NORMAL BASES OF RINGS OF CONTINUOUS FUNCTIONS CONSTRUCTED WITH THE (q_n)-DIGIT PRINCIPLE

S. EVRARD

When K is a local field with valuation ring V, K. Conrad [6] constructs normal bases of the ring $\mathcal{C}(V,K)$ of continuous functions from V to K, using what he calls the extension by q-digit expansion, where q denotes the cardinality of the residue field k of V. In this article, we extend Conrad's method to the ring $\mathcal{C}(S,K)$ of continuous functions from S to K where S denotes a subset of V. Moreover, we no more assume the finiteness of the residue field k, but replace this condition by the precompactness of S.

We first recall in Section 1 the notion of normal basis and Conrad's q-digit principle. In Section 2, we define the extension by (q_n)-digit expansion. Then, in Section 3, we generalize Conrad's q-digit principle by our (q_n)-digit principle (Theorem 3.6), that may be applied in particular to Amice's regular compact subsets [1]. In section 4, we end with several examples.

1. The q-digit principle

Let $(K,|\,|)$ be a complete valued non-archimedean field. Denote by V the corresponding valuation ring, $\mathfrak{M}$ its maximal ideal and k its residue field. Let $(E,\|\cdot\|)$ be an ultrametric Banach space over K.

Definition 1.1. A sequence $(e_n)_{n\geq 0}$ of elements of E is called a *normal basis of* E(orthonormal basis in [6]) if

(1) each $x \in E$ has a representation as $x = \sum_{n\geq 0} x_n e_n$ where $x_n \in K$ and $\lim_{n\to\infty} x_n = 0$,
(2) in the representation $x = \sum_{n\geq 0} x_n e_n$, we have $\|x\| = \sup_n |x_n|$.

Let $E_0 = \{x \in E / \|x\| \leq 1\}$. Then $E_0/\mathfrak{M}E_0$ is a k-vector space. For $e_n \in E_0$, $\overline{e}_n$ denotes the reduction of e_n modulo $\mathfrak{M}E_0$. The following proposition allows to characterize normal bases in purely algebraic terms.

Date: September 5, 2008.
1991 *Mathematics Subject Classification.* 13F20, 11S99.
Key words and phrases. Non-archimedean valued field, regular compact, generalized Vandermonde determinant, normal bases, Legendre set.
The author wishes to thank Professor Chabert for his remarks and great help.

Proposition 1.2. [2, prop.3.1.5] *Assume that the valuation is discrete and that $\|E\| = |K|$. A sequence $(e_n)_{n\in\mathbb{N}}$ of elements of E is a normal basis of E if and only if $e_n \in E_0$ for every $n \geq 0$ and $(\overline{e}_n)_{n\in\mathbb{N}}$ is a k-basis of $E_0/\mathfrak{M}E_0$.*

Assuming that k is finite with cardinality q (hence K is a local field), K. Conrad [6] uses extension by q-digit expansion to construct some normal bases of the ring $\mathcal{C}(V, K)$. We first recall this notion.

Definition 1.3. Let $(e_n)_{n\geq 0}$ be a sequence of elements of $\mathcal{C}(V, V)$. We construct another sequence of functions (f_i) in the following way :

$$\begin{cases} \text{if} & i = i_0 + i_1 q + \cdots + i_r q^r \quad (0 \leq i_j < q) \\ \text{then} & f_i = e_0^{i_0} \cdots e_r^{i_r}. \end{cases}$$

The sequence (f_i) is called *the extension of the (e_n) by q-digit expansion.*

In characteristic p, V contains a field which is isomorphic to k and then, it may be seen as a k-vector space. In this case, the q-digit principle has the following form:

Proposition 1.4. *Digit principle in characteristic p* [6, Theorem 2]
If the sequence (e_n) is a normal basis of the ring of continuous k-linear functions from V to K, then the extension of the (e_n) by q-digit expansion is a normal basis of $\mathcal{C}(V, K)$.

As noted by K. Conrad, in characteristic 0 there is no analogue of the subspace of linear functions. Nevertheless, there is another version that holds in any characteristic :

Proposition 1.5. *Digit principle in any characteristic* [6, Theorem 3]
Let $(e_n)_{n\geq 0}$ be a sequence of elements of $\mathcal{C}(V, V)$ such that the reductions $\overline{e}_i \in \mathcal{C}(V, k)$ are constant on the cosets modulo $\mathfrak{M}^{i+1}$ and the map

$$\phi_n : \begin{cases} V/\mathfrak{M}^n & \to & k^n \\ x & \mapsto & (\overline{e}_0(x), \cdots, \overline{e}_{n-1}(x)) \end{cases} \quad \textit{is bijective.}$$

Then the extension of the (e_n) by q-digit expansion is a normal basis of $\mathcal{C}(V, K)$.

To generalize the q-digit principle to subsets S, the map ϕ_r will be required to be only injective, as $S/\mathfrak{M}^r$ does not necessarily contain q^r elements.

2. The (q_n)-digit expansion

Hypotheses and notation. Let V be a discrete valuation domain, with valuation v. Denote by K the quotient field of V, $\mathfrak{M}$ the maximal ideal of V, π a generator of $\mathfrak{M}$ (with $v(\pi) = 1$), $k = V/\mathfrak{M}$ the residue field and q the cardinality (finite or not) of k. Let S be an infinite subset of V.

We denote by $\widehat{V}$, $\widehat{K}$, and $\widehat{S}$ the completions of V, K and S with respect to the $\mathfrak{M}$-adic topology. We still denote by v the extension of v to $\widehat{K}$. For every $n \geq 0$, we denote by $S/\mathfrak{M}^n$ the set formed by the classes of S mod $\mathfrak{M}^n$ and we define q_n as the cardinality of $S/\mathfrak{M}^n$ ($q_0 = 1$).
We assume that S is precompact, that is, $\widehat{S}$ is compact, and we know that this is equivalent to the fact that all the q_n's are finite.

Of course, the sequence (q_n) is a non-decreasing and non-stationary sequence. Now, we define the (q_n)-digit expansion of a positive integer m:

Proposition 2.1. *Let $(q_n)_{n\geq 0}$ be a non-decreasing and non-stationary sequence of integers, with $q_0 = 1$. For every $m > 0$, there exists a unique representation of m as:*

$$m = m_0 + m_1 q_1 + \cdots + m_r q_r$$

where r is such that

$$q_r \leq m < q_{r+1}$$

and where, for every j in $[1, r]$,

$$m_j \geq 0 \quad \text{and} \quad m_0 + m_1 q_1 + \cdots + m_j q_j < q_{j+1}.$$

This representation is called the (q_n)-digit expansion of m.

Proof. Suppose there is such a representation of m. For $0 \leq k \leq r$, let

$$N_k = m_0 + m_1 q_1 + \cdots + m_k q_k.$$

Hence, for $1 \leq k \leq r$, one has:

$$N_k = N_{k-1} + m_k q_k, \text{ with } N_{k-1} < q_k.$$

So, m_k is the quotient of the division of N_k by q_k and N_{k-1} is the rest. Consequently, the sequence (m_k) is uniquely determined.
Conversely, let us prove that such a sequence satisfies our hypothesis. Consider the sequences $N_r, N_{r-1}, \cdots, N_0$ and $m_r, m_{r-1}, \cdots, m_0$ defined by induction in the following way:

$$\begin{cases} N_r = m \\ m_k = \left[\frac{N_k}{q_k}\right] & \text{for } 0 \leq k \leq r \\ N_{k-1} = N_k - m_k q_k & \text{for } 1 \leq k \leq r. \end{cases}$$

By definition of r, $m_r = [m/q_r] \neq 0$. At each step ($1 \leq k \leq r$), one has $N_{k-1} < q_k$ and $m = N_{k-1} + m_k q_k + \cdots + m_r q_r$. Indeed,

$$\sum_{l=k}^{r} m_l q_l = \sum_{l=k}^{r} (N_l - N_{l-1}) = m - N_{k-1}.$$

Hence,

$$m = N_0 + m_1 q_1 + \cdots + m_r q_r,\ m_0 = \left[\frac{N_0}{q_0}\right] = N_0.$$

Finally, $m = \sum_{k=0}^{r} m_k q_k$ and, for $0 \leq k \leq r$,

$$m_0 + m_1 q_1 + \cdots + m_k q_k = m - (m_{k+1} q_{k+1} + \cdots + m_r q_r) = N_k < q_{k+1}.$$

□

Remarks 2.2. (1) Let $m = m_0 + m_1 q_1 + \cdots + m_r q_r$ be the (q_n)-digit expansion of m. Then, for $0 \leq j \leq r$, one has:
- $0 \leq m_j < \frac{q_{j+1}}{q_j}$,
- in particular, if $q_j = q_{j+1}$ then $m_j = 0$.

(2) The condition $0 \leq m_j < \frac{q_{j+1}}{q_j}$ is not sufficient to define the m_j's. If we consider the sequence $q_n = 2n + 1$ of odd integers, the (q_n)-digit expansion of $m = 5$ is $m = 5 = q_2$, but one can also write $m = 2 + 3 = 2q_0 + q_1$ with $m_0 = 2 < \frac{q_1}{q_0} = 3$.

(3) On the contrary, the condition $0 \leq m_j < \frac{q_{j+1}}{q_j}$ does characterize the (q_n)-digit expansion when q_j divides q_{j+1}. Indeed, if $\alpha_j = q_{j+1}/q_j$ is an integer and $0 \leq m_j < \alpha_j$, then $m_0 < q_1$, and by induction, $(m_0 + m_1 q_1 + \cdots + m_{j-1} q_{j-1}) + m_j q_j < q_j + (\alpha_j - 1) q_j = \alpha_j q_j = q_{j+1}$.

(4) If the sequence (q_n) is associated to a subset S (that is $q_n = \mathrm{Card}(S/\mathfrak{M}^n)$), then we have $q_n \leq q_{n+1} \leq q.q_n$. As already said, (q_n) is a non-decreasing and non-stationary sequence. Note that the sequence needs not to be strictly increasing and q_n does not necessarily divide q_{n+1}, as shown by $V = \mathbb{Z}_5$ and $S = 125\mathbb{Z}_5 \bigcup \{25 + 125\mathbb{Z}_5\} \bigcup \{1 + 125\mathbb{Z}_5\}$. One has: $S/(5) = \{0, 1\}$ and $q_1 = 2$; $S/(25) = \{0, 1\}$ and $q_2 = 2$; $S/(125) = \{0, 1, 25\}$ and $q_3 = 3$; $q_4 = 15$ and, more generally, $q_n = 3 \times 5^{n-3}$ for $n \geq 3$.

Definition 2.3. Let $(e_n)_{n \geq 0}$ be a sequence of elements of a commutative monoid (with an identity element). *The extension of the sequence* $(e_n)_{n \geq 0}$ *by* (q_n)*-digit expansion* is the following sequence $(f_m)_{m \geq 0}$:

$$f_m = e_0^{m_0} \times e_1^{m_1} \times \cdots \times e_r^{m_r}$$

where $m = m_0 + m_1 q_1 + \cdots + m_r q_r$ is the (q_n)-digit expansion of m.

Remarks 2.4. (1) $f_0 = 1$.

(2) If there exists j such that $q_j = q_{j+1}$, then the term e_j of the sequence (e_n) never appears in any element of the sequence (f_m).

(3) For $q_r \leq m < q_{r+1}$, if $m = m_r q_r + N_r$ with $N_r < q_r$, then

$$f_m = e_r^{m_r} \times f_{N_r}.$$

We now try to find conditions on the subset S and on the sequence $(e_n)_{n\geq 0}$ of elements of $\mathcal{C}(\widehat{S},\widehat{V})$ for the sequence $(f_m)_{m\geq 0}$ to be a normal basis of $\mathcal{C}(\widehat{S},\widehat{K})$. We first assume that the sequence $(e_n)_{n\geq 0}$ satisfies a condition similar to that considered by K. Conrad. More precisely, let $(e_n)_{n\geq 0}$ be a sequence of elements of $\mathcal{C}(\widehat{S},\widehat{V})$ such that, for each $n\geq 0$, the reduction $\overline{e}_n$ of e_n in $\mathcal{C}(\widehat{S},k)$ is constant on the cosets of S modulo $\mathfrak{M}^{n+1}$. Denote by $(f_m)_{m\geq 0}$ the extension of $(e_n)_{n\geq 0}$ by (q_n)-digit expansion. It is obvious that, for $0\leq m<q_r$, the reductions $\overline{f}_m$ in $\mathcal{C}(\widehat{S},k)$ are constant on the cosets of S modulo $\mathfrak{M}^r$. In order to determine whenever this sequence is a normal basis of $\mathcal{C}(\widehat{S},\widehat{K})$, we use the following lemma.

Lemma 2.5. *Let $(g_n)_{n\geq 0}$ be a sequence of $\mathcal{C}(\widehat{S},\widehat{V})$ such that, for $0\leq m<q_r$, the reduction $\overline{g}_m$ in $\mathcal{C}(\widehat{S},k)$ are constant on the cosets of S modulo $\mathfrak{M}^r$. The following assertions are equivalent:*

1. *(g_n) is a normal basis of $\mathcal{C}(\widehat{S},\widehat{K})$,*
2. *$(\overline{g}_n)$ is a k-linear basis of $\mathcal{C}(\widehat{S},k)$,*
3. *for each integer $r\geq 1$, $(\overline{g}_m)_{0\leq m<q_r}$ is a k-basis of the space $\mathcal{F}(S/\mathfrak{M}^r,k)$ of functions from $S/\mathfrak{M}^r$ to k,*
4. *for each n, the $\overline{g}_m$'s ($0\leq m<n$) are k-linearly independent.*

Proof. Proposition 1.2 gives the equivalence between assertions (1) and (2). The equivalence between assertions (3) and (4) follows from the dimension of the vector space $\mathcal{F}(S/\mathfrak{M}^r,k)$. Obviously, (2) implies (4). Finally, (3) implies (2) as a continuous function from $\widehat{S}$ to k is locally constant and can be seen as a map from $S/\mathfrak{M}^r$ to k for some r. □

Proposition 2.6. *Let $(g_n)_{n\geq 0}$ be a sequence of functions such that, for every $0\leq m<q_r$, the reductions $\overline{g}_m$ in $\mathcal{C}(\widehat{S},k)$ are constant on the cosets of S modulo $\mathfrak{M}^r$. For $r\geq 1$, let G_r be the following matrix:*

$$G_r=(\overline{g}_j(a_i))_{0\leq i,j<q_r},$$

where $(a_i)_{0\leq i<q_r}$ denotes a complete set of residues of S modulo $\mathfrak{M}^r$. Then the following properties hold true:

1. *$\det G_r$ does not depend on the a_i's (except for the sign).*
2. *The $\overline{g}_m$'s ($0\leq m<q_r$) are k-linearly independent if and only if $\det G_r\neq 0$.*

Proof. (1) If $(b_i)_{0\leq i<q_r}$ is another complete set of residues of S modulo $\mathfrak{M}^r$, there exists a permutation σ such that $b_i\equiv a_{\sigma(i)} \pmod{\mathfrak{M}^r}$. As the $\overline{g}_j$'s are constant on the cosets of S modulo $\mathfrak{M}^r$, the rows of $(\overline{g}_j(a_i))_{0\leq i,j<q_r}$ and of $(\overline{g}_j(b_i))_{0\leq i,j<q_r}$ are then permuted.

(2) Suppose that the λ_m's $\in k$ ($0\leq m<q_r$) are such that

$$\lambda_0\overline{g}_0+\lambda_1\overline{g}_1+\cdots+\lambda_{q_r-1}\overline{g}_{q_r-1}=0.$$

Evaluating the g_m's $(0 \leq m < q_r)$ on the q_r elements of $S/\mathfrak{M}^r$, we obtain a system of q_r equations in the q_r unknowns λ_m. This system has a unique solution if and only if $\det G_r \neq 0$. □

3. Normal basis obtained by the (q_n)-digit principle

We still consider hypotheses and notation introduced in Section 2 and we complete them by the following:

Hypotheses and notation. Let $r \in \mathbb{N}$ be fixed and denote by $(a_i)_{0\leq i<q_{r+1}}$ a complete set of residues of S modulo $\mathfrak{M}^{r+1}$ such that $(a_i)_{0\leq i<q_r}$ is a complete set of residues of S modulo $\mathfrak{M}^r$. For $0 \leq i < q_r$, let

$$\gamma_i = \mathrm{Card}\{j \mid 0 \leq j < q_{r+1}, a_j \equiv a_i \pmod{\mathfrak{M}^r}\}.$$

Moreover we order the a_i's $(0 \leq i < q_r)$ such that:

$$\gamma_0 \geq \cdots \geq \gamma_{q_r-1} \geq 1.$$

Let $(e_n)_{n\geq 0}$ be a sequence of elements of $\mathcal{C}(\widehat{S}, \widehat{V})$ such that, for each $n \geq 0$, the reduction $\overline{e}_n$ of e_n in $\mathcal{C}(\widehat{S}, k)$ is constant on the cosets of S modulo $\mathfrak{M}^{n+1}$. Denote by $(f_m)_{m\geq 0}$ the extension of $(e_n)_{n\geq 0}$ by (q_n)-digit expansion. Clearly, we have:

Lemma 3.1. *There are exactly γ_{q_r-1} complete sets of residues of S modulo $\mathfrak{M}^r$ in a complete set of residues of $S/\mathfrak{M}^{r+1}$. Moreover, for all $0 \leq i, j < q_{r+1}$ such that $a_i \equiv a_j \pmod{\mathfrak{M}^r}$, one has:*

(1) $\forall k < r, \overline{e}_k(a_i) = \overline{e}_k(a_j)$
(2) $\forall k < q_r, \overline{f}_k(a_i) = \overline{f}_k(a_j)$.

3.1. **A necessary condition.**

Lemma 3.2. *Suppose that there exists r such that q_r divides q_{r+1} and write $q_{r+1} = \alpha_r \times q_r$. If the $\overline{f}_m$'s $(0 \leq m < q_{r+1})$ are k-linearly independent, then*

$$\gamma_0 = \gamma_1 = \cdots = \gamma_{q_r-1} = \alpha_r = \frac{q_{r+1}}{q_r}.$$

Proof. Assume that $\gamma_0 > \alpha_r$. First, remark that $q_r < q_{r+1}$ since, if $q_r = q_{r+1}$, one has $\gamma_i = 1 = \alpha_r$ for every i. In the matrix $G_{r+1} = (\overline{f}_j(a_i))_{0\leq i,j<q_{r+1}}$, we arrange the columns with respect to the following sequence:

$$1, \overline{e}_r, \cdots, \overline{e}_r^{\alpha_r-1}, \overline{f}_1, \cdots, \overline{f}_1\overline{e}_r^{\alpha_r-1}, \cdots, \overline{f}_i\overline{e}_r^{j}, \cdots, \overline{f}_{q_r-1}\overline{e}_r^{\alpha_r-1}.$$

We denote by $C_{i,j}$ the column corresponding to $\overline{f}_i\overline{e}_r^j$ and, for $1 \leq i < q_r$ and $0 \leq j < \alpha_r$, we use the following elementary transformations on columns :

$$C_{i,j} \leftarrow C_{i,j} - \overline{f}_i(a_0)C_{0,j}.$$

For $1 \leq l < q_{r+1}$, the term in the column $C_{i,j}$ and the row L_l becomes:

$$\overline{f}_i(a_l)\overline{e}_r^j(a_l) - \overline{f}_i(a_0)\overline{e}_r^j(a_l).$$

It follows from Lemma 3.1 that, whenever l $(0 \leq l < q_{r+1})$ is such that $a_l \equiv a_0 \pmod{\mathfrak{M}^r}$, $\overline{f}_i(a_0) = \overline{f}_i(a_l)$ and, after permutations on the rows of the matrice, the γ_0 first new rows (corresponding to such an a_l) end with null terms. Consequently, the new matrix is of the form

$$\left(\begin{array}{c|c} A & 0 \\ B & C \end{array}\right) \text{ where } A \in M_{\alpha_r}(k),$$

and, as $\gamma_0 > \alpha_r$, the first line of C is null. Finally,

$$\det G_{r+1} = \det G_{r+1} = \det A \times \det C = 0.$$

□

This necessary condition defines a class of subsets of V called Legendre subsets in [7]. Before stating our main theorem, we recall some properties of these sets.

3.2. **Legendre sets.**

Definition 3.3. The subset S is called a *Legendre set* if, for every r in $\mathbb{N}$, each class of S modulo $\mathfrak{M}^r$ contains the same number of elements modulo $\mathfrak{M}^{r+1}$.

If S is a Legendre set then, for every $r \geq 0$, q_r divides q_{r+1} and for every $0 \leq i < q_r$, one has:

$$\gamma_i = \frac{q_{r+1}}{q_r}.$$

Such subsets have been studied by Y. Amice [1] as regular compact subsets in the case when K is a local field and S is compact and by Y. Fares and the author [7] in a more general setting . Let us recall a property of the Legendre sets that we will use in the applications. We first recall the following definitions:

Definition 3.4. Let $(a_n)_{n\geq 0}$ be a sequence of elements of S.

(1) The sequence is called a *v-ordering of* S [3] when, for every $n > 0$,

$$v\left(\prod_{0\leq k<n}(a_n - a_k)\right) = \inf_{x\in S} v\left(\prod_{0\leq k<n}(x - a_k)\right).$$

(2) The sequence is called *a very well distributed sequence of* S [1] if, for every $r > 0$ and every $\lambda \in \mathbb{N}$, $(a_{\lambda q_r}, \cdots, a_{(\lambda+1)q_r-1})$ is a complete set of residues of $S/\mathfrak{M}^r$.

We then have a very nice property:

Proposition 3.5. [7]

- *A very well distributed sequence of a subset is a v-ordering.*
- *Every v-ordering of a Legendre set is a very well distributed sequence.*

Here are some examples of Legendre sets:

Example 1. Assume that the residue field k is finite of cardinality q.

(1) V is a Legendre set and $q_n = q \times q_{n-1} = q^n$.
(2) Let $S = \cup_{j=1}^{r} b_j + \mathfrak{M}$, where $b_1, \cdots, b_r$ are not congruent mod $\mathfrak{M}$, then S is a Legendre set and $q_n = rq^{n-1}$.
(3) Let $u \in V$ be such that $v(u) = 0$. Then $S = \{u^n;\, n \in \mathbb{N}\}$ is a Legendre set.

We are ready to state our theorem.

3.3. **Extension of Conrad's q-digit principle.**

Theorem 3.6. *Let V be a discrete valuation domain with maximal ideal $\mathfrak{M}$ and residue field $k = V/\mathfrak{M}$. Let S be a precompact subset of V and, for $n \geq 0$, let $q_n = card(S/\mathfrak{M}^n)$. Assume that, for every r, q_r divides q_{r+1}. Let (e_i) be a sequence of elements of $\mathcal{C}(\widehat{S}, \widehat{V})$ such that the reductions $\overline{e}_i \in \mathcal{C}(\widehat{S}, k)$ are constant on the cosets of S modulo $\mathfrak{M}^{i+1}$ and suppose that, for every $r \geq 0$, the following map is injective:*

$$\phi_r : \left\{ \begin{array}{ccc} S/\mathfrak{M}^{r+1} & \to & k^{r+1} \\ x & \mapsto & (\overline{e}_0(x), \cdots, \overline{e}_r(x)) \end{array} \right.$$

Then the extension $(f_m)_{m\geq 0}$ of the $(e_n)_{n\geq 0}$ by (q_n)-digit expansion is a normal basis of $\mathcal{C}(\widehat{S}, \widehat{K})$ if and only if S is a Legendre set.

Proof. The necessary condition follows from Lemmas 2.5 and 3.2. Using Proposition 2.6, we show that the condition is sufficient. We prove by induction on r that $\det G_r \neq 0$. For $r = 0$, one has

$$\det G_1 = V(\overline{e}_0(a_0), \cdots, \overline{e}_0(a_{q_1-1}))$$

where $V(\cdot)$ denotes the Vandermonde determinant. By hypothesis, ϕ_0 is injective, hence $\det G_1 \neq 0$. Now, we suppose that $\det G_r \neq 0$ and we show that $\det G_{r+1} \neq 0$. First, as there are exactly α_r complete sets of residues of S modulo $\mathfrak{M}^r$ in $(a_i)_{0\leq i<q_r}$, we can assume that for $0 \leq i < q_r$ and $0 \leq l < \alpha_r$,

$$a_{i+lq_r} \equiv a_i \pmod{\mathfrak{M}^r}.$$

then we compute $\det G_{r+1}$ by ordering each row L_{r+1} in the matrix as follows:

$$L_1 = (\overline{f}_0, \cdots, \overline{f}_{q_1-1}) = (1, \overline{e}_0, \cdots, \overline{e}_0^{q_1-1})$$

and, for $r \geq 1$,

$$L_{r+1} = (L_r, \overline{e}_r L_r, \cdots, \overline{e}_r^{\alpha_r-1} L_r).$$

So we can write:

$$G_{r+1} = \begin{pmatrix} I_{q_r} & J_0 & \dots & J_0^{\alpha_r-1} \\ \vdots & J_1 & \dots & J_1^{\alpha_r-1} \\ \vdots & \vdots & \vdots & \vdots \\ I_{q_r} & J_{\alpha_r-1} & \dots & J_{\alpha_r-1}^{\alpha_r-1} \end{pmatrix} \times \begin{pmatrix} G_r & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & G_r \end{pmatrix},$$

with, for $0 \leq l < \alpha_r$,

$$J_l = \begin{pmatrix} \overline{e}_r(a_{lq_r}) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \overline{e}_r(a_{(l+1)q_r-1}) \end{pmatrix}.$$

We now compute the determinant of B, noticing that the matrices J_l and J_j are commuting:

$$\det B = V(J_0, \cdots, J_{\alpha_r-1}) = \prod_{0 \leq l < j < \alpha_r} \det(J_j - J_l).$$

We then obtain

$$\det G_{r+1} = \det G_r^{\alpha_r} \times \prod_{i=0}^{q_r-1} V\left(\overline{e}_r(a_i), \overline{e}_r(a_{q_r+i}), \cdots, \overline{e}_r(a_{(\alpha_r-1)q_r+i})\right).$$

By induction hypothesis, $\det G_r \neq 0$. Moreover, as for $j < r$, one has, for every $0 \leq l < \alpha_r$,

$$\overline{e}_j(a_i) = \overline{e}_j(a_{lq_r+i}),$$

the injectivity of ϕ_{r+1} implies that, for $0 \leq j < l \leq \alpha_r$, one has

$$\overline{e}_r(a_{i+jq_r}) \neq \overline{e}_r(a_{i+lq_r}).$$

Hence, for every i $(1 \leq i \leq q_r)$,

$$V\left(\overline{e}_r(a_i), \overline{e}_r(a_{q_r+i}), \cdots, \overline{e}_r(a_{(\alpha_r-1)q_r+i})\right) \neq 0.$$

□

4. Applications

4.1. **Examples of normal bases obtained by the (q_n)-digit principle.** For the following examples, the hypotheses of Theorem 3.6 are clearly satisfied.

Proposition 4.1. *Let S be a Legendre set, and denote by F a complete set of residues of V mod $\mathfrak{M}$. Each x in S has a unique representation of the form $x = x_0 + x_1\pi + \cdots + x_j\pi^j + \cdots$ with $x_j \in F$. For each $j \geq 0$, let*

$$\omega_j : \begin{cases} S & \to & V \\ x & \mapsto & x_j \end{cases}$$

Then (Ω_m), the extension of (ω_n) by (q_n)-digit expansion is a normal basis of $\mathcal{C}(\widehat{S}, \widehat{K})$.

The second example uses hyperdifferential operators as defined by Voloch in [9]: We suppose here that the characteristic of V is $p > 0$, then we can consider V as a k-vector space. He defines a sequence of k-linear maps δ_r by the following condition:

$$\forall r \in \mathbb{N}, \forall m \in \mathbb{N}, \delta_r(\pi^m) = \begin{pmatrix} m \\ r \end{pmatrix} \pi^{m-r}.$$

Proposition 4.2. *Let S be a Legendre set of V. The sequence (Δ_m) extension of (δ_r) by (q_n)-digit expansion is a normal basis of $\mathcal{C}(\widehat{S}, \widehat{K})$.*

4.2. **A polynomial example.** We end with a polynomial example. We already know ([5] or [4]) that, if S is a subset in a discrete valuation ring V and $(a_n)_{n\geq 0}$ is a v-ordering of S, then the sequence of polynomials :

$$u_r(X) = \prod_{0\leq i<r} \frac{X - a_i}{a_r - a_i}$$

is a normal basis of $\mathcal{C}(\widehat{S}, \widehat{K})$. Here is another example:

Proposition 4.3. *Let S be a Legendre set and $(a_n)_{n\geq 0}$ be a v-ordering of S. Let (e_r) defined by :*

$$e_0(X) = X$$
$$e_r(X) = \prod_{0\leq i<q_r} \frac{X - a_i}{a_{q_r} - a_i} \text{ for } r \geq 1.$$

The sequence (f_m), extension of (e_r) by (q_n)-digit expansion, is a normal basis of $\mathcal{C}(\widehat{S}, \widehat{K})$.

Proof. Of course, e_r is an integer-valued polynomial, with $\deg(e_r) = q_r$. First, we want to prove that for every $r, \overline{e}_r \in \mathcal{C}(\widehat{S}, k)$ is constant on the cosets of S modulo $\mathfrak{M}^{r+1}$. As recalled in Proposition 3.5, every v-ordering of a Legendre set S is very well distributed in S. So, for each x in S, there exists a unique s such that $0 \leq s < q_{r+1}$ and $x \equiv a_s\ [\mathfrak{M}^{r+1}]$. We have to prove that

$$\overline{e}_r(x) = \overline{e}_r(a_s).$$

First suppose that $s \geq q_r$.

$$\forall i \in \{0, \ldots, q_r - 1\}, \frac{x - a_i}{a_s - a_i} = 1 + \frac{x - a_s}{a_s - a_i}.$$

As $v(x - a_s) \geq r + 1$ and $v(a_s - a_i) < r + 1$, we have

$$\frac{x - a_s}{a_s - a_i} \equiv 0\ [\mathfrak{M}] \text{ and } \prod_{0\leq i\leq q_r-1} \frac{x - a_i}{a_s - a_i} \equiv 1\ [\mathfrak{M}].$$

To conclude, write

$$e_r(x) = e_r(a_s) \times \prod_{0\leq i<q_r} \frac{x - a_i}{a_s - a_i}.$$

Then $e_r(x) \equiv e_r(a_s)\ [\mathfrak{M}]$.

Suppose now that $s < q_r$. Then $\overline{e}_r(a_s) = 0$. If we suppose that

$$v(\prod_{0\le i<q_r}(x-a_i)) = v(\prod_{0\le i<q_r}(a_{q_r}-a_i)),$$

then x could replace a_{q_r} in a v-ordering. Meanwhile, we could construct a new v-ordering

$$a_0,\dots,a_{q_r-1},x,b_{q_r+1},\dots,b_{q_{r+1}-1},\dots$$

Since a v-ordering must be a very well distributed sequence,

$$a_0,\dots,a_{q_r-1},x,b_{q_r+1},\dots,b_{q_{r+1}-1}$$

must be a complete set of residues modulo $\mathfrak{M}^{r+1}$. This is impossible, since $v(x-a_s)\ge r+1$. So

$$v(\prod_{0\le i<q_r}(x-a_i)) > v(\prod_{0\le i<q_r}(a_{q_r}-a_i)) \text{ and } \overline{e}_r(x)=0.$$

We now prove by induction on r that the ϕ_r's are injective. It is equivalent to prove that

$$\Phi_r(x)=\Phi_r(y) \Rightarrow x\equiv y \pmod{\mathfrak{M}^{r+1}},$$

where the map Φ_r is

$$\Phi_r : \begin{cases} S & \to & k^{r+1} \\ x & \mapsto & (\overline{e}_0(x),\dots,\overline{e}_r(x)) \end{cases}$$

Since $\overline{e}_0(X)=X$, clearly $\overline{e}_0(x)=\overline{e}_0(y)$ implies $x\equiv y \pmod{\mathfrak{M}}$, so ϕ_0 is injective. We then suppose that ϕ_{r-1} is injective. If $x\not\equiv y \pmod{\mathfrak{M}^r}$, it follows by induction that $\Phi_{r-1}(x)\neq\Phi_{r-1}(y)$ and then $\Phi_r(x)\neq\Phi_r(y)$. Thus we may assume that x and y are both in the class of some a_j $(j<q_r)$ modulo $\mathfrak{M}^r$:

$$x=a_j+b\pi^r \text{ and } y=a_j+c\pi^r, \text{ with } b,c\in V.$$

Considering the classes of b and c in $S/\mathfrak{M}$, we show that $\overline{b}\neq\overline{c}$ implies $\overline{e}_r(x)\neq\overline{e}_r(y)$.

1) We first note that, for $\overline{b}\neq 0$, $\overline{e}_r(x)\neq 0$.

Indeed, $a_0,\dots,a_{q_r-1},x$ are then in distinct classes modulo $\mathfrak{M}^{r+1}$. They thus form the beginning of a very well distributed sequence and hence, this sequence is a v-ordering. Then

$$v(\prod_{0\le i<q_r}(a_{q_r}-a_i)) = v(\prod_{0\le i<q_r}(x-a_i)).$$

Then $v(e_r(x))=0$, and $\overline{e}_r(x)\neq 0$.

If $\overline{c}=0$, as $\overline{e}_r$ is constant on cosets modulo $\mathfrak{M}^{r+1}$, $\overline{e}_r(y)=\overline{e}_r(a_j)=0$, and then $\overline{e}_r(y)\neq\overline{e}_r(x)$. Similarly, if $\overline{b}=0$, $\overline{c}\neq 0$, we have again $\overline{e}_r(y)=0$ and

$\overline{e}_r(x) \neq 0$.

2) Now we suppose that $\overline{b} \neq 0$, $\overline{c} \neq 0$, then $\overline{e}_r(x) \neq 0$, $\overline{e}_r(y) \neq 0$.

$$\frac{e_r(x)}{e_r(y)} = \frac{x-a_j}{y-a_j} \times \prod_{0 \leq k < q_r, k \neq j} \frac{x-a_k}{y-a_k}$$

For $k \neq j$, we have

$$\frac{x-a_k}{y-a_k} = 1 + \frac{x-y}{y-a_k}.$$

As $v(x-y) = r$ and $v(y-a_k) < r$, hence $\frac{x-y}{y-a_k}$ is in V and

$$\frac{x-a_k}{y-a_k} \equiv 1 \pmod{\mathfrak{M}}.$$

On the other hand,

$$\frac{x-a_j}{y-a_j} = \frac{b}{c}.$$

As V is local and $c \notin \mathfrak{M}$, $\frac{b}{c}$ is an element of V, thus so is $\frac{e_r(x)}{e_r(y)}$ and

$$\frac{e_r(x)}{e_r(y)} \equiv \frac{b}{c} \pmod{\mathfrak{M}}.$$

Now, $\overline{b} \neq \overline{c}$ implies $\frac{\overline{b}}{\overline{c}} \neq 1$, hence $\frac{\overline{e}_r(x)}{\overline{e}_r(y)} \neq 1$, that is $\overline{e}_r(x) \neq \overline{e}_r(y)$. □

References

[1] Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964) 117-180.

[2] Y. Amice, *Les nombres p-adiques*, Presses Universitaires de France, Paris (1975).

[3] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.* **490** (1997), 101-127.

[4] M. Bhargava, K.S. Kedlaya, Continuous functions on compact subsets of local fields, *Acta Arith.* **91** (1999), 191-198.

[5] P.J. Cahen, J.L. Chabert, *Integer-valued polynomials*, Mathematical Survey and Monographs, vol **48**, *Amer. Math. Soc.*, Providence (1997).

[6] K. Conrad, The digit principle, *J. Number Theory* **84** (2000), 230-257.

[7] S. Evrard, Y Fares, p-adic subsets whose factorials satisfy a generalized Legendre formula, *Bull.London Math. Soc.*,**40** (2008), 3750.

[8] A.M. Robert, *A course in p-adic analysis*, **198** Springer (2000).

[9] J.F Voloch, Differential operators and interpolation series in power series field, *J. Number Theory* **71**(1998), 106-108.

LAMFA CNRS UMR 6140 Université de Picardie, 80039 Amiens, France

E-mail address: sabine.evrard@u-picardie.fr