p$-adic ideals of $A$.

**Proof.** Let us assume that $I$ is a $p$-adic ideal of $A$. From Remark 2.9, we deduce that $I = \sqrt{\mathcal{I}}$. According to a general result of commutative algebra (cf. [13]), we have

$$I = I_1 \cap I_2 \cap \ldots \cap I_r,$$

where each ideal $I_i$ is a prime ideal of $A$. Moreover $I_i \not\subset I_j$ if $i \neq j$. The $I_i$’s are called the minimal prime ideals of $I$. On the other hand since $I = \sqrt{\mathfrak{p} I}$, we have

$$I = \bigcap \left\{ \mathcal{I} \mid \mathcal{I} \text{ is a } p\text{-adic prime ideal of } A \text{ such that } I \subset \mathcal{I} \right\}.$$

Let $\mathcal{I}$ be a $p$-adic prime ideal of $A$ such that $I_1 \cap \ldots \cap I_r \subset \mathcal{I}$. Since $\mathcal{I}$ is a prime ideal, there exists $i \in \{1, \ldots, r\}$ such that $I_i \subset \mathcal{I}$. Since $I_i$ is a minimal prime ideal of $I$, we deduce that $I_i = \mathcal{I}$. We conclude that $I_i$ is a $p$-adic ideal of $A$. Similarly $I_1, \ldots, I_{i-1}, I_{i+1}, \ldots, I_r$ are $p$-adic ideals of $A$. □
3 Characterization of $p$-adic spectrum of a ring

The $p$-adic spectrum of a ring was first introduced by Robinson [16] in order to give a $p$-adic analogue of the real spectrum of a ring. This construction has been generalized to finite extension fields of $\mathbb{Q}_p$ by Belair [1]; and independently by Bröcker et Schinke [5]. Here we follow more closely the approach of [2].

Let $A$ be a ring, and let us consider the relation $\sim_p$ on the homomorphisms $A \rightarrow L$, where $L \models \text{Th}(\mathbb{Q}_p)$. Let $f : A \rightarrow L$ and $g : A \rightarrow M$ be two homomorphisms, where $L, M \models \text{Th}(\mathbb{Q}_p)$. We say that $f$ and $g$ are equivalent, denoted by $f \sim_p g$, if there is $\varphi : L \rightarrow M$ such that $g = \varphi \circ f$, that is, if the following diagramme commutes:

$$
\begin{array}{ccc}
A & \xrightarrow{f} & K \\
\downarrow{g} & & \downarrow{\varphi} \\
L & \end{array}
$$

The model-completeness of the theory $\text{Th}(\mathbb{Q}_p)$ insures that the relation $\sim_p$ is an equivalence relation. We can now state (see also [2]):

**Definition 3.1** Let $A$ be a ring. The $p$-adic spectrum of $A$, denoted by $\text{Spec}_p(A)$, is the topological space defined by

$$
\text{Spec}_p(A) = \left\{ A \rightarrow L \mid L \models \text{Th}(\mathbb{Q}_p) \right\} / \sim_p,
$$

and whose topology is given by the open basis

$$
\left\{ D_n(a) \mid n \in \mathbb{N} \text{ and } a_i \in A \text{ for } 1 \leq i \leq r \right\},
$$

where

$$
D_n(a) = \left\{ (A \xrightarrow{\varphi} L) / \sim_p \mid L \models \bigwedge_{i=1}^{r} P_{n_i}(\varphi(a_i)) \right\}.
$$

**Remark 3.2** 1) It is easy to see (using Macintyre’s theorem) that all the sets $D_n(a)$ are well-defined.

2) The element of $\text{Spec}_p(A)$ which is represented by $\alpha : A \rightarrow K_\alpha$ will also be denoted by $\alpha$.

A subset $C$ of $\text{Spec}_p(A)$ is called constructible subset if $C$ can be obtained by taking a finite number of intersections, unions and complements from open basis of $\text{Spec}_p(A)$.

**Proposition 3.3 (c.f. [2])**. Let $A$ be an arbitrary ring. Then for all $a \in A^r$ and all $n \in \mathbb{N}^r$, $D_n(a)$ is a quasi-compact space. In particular, the $p$-adic spectrum $\text{Spec}_p(A)$ of $A$ is a quasi-compact space.
The quasi-compactness of the $p$-adic spectrum has been used in [9] with combination of other arguments to show the rationality of the Łojasiewicz’s exposant for $p$-adic semi-algebraic functions. Now we give a relationship between the notion of $p$-adic ring and that of $p$-adic spectrum of this ring:

**Proposition 3.4** Let $A$ be an integral domain. Then $\text{Spec}_p(A)$ is not empty if and only if $A$ is $p$-adic.

**Proof.** It is clear that to give a point of $\text{Spec}_p(A)$ is equivalent to give a homomorphism from $A$ to some $p$-adically closed field $L$. □

Now let us remark that a point of the real spectrum $\text{Spec}_r(A)$ of the ring $A$ can be regarded as an ordered pair $(I, \leq)$, where $I$ is a real prime ideal of $A$ and $\leq$ a linear order on the residue field $k(I)$ of $I$. But to give a linear order $\leq$ on $k(I)$ is equivalent to give its positive cone

$$\{x \in k(I) \mid 0 \leq x\} = \{x \in k(I) \mid x = y^2 \text{ and } y \in R\} = k(I) \cap R^{(2)},$$

where $R$ is a real closed extension field of $k(I)$. Let us note that

$$k(I) \cap R^{(2n)} = k(I) \cap R^{(2)} \quad \text{and} \quad k(I) \cap R^{(2n+1)} = k(I) \quad \text{for all } n \geq 1.$$

Thus the subset $k(I) \cap R^{(2)}$ is sufficient to determine a linear order on $k(I)$. Therefore a point of the real spectrum $\text{Spec}_r(A)$ of $A$ may be viewed as an ordered pair $(I, k(I) \cap R^{(2)})$, where $I$ is a real prime ideal of $A$ and $R$ is a real closed extension field of the residue field $k(I)$ of $I$. For more details about the real spectrum of a ring and its application in real geometry we refer the reader to [3]. The following result provides a $p$-adic analogue of the above remark (see also [18]):

**Theorem 3.5 (Characterization of the $p$-adic spectrum)** Let $A$ be an arbitrary ring. The following statements are equivalent:

1. There exists a point $\alpha$ of $\text{Spec}_p(A)$.

2. There exists $(I_\alpha, (k(I_\alpha) \cap L^{(n)})_{n \geq 1})$, where $I_\alpha$ is a $p$-adic prime ideal of $A$ and $L$ a $p$-adically closed extension field of the residue field $k(I_\alpha)$ of $I_\alpha$.

**Proof.** Let $\alpha$ be a point of $\text{Spec}_p(A)$. Then $\alpha$ is given by a homomorphism $\alpha : A \rightarrow L$, where $L$ is a $p$-adically closed field. Let us consider the ideal $I_\alpha = \ker(\alpha)$. According to Definition 2.5, the residue field $k(I_\alpha)$ of $I_\alpha$ is formally $p$-adic field. Moreover, $L$ is a $p$-adically closed extension field of $k(I_\alpha)$. Thus the ordered pair $(I_\alpha, (k(I_\alpha) \cap K^{(n)})_{n \geq 1})$ is the pair wanted. Now if

$$\psi : A \rightarrow M$$
is an other homomorphism associated to $\alpha$, with $M$ is a $p$-adically closed field. Then there exists a homomorphism $\phi : L \to M$ such that $\psi = \phi \circ \alpha$. Then $I_\psi = I_\alpha$ and $k(I_\psi) = k(I_\alpha)$. From corollary 1.4, we have

$$k(I_\alpha) \cap K^{(n)} = k(I_\psi) \cap L^{(n)} \quad \text{for all } n \geq 1.$$  

Inversely, let $(I, (k(I) \cap L^{(n)})_{n \geq 1})$ be an ordered pair, with $I$ is a $p$-adic prime ideal of $A$ and $L$ a $p$-adically closed extension field of the residue field $k(I)$ of $I$. Let $s : A \to A/I$ the canonical homomorphism and $i : A/I \to k(I)$ the canonical embedding. Therefore

$$A \xrightarrow{s} A/I \xrightarrow{i} k(I) \xrightarrow{\psi} K.$$ 

Let us put $\varphi = \Psi \circ i \circ s$. Then $\varphi$ is a homomorphism from $A$ to the $p$-adically closed field $L$. The coset equivalence of this homomorphism with respect to $\sim_p$ is a point of $\text{Spec}_p(A)$. □

## 4 Variants of $p$-adic Nullstellensatz

In this section we prove an abstract Nullstellensatz for the $p$-adic spectrum of a ring. We also state some conjectures concerning the Nullstellensatz for the rings of formal and convergent power series over the $p$-adic number field $\mathbb{Q}_p$.

Let $A$ be a ring and $x \in A$. For all $\alpha \in \text{Spec}_p(A)$, we will write $x(\alpha) = \alpha(x)$. It is easy to see that

$$\text{supp}(\alpha) = \{x \in A \mid x(\alpha) = 0\}$$

is a $p$-adic prime ideal of $A$. If $I$ is an ideal of $A$, we denote by $\mathcal{Z}(I)$ the subset of $\text{Spec}_p(A)$ given by

$$\mathcal{Z}(I) = \{\alpha \in \text{Spec}_p(A) \mid x(\alpha) = 0 \quad \forall x \in I\}.$$ 

If $X$ is a subset of $\text{Spec}_p(A)$, we denote by $\mathcal{J}(X)$ the ideal of $A$ defined by

$$\mathcal{J}(X) = \{x \in A \mid x(\alpha) = 0 \quad \forall \alpha \in X\}.$$ 

Let us remark that if $I$ is an ideal of $A$, then

$$\mathcal{J}(\mathcal{Z}(I)) = \bigcap_{\alpha \in \mathcal{Z}(I)} \{x \in A \mid x(\alpha) = 0\} = \bigcap_{\alpha \in \mathcal{Z}(I)} \text{supp}(\alpha).$$
The operators $\mathcal{J}$ and $\mathcal{Z}$ verify the same elementary properties as their analogous in the real spectrum. In particular, for all $X \subset \text{Spec}_p(A)$

$$X = \mathcal{Z}(\mathcal{J}(X)).$$

However the composition in the reverse order is determined by the abstract Nullstellensatz.

**Theorem 4.1** (Nullstellensatz for $\text{Spec}_p(A)$). Let $A$ be a ring. Then for any ideal $I$ of $A$, we have

$$\mathcal{J}(\mathcal{Z}(I)) = \sqrt{I}.$$  

**Proof.** Let $x \in \sqrt{I}$. Then for any $p$-adic prime ideal $J$ of $A$ such that $I \subseteq J$, one has $x \in J$. Since for all $\alpha \in \mathcal{Z}(I)$, supp($\alpha$) is a $p$-adic prime ideal of $A$ such that $I \subseteq \text{supp}(\alpha)$. Therefore we have for all $\alpha \in \mathcal{Z}(I)$, $x \in \text{supp}(\alpha)$. It follows that $x \in \bigcap_{\alpha \in \mathcal{Z}(I)} \text{supp}(\alpha)$. Thus $x \in \mathcal{J}(\mathcal{Z}(I))$, and $\sqrt{I} \subseteq \mathcal{J}(\mathcal{Z}(I))$.

Inversely, if $x \notin \sqrt{I}$. Then there exists a $p$-adic prime ideal $J$ of $A$ such that $I \subseteq J$ and $x \notin J$. Let us consider the following homomorphism $\alpha : A \rightarrow A/J \rightarrow k(J) \rightarrow L$. We remark that $\alpha \in \mathcal{Z}(I)$. Moreover, we have: $x(\alpha) \neq 0$. Thus $x \notin J$. Therefore $x \notin \mathcal{J}(\mathcal{Z}(I))$, and $\mathcal{J}(\mathcal{Z}(I)) \subseteq \sqrt{I}$. We conclude that $\sqrt{I} = \mathcal{J}(\mathcal{Z}(I))$. \qed

Let $K$ be a $p$-adically closed field. Using the notion $p$-adic ideal and the model-completeness of $\text{Th}(\mathbb{Q}_p)$, we have shown in [17] the following result.

**Theorem 4.2** ($p$-adic Nullstellensatz for polynomials). For any ideal $I$ of $K[X]$, \[\sqrt{I} = \mathcal{J}(\mathcal{Z}(I)).\]

We denote by $C^\infty (\mathbb{Q}_p^m,0)$ the set of $C^\infty$ function germs at the origin 0 of $\mathbb{Q}_p^m$. For $f \in C^\infty (\mathbb{Q}_p^m,0)$, we denote by $T(f)$ the Taylor series of $f$ at 0. Let $X$ be a closed germ at the origin 0 of $\mathbb{Q}_p^m$. We say that a formal power series $\hat{f} \in \mathbb{Q}_p[[X]]$ vanishes on $X$ if for any $f \in C^\infty (\mathbb{Q}_p^m,0)$ such that $\hat{f} = T(f)$ and any $a > 0$, there exists a neighborhood $U$ of 0 such that

$$|f(x)|_p \leq \|x\|_p^a$$

for any $x \in U \cap \hat{X}$,

where $\hat{X}$ is a representant of $X$. For an ideal $I$ of $\mathbb{Q}_p[[X]]$, we denote by $\mathcal{Z}(I)$ the set defined by

$$\mathcal{Z}(I) = \left\{ X \mid \hat{f} \text{ vanishes on } X \text{ for any } \hat{f} \in I \right\},$$

and by $\mathcal{J}(\mathcal{Z}(I))$ the ideal of $\mathbb{Q}_p[[X]]$ defined by

$$\mathcal{J}(\mathcal{Z}(I)) = \left\{ \hat{f} \in \mathbb{Q}_p[[X]] \mid \hat{f} \text{ vanishes on } X \text{ for any } X \in \mathcal{Z}(I) \right\}.$$
The Nullstellensatz for the ring \( \mathbb{R}[[X]] \) is proved by Risler [15]. In view of the analogy with the real case, we propose

**Conjecture 4.3** (\( p \)-adic Nullstellensatz for formal power series). For any ideal \( I \) of \( \mathbb{Q}_p[[X]] \),

\[
\sqrt[p]{I} = \mathcal{J}(\mathcal{Z}(I)).
\]

Let us recall that a subset \( S \) of \( \mathbb{Q}_p^n \) is called \( p \)-adic analytic set at \( 0 \) if there exists convergent power series \( g_1, \ldots, g_r \in \mathbb{Q}_p\{X\} \) and an open \( U \) of \( \mathbb{Q}_p^n \) contains \( 0 \) such that

\[
S \cap U = \{ x \in U \mid \tilde{g}_1(x) = \cdots = \tilde{g}_r(x) = 0 \},
\]

where \( \tilde{g}_1, \ldots, \tilde{g}_r \) are respectively analytic representant functions of \( g_1, \ldots, g_r \) defined on \( U \). We refer the reader to [8] for a systematic study of \( p \)-adic analytic sets. For an ideal \( I \) of \( \mathbb{Q}_p\{X\} \) generated by \( f_1, \ldots, f_r \), we denote by \( \mathcal{Z}(I) \) the germ at the origin \( 0 \) of \( \mathbb{Q}_p^n \) associated to the \( p \)-adic analytic set at \( 0 \) defined by \( f_1, \ldots, f_r \), and by \( \mathcal{J}(\mathcal{Z}(I)) \) the ideal of \( \mathbb{Q}_p\{X\} \) defined by

\[
\mathcal{J}(\mathcal{Z}(I)) = \left\{ f \in \mathbb{Q}_p\{X\} \mid \tilde{f}(x) = 0 \quad \forall x \in \Omega \cap \tilde{X} \right\},
\]

where \( \tilde{X} \) is a representant of \( X \) and \( \Omega \) an open of \( \mathbb{Q}_p^n \) contains \( 0 \). The Nullstellensatz for the ring \( \mathbb{R}\{X\} \) of convergent power series was proved in [15]. In the \( p \)-adic case, we state

**Conjecture 4.4** (\( p \)-adic Nullstellensatz for convergent power series). For any ideal \( I \) of \( \mathbb{Q}_p\{X\} \),

\[
\sqrt[p]{I} = \mathcal{J}(\mathcal{Z}(I)).
\]

**ACKNOWLEDGEMENTS.** We would like to thank Professor Abedelhafid El Khadiri for helpful discussions and encouragements.

**References**


*Received: November, 2008*