Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

p-ADIC SUBSETS WHOSE FACTORIALS SATISFY A GENERALIZED LEGENDRE FORMULA

SABINE EVRARD AND YOUSSEF FARES

To Hamadi Fares

Abstract

Amice studied the notion of a regular compact subset in a local field K, with valuation v and maximal ideal $\mathfrak{M}$. In her work, she introduced the notion of well distributed sequences and showed that every regular compact subset S admits well distributed sequences and that its factorial sequence $(n!_S)$ satisfies a generalized Legendre formula:

$$v(n!_S) = \sum_{i=1}^{i=\infty} \left[\frac{n}{q_i} \right]$$

for every integer n and where q_i denotes the number of classes of S modulo $\mathfrak{M}^i$.

In this article, in more general settings, we show the converse assertions. More precisely, we prove that, for every precompact subset of any discrete valuation domain V, the following assertions are equivalent:
(1) the topological closure of S is a regular subset,
(2) S admits a very well distributed sequence,
(3) S satisfies the generalized Legendre formula.

1. *Introduction*

Let p be a prime number and denote by $v_p(l)$ the highest power of p dividing l. For every $n \geq 1$, we have the Legendre formula:

$$v_p(n!) = \sum_{k \geq 1} \left[\frac{n}{p^k} \right]$$

where $[x]$ denotes the integer part of x. Using the notion of v-ordering, the factorials were generalized by Barghava [**3**]. He associated to any subset S of $\mathbb{Z}$ and more generally, of a Dedekind domain D, a sequence of ideals of D, denoted by $(n!_S)_{n\in\mathbb{N}}$, which preserves the classical arithmetical properties of factorials. In this article, we study what we call Legendre sets: Subsets S of a discrete valuation domain V, with maximal ideal $\mathfrak{M}$, whose factorial sequence $(n!_S)_{n\in\mathbb{N}}$ satisfies the (similar) Legendre formula,

$$\forall n \in \mathbb{N},\ v(n!_S) = \sum_{i=1}^{i=\infty} \left[\frac{n}{q_i} \right],$$

where q_i denotes the number of classes of S modulo $\mathfrak{M}^i$. Pólya [**9**] had already showed such a formula, for every discrete valuation ring V with finite residue field of cardinality q:

$$v(n!_V) = \sum_{k \geq 1} \left[\frac{n}{q^k} \right].$$

Y. Amice [**1**] studied a class of subsets that she called regular compact subsets and these subsets satisfy the generalized Legendre formula. We recall her work in section 4.

2000 *Mathematics Subject Classification* (primary)11B65,11B50, (secondary)13F20 .

The aim of this article is to characterize the Legendre sets. Our main result is Theorem 6.2 which establishes links between sets admitting very well distributed sequences, regular precompact subsets and Legendre sets: for every precompact subset of any discrete valuation domain V, the following assertions are equivalent:

(1) The topological closure of S is a regular subset,
(2) S admits a very well distributed sequence,
(3) S satisfies the generalized Legendre formula.
(4) Every v-ordering of S is a very well distributed sequence.

Generalizing the notion of very well distributed and well ordered sequences, as studied by P.J. Cahen and J.L. Chabert [**5**], we also prove that Legendre sets admit such a sequence. We end with some examples of Legendre sets.

2. *The characteristic sequence and the v-orderings*

Hypothesis and notation. In the whole article, we consider a discrete valuation ring V, with valuation v, quotient field K, maximal ideal $\mathfrak{M}$, and residue field $k = V/\mathfrak{M}$. We denote by S an infinite subset of V.
For every fractional ideal $\mathfrak{I}$ of V, denote by $v(\mathfrak{I})$ the valuation of $\mathfrak{I}$, that is,

$$v(\mathfrak{I}) = \inf\{v(x) | x \in \mathfrak{I}\}.$$

Definition 1. [**2**] A *v-ordering of S* is a sequence $(a_n)_{n\geq 0}$ of elements of S such that, for every $n > 0$,

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

As V is a discrete valuation ring, every subset of V admits a v-ordering and we have the following property:

Proposition 2.1. *([**2**])The sequence $(w_S(n))_{n\in\mathbb{N}}$ defined by*

$$w_S(n) = \sum_{k=0}^{n-1} v(a_n - a_k),$$

where the sequence $(a_n)_{n\geq 0}$ is a v-ordering of S, does not depend on the choice of the sequence $(a_n)_{n\geq 0}$.

To prove Proposition 2.1, it suffices to show the link between v-orderings and integer-valued polynomials. Recall that *the ring of integer-valued polynomials on S* is

$$\mathrm{Int}(S, V) = \{f \in K[X] | f(S) \subseteq V\}.$$

Definition 2. [**5**] For each $n \in \mathbb{N}$, *the characteristic ideal of index n* (of the ring $\mathrm{Int}(S, V)$) is the set $\mathfrak{I}_n(S, V)$ formed by the leading coefficients of the polynomials in

$$\mathrm{Int}_n(S, V) = \{f \in \mathrm{Int}(S, V) | \deg f \leq n\}.$$

As $\mathrm{card}(S)$ is infinite, all the $\mathfrak{I}_n(S, V)$ are fractional ideals.

Definition 3. For each $n \in \mathbb{N}$, *the factorial ideal* of index n is the inverse ideal $n!_S$ of the fractional ideal $\mathfrak{I}_n(S, V)$, that is

$$n!_S = \mathfrak{I}_n(S, V)^{-1} = \{x \in K \mid x\mathfrak{I}_n(S, V) \subseteq V\}.$$

Moreover, one can easily see that ([**5**]) :

$$n!_S = \{x \in K | xInt_n(S,V) \subseteq V[X]\}.$$

We have the following lemma:

LEMMA 2.2. *Let $(a_n)_{n\geq 0}$ be a sequence of distinct elements of S and $(f_n)_{n\geq 0}$ be the sequence of polynomials defined by*

$$f_n(X) = \prod_{i=0}^{n-1} \frac{X - a_i}{a_n - a_i}.$$

The sequence $(a_n)_{0\leq k\leq n}$ is a v-ordering of S if and only if the sequence $(f_k)_{0\leq k\leq n}$ is a basis of the V-module $Int_n(S,V)$.

We then get the independency seen in Proposition 2.1: $w_S(n) = v(n!_S)$.

DEFINITION 4. The sequence $(w_S(n))_{n\in\mathbb{N}}$, which is also $(v(n!_S))_{n\in\mathbb{N}}$, is called *the characteristic sequence of S*.

Suppose that S is a precompact subset of V. Then, we know that every set $S/\mathfrak{M}^s$ (the set of classes of S modulo $\mathfrak{M}^s$) is finite. Denote by q_s the number of classes of S modulo $\mathfrak{M}^s$.

DEFINITION 5. A precompact subset S of V is called a *Legendre set* if its characteristic sequence satisfies the following Legendre formula:

$$\forall n \in \mathbb{N},\ v(n!_S) = \sum_{i=1}^{i=\infty} \left[\frac{n}{q_i}\right].$$

For example, when the residue field k is finite of cardinality q, V is a Legendre set and $q_s = q^s$.

Notation. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of S. For each $x \in S$, $n \in \mathbb{N}^*, r \in \mathbb{N}$, let
(1) $D(x,n,r) = \{a_k \mid 0 \leq k < n,\ v(x - a_k) \geq r\}$
and, when $x = a_n$, $D(n,r) = D(a_n,n,r)$;
(2) $C(x,n,r) = \{a_k \mid 0 \leq k < n,\ v(x - a_k) = r\}$
and, when $x = a_n$, $C(n,r) = C(a_n,n,r)$
(3) $d(x,n,r) = |D(x,n,r)|$; $c(x,n,r) = |C(x,n,r)|$
$d(n,r) = |D(n,r)|$; $c(n,r) = |C(n,r)|$.
One can see these subsets as the intersection of a ball or a sphere and the n first terms of the sequence $(a_n)_{n\in\mathbb{N}}$. We then have the following lemma:

LEMMA 2.3.

$$v(\prod_{k=0}^{n-1}(x - a_k)) = \sum_{s\geq 1} d(x,n,s)$$

Proof. If x is one of the a_k, $0 \leq k < n$, it's obvious. Otherwise, we have:

$$v(\prod_{k=0}^{n-1}(x - a_k)) = \sum_{s\geq 0} s \cdot c(x,n,s)$$

$$= \sum_{s\geq 0} s(d(x,n,s) - d(x,n,s+1)) = \sum_{s\geq 1} d(x,n,s)$$

□

3. *Well distributed sequences*

We give definitions and properties which extend those given by J. Yeramian in [**10**] when $S = V$ and which were introduced in more general settings by Y. Amice in [**1**]. We generalize their work by proving that, in fact, such very well distributed sequences characterize regular compact subsets. In this section, S is supposed to be precompact and we denote by q_s the number of classes of $S/\mathfrak{M}^s$.

DEFINITION 6. Let $(a_n)_{n\geq 0}$ be a sequence of elements of S.

(i) The sequence is said to be *a very well distributed sequence of* S if, for every $s > 0$ and every $\lambda \in \mathbb{N}$, $(a_{\lambda q_s}, \cdots, a_{(\lambda+1)q_s-1})$ is a complete set of residues of $S/\mathfrak{M}^s$.

(ii) The sequence is said to be *a well distributed sequence of order* r *of* S if, for every $1 \leq s \leq r$ and every $\lambda \in \mathbb{N}$, $(a_{\lambda q_s}, \cdots, a_{(\lambda+1)q_s-1})$ is a complete set of residues of $S/\mathfrak{M}^s$.

(iii) The sequence is said to be *a well distributed sequence of order* r *and length* N *of* S if, for every $1 \leq s \leq r$ and every $\lambda \in \mathbb{N}$, such that $(\lambda+1)q_s \leq N$, $(a_{\lambda q_s}, \cdots, a_{(\lambda+1)q_s-1})$ is a complete set of residues of $S/\mathfrak{M}^s$, and the remaining terms $a_{[\frac{N}{q_s}]q_s}, \cdots, a_{N-1}$ are non congruent modulo $\mathfrak{M}^s$.

REMARK 1.

(i) If (a_n) is well distributed of order r and length N, then, for every $s \leq r$ and every $n \leq N$, there are $\left[\frac{n}{q_s}\right]$ complete sets of residues of $S/\mathfrak{M}^s$ in $(a_0, \cdots, a_{n-1})$.

(ii) A sequence of elements of S is a very well distributed sequence if and only if it is a well distributed sequence of order r, for every r.

The following obvious lemma will be very useful:

LEMMA 3.1. *A sequence* $(a_n)_{n\in\mathbb{N}}$ *of elements of* S *is a well distributed sequence of order* r *and length* N *if and only if for every* $1 \leq s \leq r$*, and every* $0 \leq m < n < N$ *one has*

$$\left[\frac{n}{q_s}\right] = \left[\frac{m}{q_s}\right] \Rightarrow v(a_n - a_m) < s.$$

LEMMA 3.2. *Let* $(a_n)_{n\in\mathbb{N}}$ *be a sequence of elements of* S *which is well distributed of order* r *and length* N*. Let* $n < N$*. One has:*

(i) *for* $s \leq r$, $d(n,s) = \left[\frac{n}{q_s}\right]$,

(ii) *for* $s \leq r-1$, $c(n,s) = \left[\frac{n}{q_s}\right] - \left[\frac{n}{q_{s+1}}\right]$,

(iii) *if* $N \leq q_r$*, then*

$$v(\prod_{i=0}^{n-1}(a_n - a_i)) = \sum_{s\geq 1}\left[\frac{n}{q_s}\right].$$

Proof. (1) In the sequence $(a_0, \cdots, a_{n-1})$, there are $\lambda = \left[\frac{n}{q_s}\right]$ complete sets of residues of $S/\mathfrak{M}^s$, so there are exactly λ elements a_i which satisfy $v(a_n - a_i) \geq s$ in the sequence $(a_0, \cdots, a_{\lambda q_s - 1})$. Moreover, as $(a_{\lambda q_s}, \cdots, a_n)$ is the beginning of a new complete set of residues of $S/\mathfrak{M}^s$, there is no other element congruent to a_n.
(2) is obvious.
(3) If $N \leq q_r$, we know that $a_0, \cdots, a_n$ are not congruent modulo $\mathfrak{M}^r$, and thus $d(n,s) = 0$ for

$s \geq r$. Using Lemma 2.3 and (1), we have:

$$v(\prod_{i=0}^{n-1}(a_n - a_i)) = \sum_{s\geq 1} d(n,s) = \sum_{s=1}^{r-1} d(n,s) = \sum_{s\geq 1}\left[\frac{n}{q_s}\right].$$

□

As a consequence:

PROPOSITION 3.3. *Let $(a_n)_{n\in\mathbb{N}}$ be a very well distributed sequence of S. Then, for every $n \geq 1$,*

$$v(\prod_{i=0}^{n-1}(a_n - a_i)) = \sum_{s\geq 1}\left[\frac{n}{q_s}\right].$$

Recall that we want to compute the characteristic sequence of a subset S. We have seen that the sequence $(v(n!_S))$ is linked with the v-orderings of the subsets. That is why the following proposition is particulary interesting:

PROPOSITION 3.4. *A very well distributed sequence of S is a v-ordering of S.*

Proof. Let $(a_n)_{n\in\mathbb{N}}$ be a very well distributed sequence of S. Let $n \in \mathbb{N}$, thanks to Proposition 3.3, one has

$$v(\prod_{i=0}^{n-1}(a_n - a_i)) = \sum_{s\geq 1}\left[\frac{n}{q_s}\right].$$

Let $x \in S$ and $s \in \mathbb{N}^*$. In $(a_0, \cdots, a_{n-1})$, there are $[\frac{n}{q_s}]$ complete sets of residues of $S/\mathfrak{M}^s$: x is congruent modulo $\mathfrak{M}^s$ with at least $[\frac{n}{q_s}]$ elements in $(a_0, \cdots, a_{n-1})$.

$$d(x,n,s) \geq [\frac{n}{q_s}]$$

$$v(\prod_{k=0}^{n-1}(x - a_k)) = \sum_{s\geq 1} d(x,n,s) \geq \sum_{s\geq 1}\left[\frac{n}{q_s}\right].$$

Hence,

$$v(n!_S) = \inf_{x\in S} v(\prod_{k=0}^{n-1}(x - a_k)) = \sum_{s\geq 1}\left[\frac{n}{q_s}\right] = v(\prod_{k=0}^{n-1}(a_n - a_k)).$$

By induction, if we suppose that $(a_0, \cdots, a_{n-1})$ is a v-ordering, we then obtain that $(a_0, \cdots, a_n)$ is a v-ordering. □

Thus we have:

PROPOSITION 3.5. *If the subset S of V admits a very well distributed sequence, then S is a Legendre set.*

The question is to find subsets admitting very well distributed sequences. The next section gives an example of such subsets.

4. *Regular precompact sets*

For $x \in S$ and $r \in \mathbb{N}^*$, let

$$B(x,r) = \{y \in S \mid v(x-y) \geq r\},$$

and denote by $|B(x,r)/\mathfrak{M}^{r+1}|$ the cardinality of the set $B(x,r)/\mathfrak{M}^{r+1}$. It is obvious that for all $x, x' \in V$, $B(x,r)/\mathfrak{M}^{r+1} = B(x',r)/\mathfrak{M}^{r+1}$ if and only if $x \equiv x' \pmod{\mathfrak{M}^{r+1}}$.

Definition 7. A subset S of V is said to be *regular* if, for every $r \in \mathbb{N}^*$, there exists α_r such that, for every x of S, the ball $B(x,r)$ is a disjoint union of α_r balls $B(z,r+1)$, with $z \in S$.

This definition generalizes the Amice's definition of a regular compact subset, introduced in local fields [**1**]. We can also see immediatly that for a precompact subset S, the following assertions are equivalent:

(1) $\forall r \in \mathbb{N}^*, \forall (x,y) \in S^2, |B(x,r)/\mathfrak{M}^{r+1}| = |B(y,r)/\mathfrak{M}^{r+1}|$.
(2) the subset S is regular.

In particular, for a regular precompact subset, one has:

$$\forall r \in \mathbb{N}^*, q_{r+1} = \alpha_r q_r,$$

where α_r is the number of disjoint balls $B(z_k, r+1)$ in S.

Proposition 4.1. *If S is a regular precompact subset of V, then it admits a very well distributed sequence, and hence, is a Legendre subset.*

Proof. We construct by induction on $r \in \mathbb{N}$ a sequence $(a_n)_{n\in\mathbb{N}}$ which is well distributed of order r and length q_r. Obviously, a complete set of residues of $S/\mathfrak{M}$ is well distributed of order 1 and length q_1. Suppose now that the sequence $(a_0, \cdots, a_{q_r-1})$ is well distributed of order r. For every $0 \leq j \leq q_r - 1$, denote by $b_{j,0}, \cdots b_{j,\alpha_r-1}$ a complete set of residues of $B(a_j,r)/\mathfrak{M}^{r+1}$, where $b_{j,0} = a_j$. For every m such that $q_r \leq m < q_{r+1}$, write $m = kq_r + l$, where $k \geq 1$ and $0 \leq l < q_r$. We put $a_m = b_{l,k}$ and prove that $(a_0, \cdots, a_{q_{r+1}-1})$ is a well distributed sequence of order $r+1$ and length q_{r+1}. First, by construction, $(a_0, \cdots, a_{q_{r+1}-1})$ is a complete set of residues of $S/\mathfrak{M}^{r+1}$. Let $1 \leq s \leq r$ and $m < n < q_{r+1}$ be such that $[\frac{m}{q_s}] = [\frac{n}{q_s}]$. Using the divisibility of the q_n by q_s, we have $[\frac{m}{q_r}] = [\frac{n}{q_r}]$. Then we can write $m = kq_r + l$ and $n = kq_r + l'$ where $0 \leq k \leq \alpha_r - 1$ and $0 \leq l, l' < q_r$. Hence

$$v(a_m - a_n) = v(b_{l,k} - b_{l',k}) = v(a_l - a_{l'}).$$

As $m \neq n$, we have $l \neq l'$ and, by induction hypothesis, $v(a_m - a_n) < s$.
The sequence constructed is a very well distributed sequence, as it is well distributed of order r and length q_r for every $r \geq 0$. □

5. *Subsets admitting a well distributed sequence*

In this section, S is an infinite precompact subset and $q_r = |S/\mathfrak{M}^r|$.

Proposition 5.1. *If a subset S of V admits a well distributed sequence $(a_n)_{n\in\mathbb{N}}$ of order r and length $N \geq 2q_r$, then for every $1 \leq s \leq r$, one has*

$$q_{s-1} | q_s.$$

Proof. Let $1 \leq s \leq r$. In $(a_0, \cdots, a_{2q_s-1})$ there are 2 complete sets of residues of $S/\mathfrak{M}^s$. Hence, for every $x \in S$,

$$\begin{array}{l} |B(x, s-1)/\mathfrak{M}^s| = \\ \text{card}\,\{a_i \mid 0 \leq i < q_s,\ v(x-a_i) \geq s-1\} = \\ \text{card}\,\{a_i \mid q_s \leq i < 2q_s,\ v(x-a_i) \geq s-1\} \end{array}$$

Hence $\text{card}\,\{a_i \mid 0 \leq i < 2q_s,\ v(x-a_i) \geq s-1\}$ is even. Suppose that q_{s-1} does not divide q_s. Then there exists (at least) one element x in S such that $\text{card}\,\{a_i \mid 0 \leq i < 2q_s,\ v(x-a_i) \geq s-1\}$ is odd. That is impossible.

□

COROLLARY 5.2. *If the subset S admits a very well distributed sequence then, for every r, q_r divides q_{r+1}.*

REMARK 2. The condition on the length in Proposition 5.1 is sharp, since, for example, the set $S = \{\pi^n, n \geq 1\} \bigcup \{0\}$, where π is a generator of $\mathfrak{M}$, is such that q_2 does not divide q_3, and we can find a v-ordering which is well distributed of order 2 and length $3 = 2q_2 - 1$, whereas it is not well distributed of order 2 and length $4 = 2q_2$. For this set S, we have $q_r = r$ and the sequence defined by $u_0 = 0$ and $u_n = \pi^n$ is a v-ordering of S. One has

- $\{0\}$ is a complete set of residues of $S/\mathfrak{M}$,
- $\{0, \pi\}$ is a complete set of residues of $S/\mathfrak{M}^2$,
- $\{0, \pi, \pi^2\}$ is a complete set of residues of $S/\mathfrak{M}^3$,
- $\{0, \pi, \pi^2, \pi^3\}$ is a complete set of residues of $S/\mathfrak{M}^4$.

In $\{0, \pi, \pi^2, \pi^3\}$, there is only one complete set of residues of $S/\mathfrak{M}^2$, and that prove that this sequence is not a well distributed sequence of order 2 and length 4.

PROPOSITION 5.3. *The precompact subset S admits a very well distributed sequence if and only if it is a regular precompact subset.*

Proof. Let (a_n) be a very well distributed sequence of S, Corollary 5.2 shows that for every r, q_r divides q_{r+1}. Let $q_{r+1} = \alpha_r q_r$. As (a_n) is a very well distributed sequence, we know that $(a_0, \cdots, a_{q_{r+1}-1})$ is a complete set of residues of $S/\mathfrak{M}^{r+1}$ and there are exactly α_r complete sets of residues of $S/\mathfrak{M}^r$ in $(a_0, \cdots, a_{q_{r+1}-1})$. Hence, for every x of S, one has

$$|B(x, r)/\mathfrak{M}^{r+1}| = \alpha_r.$$

The converse has already be seen in Proposition 4.1. □

Each regular precompact subset is a Legendre subset. We now study the converse.

6. *Characterization of the Legendre subsets*

In this section, S is an infinite precompact subset and $q_r = |S/\mathfrak{M}^r|$.

PROPOSITION 6.1. *Let S be a precompact subset, and suppose that there exist N, r such that for every $n \leq N < q_{r+1}$, one has*

$$v(n!_S) = \sum_{s \geq 1} \left[\frac{n}{q_s} \right],$$

then every v-ordering of S is a well distributed sequence of order $r+1$ and length $N+1$.

Proof. Suppose that there exists a v-ordering $(a_n)_{n\in\mathbb{N}}$ of S which is not well distributed of order $r+1$ and length $N+1$ ($N \geq 1$). Let t be such that (a_n) is well distributed of order t and length q_t but it is not well distributed of order $t+1$ and length q_{t+1} $(1 \leq t \leq r)$.Then, denote by i the least integer such that (a_n) is not well distributed of order $t+1$ and length $i+1$ ($q_t \leq i < q_{t+1}$) and by s the least integer such that (a_n) is not well distributed of order s and length $i+1$ $(1 \leq s \leq t+1)$. By Lemma 3.1, there exists $j < i$ such that

$$\left[\frac{i}{q_s}\right] = \left[\frac{j}{q_s}\right] \text{ and } v(a_i - a_j) \geq s.$$

Since (a_n) is a v-ordering, we have:

$$v(i!_S) = v\left(\prod_{k=0}^{i-1}(a_i - a_k)\right) = \sum_{l\geq 1} d(i,l),$$

with $d(i,l) = \operatorname{card}\{a_k \mid 0 \leq k < i,\, v(a_i - a_k) \geq l\}$. By definition of i, the sequence (a_n) is well distributed of order $t+1$ and length i. So, for $l \leq t+1$, in $(a_0, \cdots, a_{i-1})$, there are $\left[\frac{i}{q_l}\right]$ complete sets of residues modulo $\mathfrak{M}^l$, and hence

$$d(i,l) \geq \left[\frac{i}{q_l}\right].$$

Let us look in particular to $d(i,s)$. Writing $\lambda = \left[\frac{i}{q_s}\right]$, we have:

$$\lambda q_s - 1 < j < i < \lambda(q_s + 1).$$

Consequently, $D(i,s)$ contains a_j while a_j is not in $(a_0, \cdots, a_{\lambda q_s - 1})$. Hence

$$d(i,s) \geq \left[\frac{i}{q_s}\right] + 1$$

and

$$v(i!_S) = \sum_{l\geq 1} d(i,l) \geq 1 + \sum_{l=1}^{t}\left[\frac{i}{q_l}\right]$$

This inequality contradicts the hypothesis. □

Now, we are able to state our main theorem.

THEOREM 6.2. *For a precompact subset S of V, the following assertions are equivalent:*
(i) *S is a Legendre subset.*
(ii) *S admits a very well distributed sequence.*
(iii) *S is regular subset.*
(iv) *Every v-ordering of S is a very well distributed sequence.*

Proof. Proposition 5.3 shows (2)⇔ (3). It is obvious that (4)⇒ (2) and Proposition 3.5 shows that (2)⇒(1). Finally, it follows from Proposition 6.1 that (1)⇒(4). □

EXAMPLE 1. Suppose that the residue field k is finite of cardinality q.
(i) Let $S = V^\times$, then S is a Legendre subset and for every $r \in \mathbb{N}^*$, one has $q_r = (q-1)q^{r-1}$.
(ii) Let E and F be subsets of V such that $E \subset F$ and E is dense in F, then F is a Legendre set if and only if E is a Legendre set.

Assertion (2) follows from the following lemma.

LEMMA 6.3. *([7], [6])Let E and F be subsets of a discrete valuation ring V with finite residue field. Assume that $E \subset F$. Then E is dense in F if and only if*

$$E/\mathfrak{M}^r = F/\mathfrak{M}^r, \forall r \in \mathbb{N}^*.$$

7. *Another characterization of Legendre subsets*

In this section we suppose that the characteristic sequence of the subset S satisfies a formula like the Legendre one, but without assuming that the integers (l_r) involved in the formula denote the cardinality of the sets $S/\mathfrak{M}^r$.

PROPOSITION 7.1. *Let S be an infinite subset of V satisfying:*

$$\forall n \in \mathbb{N},\ v(n!_S) = \sum_{i=1}^{i=\infty} \left[\frac{n}{l_i}\right]$$

where $(l_r)_{r\in\mathbb{N}}$ is a sequence of integers such that l_r divides l_{r+1} for every r. Then S is a Legendre set and $q_r = l_r$.

Proof. Let (a_n) be a v-ordering of S. We show by induction on r that $l_r = q_r$. One has $v(\prod_{i=0}^{n-1}(a_n - a_i)) = 0$ for $n < l_1$. So $a_0, \cdots, a_{l_1-1}$ are not congruent modulo $\mathfrak{M}$ and $l_1 \leq q_1$. Moreover, $v(\prod_{i=0}^{l_1-1}(a_{l_1} - a_i) = 1$, thus:

$$\forall x \in S, v(\prod_{i=0}^{l_1-1}(x - a_i)) \geq 1.$$

That proves that each x is congruent modulo $\mathfrak{M}$ to some $a_0, \cdots, a_{l_1-1}$. Hence

$$q_1 = l_1.$$

Suppose now that

$$\forall s \leq r, l_s = q_s$$

Thanks to the formulation of Proposition 6.1, we know that the sequence $(a_n)_{n\in\mathbb{N}}$ is a well distributed sequence of order $r+1$ and length $\inf(l_{r+1}, q_{r+1})$. We have to prove that $l_{r+1} = q_{r+1}$. Suppose first that $q_{r+1} > l_{r+1}$. Then $(a_n)_{n\in\mathbb{N}}$ is well distributed of order $r+1$ and length l_{r+1}. Consequently, for $s \leq r+1$, there are exactly $\left[\frac{l_{r+1}}{q_s}\right]$ complete sets of residues of S, modulo $\mathfrak{M}^s$ in $(a_0, \cdots, a_{l_{r+1}-1})$, and hence, due to the divisibility of the l_s's, for $s \leq r$ and for each x in S one has:

$$d(x, l_{r+1}, s) = \left[\frac{l_{r+1}}{q_s}\right].$$

Since $q_{r+1} > l_{r+1}$, there is an element x of S which is non congruent modulo $\mathfrak{M}^{r+1}$ with $a_0, \cdots, a_{l_{r+1}-1}$. For such an x, we have:

$$v(\prod_{k=0}^{l_{r+1}-1}(x - a_k)) = \sum_{s=1}^{r}\left[\frac{l_{r+1}}{q_s}\right],$$

whereas

$$v(\prod_{k=0}^{l_{r+1}-1}(a_{l_{r+1}} - a_k)) = \sum_{s=1}^{r+1}\left[\frac{l_{r+1}}{q_s}\right] = \sum_{s=1}^{r}\left[\frac{l_{r+1}}{q_s}\right] + 1.$$

That is impossible, since, by definition of a v-ordering, $a_{l_{r+1}}$ minimizes this valuation. Suppose now that $q_{r+1} < l_{r+1}$. Since the sequence $a_0, \cdots, a_{q_{r+1}}$ is a v-ordering, one has

$$v(q_{r+1}!_S) = \sum_{s\geq 1} \left[\frac{q_{r+1}}{l_s}\right] = \sum_{s=1}^{r} \left[\frac{q_{r+1}}{l_s}\right].$$

As (a_n) is a well distributed sequence of order $r+1$ and length q_{r+1}, for $s \leq r$ one has:

$$d(q_{r+1}, s) = \left[\frac{q_{r+1}}{q_s}\right],$$

and $a_{q_{r+1}}$ is congruent modulo $\mathfrak{M}^{r+1}$ to one of the $a_0, \cdots, a_{q_{r+1}-1}$. So

$$d(q_{r+1}, r+1) \geq 1$$

and

$$v(q_{r+1}!_S) \geq \sum_{s=0}^{r} \left[\frac{q_{r+1}}{l_s}\right] + 1.$$

That is impossible. Hence, for every i, we have $q_i = l_i$. □

Example 2. Let E be a Legendre set. If a subset F of V is such that for every n, one has $n!_F = n!_E$, then F is a Legendre set.

8. *Very well distributed and well ordered sequences*

We first recall a definition given in the case where the residue field k of V is finite of cardinality q.

Definition 8. [**8**] A sequence $(a_n)_{n\in\mathbb{N}}$ of elements of V is said to be *very well distributed and well ordered* of S if, for every integers n and m,

$$v(a_n - a_m) = v_q(n-m),$$

where $v_q(n)$ denotes the largest power of q dividing n.

One can easily see that every very well distributed and well ordered sequence $(a_n)_{n\in\mathbb{N}}$ is a v-ordering and moreover, for every k, the sequence $(a_{n+k})_{n\in\mathbb{N}}$ is also a v-ordering. We then generalize this definition to subsets S of V:

Definition 9. A sequence $(a_n)_{n\in\mathbb{N}}$ of elements of S is said to be *very well distributed and well ordered* of S if, for every $k \in \mathbb{N}$, the sequence $(a_{n+k})_{n\in\mathbb{N}}$ is a v-ordering of S.

Proposition 8.1. *Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of elements of S. The following assertions are equivalent:*

(i) *The sequence $(a_n)_{n\in\mathbb{N}}$ is a very well distributed and well ordered sequence of S,*
(ii) *the sequence $(a_n)_{n\in\mathbb{N}}$ is a v-ordering of S and for every $n, r \in \mathbb{N}$,*

$$v(a_{n+r} - a_n) = v(a_r - a_0),$$

(iii) *for every $n, r \in \mathbb{N}$, $v(a_{n+r} - a_n) = w_S(r) - w_S(r-1)$.*

Proof. Let $(a_n)_{n\in\mathbb{N}}$ be a v-ordering of S. If $v(a_{n+r} - a_n) = v(a_{m+r} - a_m)$, for every $n, m, r \in \mathbb{N}$, then, for every $k \in \mathbb{N}$, the sequence $(a_{n+k})_{n\in\mathbb{N}}$ is a v-ordering of S, and we get (2)⇒ (1). We now prove that (1)⇒ (3) and suppose that for every $k \in \mathbb{N}$, the sequence $(a_{n+k})_{n\in\mathbb{N}}$ is a v-ordering of S. Put $w_S(0) = 0$. We prove by induction on $r \in \mathbb{N}^*$ that for every $n \in \mathbb{N}$, one

has: $v(a_{n+r} - a_n) = w_S(r) - w_S(r-1)$.
For $r = 1$, the sequence $(a_{n+1})_{n\in\mathbb{N}}$ is a v-ordering so

$$v(a_{n+1} - a_n) = w_S(1) - w_S(0).$$

For $r \in \mathbb{N}^*$, suppose that $v(a_{n+k} - a_n) = w_S(k) - w_S(k-1)$ for every $1 \leq k \leq r$ and every $n \in \mathbb{N}$. One has

$$v(a_{n+r+1} - a_n) = v(\prod_{k=0}^{k=r}(a_{n+r+1} - a_{n+k})) - v(\prod_{k=1}^{k=r}(a_{n+r+1} - a_{n+k})).$$

Using induction hypothesis, for every $1 \leq k \leq r$, one has :

$$v(a_{n+r+1} - a_{n+k}) = w_S(r+1-k) - w_S(r+1-k-1).$$

Hence

$$v(a_{n+r+1} - a_n) = w_S(r+1) - \sum_{k=1}^{k=r}(w_S(r+1-k) - w_S(r+1-k-1))$$

So

$$v(a_{n+r+1} - a_n) = w_S(r+1) - w_S(r).$$

We then get (1)⇒ (3).
Suppose that $v(a_{n+r} - a_n) = w_S(r) - w_s(r-1)$ for every $n \in \mathbb{N}$ and every $r \geq 1$, then, for every $k \in \mathbb{N}$, one has

$$v\left(\prod_{j=0}^{j=k-1}(a_{n+k} - a_{n+j})\right) = w_S(k).$$

We then get (3)⇒ (2) □

We have the following corollary in the case $S = V$:

Corollary 8.2. *Let $(a_n)_{n\in\mathbb{N}}$ be a v-ordering of V. The sequence $(a_n)_{n\in\mathbb{N}}$ is very well distributed and well ordered if and only if for every $n, k \in \mathbb{N}$, one has: $v(a_{n+k} - a_n) = v_q(k)$, where $v_q(k)$ is the largest power of q dividing k.*

Proof. Denote by t a generator of $\mathfrak{M}$. Let $b_0, b_1, \cdots, b_{q-1}$ be a complete set of residues of $V/\mathfrak{M}$. Let $n \in \mathbb{N}$. Using the writing of n by q-digits, one can write $n = n_0 + n_1 q + n_2 q^2 + \cdots + n_r q^r$, with $0 \leq n_i < q$ for every $0 \leq i \leq r$. Put

$$u_n = b_{n_0} + b_{n_1} t + b_{n_2} t^2 + \cdots + b_{n_r} t^r.$$

Then the sequence $(u_n)_{n\in\mathbb{N}}$ is very well distributed and well ordered and for every $n, m \in \mathbb{N}$, one has:

$$v(u_n - u_m) = v_q(n - m).$$

□

We want to extend this equality when S is a Legendre subset. For every $n \in \mathbb{N}$, put:

$$\tilde{v}(n) = \sup\{r \in \mathbb{N} \mid q_r \,\text{divides n}\}.$$

we then have:

PROPOSITION 8.3. *Let S be a Legendre subset of V, then S admits a very well distributed and well ordered sequence. Moreover, for such a sequence $(u_n)_{n\in\mathbb{N}}$, one has $v(u_n - u_m) = \tilde{v}(n-m)$ for every $n, m \in \mathbb{N}$.*

Proof. Let $(a_n)_{n\in\mathbb{N}}$ be a v-ordering of S. Using permutations on the a_n's, we construct by induction on $r \in \mathbb{N}$, a sequence $(u_n)_{0\leq n<q_r}$ such that

$$v(u_n - u_m) = \tilde{v}(n-m)$$

for every $0 \leq n, m < q_r$.
For $0 \leq n < q_1$, put $u_n = a_n$.
Let $r \in \mathbb{N}$, we suppose that $(u_n)_{0\leq n\leq q_r-1}$ has been constructed. Let $q_r \leq n < q_{r+1}$. One can write $n = n_1 q_r + n_2$ with $0 \leq n_2 < q_r$. Let i_n be the unique integer satisfying

$$\begin{cases} n_1 q_r \leq i_n \leq (n_1+1)q_r - 1 \\ v(a_{i_n} - u_{n_2}) \geq r \end{cases}$$

Put $u_n = a_{i_n}$ (we have only permuted the elements of the set $\{a_k, n_1 q_r \leq k < (n_1+1)q_r\}$). Now, compute the valuation of $u_n - u_m$. There are 3 cases:

(i) If $0 \leq n, m < q_r$, we conclude with the induction hypothesis.

(ii) If $q_r \leq n, m < q_{r+1}$, then $q_r + 1 > q_r$. One can write:

$$u_n - u_m = a_{i_n} - a_{i_m} = a_{i_n} - u_{n_2} + u_{n_2} - u_{m_2} + u_{m_2} - a_{i_m}.$$

But $v(a_{i_n} - u_{n_2}) = v(u_{m_2} - a_{i_m}) = r$. So

$$\inf(r, v(u_{n_2} - u_{m_2})) \leq v(u_n - u_m) < r + 1.$$

There are 2 cases:

(a) If $\tilde{v}(n-m) = r$, then q_r divides $n - m$. In particular, one has $n_2 = m_2$. So $v(u_n - u_m) = r = \tilde{v}(n-m)$.

(b) If $\tilde{v}(n-m) < r$, that is, if $n_2 \neq m_2$,then $v(u_n - u_m) < r$. Then $v(u_n - u_m) = v(u_{n_2} - u_{m_2})$. As $\tilde{v}(n-m) = \tilde{v}(n_2 - m_2)$, using induction hypothesis, we get $v(u_n - u_m) = r = \tilde{v}(n-m)$.

(iii) If $0 \leq m < q_r \leq n < q_{r+1}$. In this case, $q_r < q_{r+1}$ and we can write

$$u_n - u_m = a_{i_n} - u_m = a_{i_n} - u_{n_2} + u_{n_2} - u_m.$$

There are 2 cases:

(a) If q_r divides $n - m$, then $n_2 = m$, hence $v(u_n - u_m) = r = \tilde{v}(n-m)$.

(b) If q_r does not divide $n - m$, then $v(u_{n_2} - u_m) < r$ and hence, $v(u_n - u_m) = v(u_{n_2} - u_m)$. As $\tilde{v}(n-m) = \tilde{v}(n_2 - m)$, then

$$v(u_n - u_m) = r = \tilde{v}(n-m).$$

Suppose now that (a_n) is another very well distributed and well ordered sequence of V. By Proposition 8.1, for every r, n, we have:

$$v(a_{n+r} - a_n) = w_S(r) - w_S(r-1) = v(u_{n+r} - u_n) = \tilde{v}(r).$$

And hence (a_n) satisfies the formula:

$$v(a_{n+r} - a_n) = \tilde{v}(r)$$

□

9. *Examples*

In all the following examples, we suppose that V is a discrete valuation ring with finite residue field of cardinality q.

PROPOSITION 9.1.
(i) *If G is a subgroup of $(V,+)$, then G is a Legendre set.*
(ii) *If G is a subgroup of $(V^\times,\times)$, then G is a Legendre set.*

Proof. (1) Let $x,y\in G$ and $r\in\mathbb{N}$. Let $\varphi: G\longrightarrow G$ defined by $\varphi(z)=y-x+z$. Then φ is an isometry and $\varphi(B(x,r))=B(y,r)$, where

$$B(a,r)=\{z\in G\mid v(a-z)\geq r\}.$$

To prove (2), we consider $\varphi: G\longrightarrow G$ defined by $\varphi(z)=\left(\frac{y}{x}\right)z$. □

EXAMPLE 3. Let $u\in V$ be such that $v(u)=0$. Then $E=\{u^n;\, n\in\mathbb{N}\}$ is a Legendre set.

Proof. The set E is a subset of the subgroup $F=\{u^n;\, n\in\mathbb{Z}\}$ of $V^\times$. To conclude, it suffices to prove that E is dense in F . Let $r\in\mathbb{N}$ and $m\in\mathbb{Z}$.

$$\forall n\in\mathbb{N}, v(u^n-u^m)=v(u^m(u^{n-m}-1))=v(u^{n-m}-1).$$

Denote by δ the order of u in $(V/\mathfrak{M}^r)^\times$. If $\delta\mid n-m$, then $v(u^{n-m}-1)\geq r$. We then take $n=m+k\delta$. □

This example can be generalized:

EXAMPLE 4. Let $u_1,u_2,\cdots,u_k\in V$ be such that $v(u_1)=\cdots=v(u_k)=0$. Then $E_k=\{u_1^{n_1}\cdots u_k^{n_k};\, n_1,\cdots,n_k\in\mathbb{N}\}$ is a Legendre set.

Proof. Let us prove this assertion when $k=2$: E_2 is dense in $F_2=\{u_1^{m_1}u_2^{m_2};\, m_1,m_2\in\mathbb{Z}\}$. For a fixed r and for m_1 and m_2 in $\mathbb{Z}$, one has:

$$u_1^{m_1}u_2^{m_2}-u_1^{n_1}u_2^{n_2}=u_1^{m_1}(u_2^{m_2}-u_2^{n_2})+u_2^{n_2}(u_1^{m_1}-u_1^{n_1})$$

so that,

$$v(u_1^{m_1}u_2^{m_2}-u_1^{n_1}u_2^{n_2})\geq\inf(v(u_2^{m_2}-u_2^{n_2}),v(u_1^{m_1}-u_1^{n_1})).$$

It suffices to choose $n_i=m_i+k_i\delta_i$ where δ_i is the order of u_i in $(V/\mathfrak{M}^r)^\times$ and k_i sufficiently large so that $m_i\geq 0$. □

The following example has already been studied in [**4**], but it is interesting to see that, thanks to Legendre sets, we can more easily compute their characteristic sequences.

EXAMPLE 5. Let V be a discrete valuation ring with finite residue field of cardinality q, and S be a subset of V such that $S=\cup_{j=1}^r b_j+\mathfrak{M}^l$ where, for $i\neq j, v(b_i-b_j)=h$ $(0\leq h<l)$. Then S is a Legendre set, $q_1=q_2=\cdots=q_h=1$, $q_{h+1}=\cdots=q_l=r$, $q_s=rq^{s-l}$ for $s\geq l$ and

$$w_S(n)=\sum_{i\geq 1}\left[\frac{n}{q_i}\right]=nh+(l-h)\left[\frac{n}{r}\right]+\sum_{s\geq 0}\left[\frac{n}{rq^s}\right].$$

References

1. Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964) 117-180.
2. M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.* **490** (1997), 101-127.
3. M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly* **107** (2000), 783-799.
4. J. Boulanger, J.L. Chabert, S. Evrard, G. Gerboud, The Characteristic Sequence of Integer-Valued Polynomials on a Subset, in *Advances in Commutative Ring Theory, Lecture Notes in Pure and Appl. Math.*, **205** (1999), 161-174. Dekker, New York.

5. P.J. Cahen, J.L. Chabert, *Integer-valued polynomials*, Mathematical Surveys and Monographs, vol **48**, Amer. Math. Soc., Providence (1997).
6. Y. Fares, *Polynômes à valeurs entières et conservation des factorielles*, Ph.D. thesis, Université de Picardie Jules Verne, Amiens, juillet 2006.
7. R. Gilmer and W. Smith, On the polynomial equivalence of subsets E and $f(E)$ of $\mathbb{Z}$, *Arch. Math.* **73** (1999) 355-365.
8. E. Helsmoortel, Module de continuité de polynômes d'interpolation. Application à l'étude du comportement local des fonctions continues sur un compact régulier d'un corps local, *C. R. Acad. Sci. Paris.* **268** (1969), 1168-1171.
9. G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. Reine Angew. Math.* **149** (1919), 97-116.
10. J. Yeramian, Anneaux de Bhargava, *Comm. Algebra.* **32** (2004), 3043-3069.

S. Evrard and Y. Fares
Laboratoire de Mathématiques
fondamentales et appliquées d'Amiens,
CNRS UMR 6140, 33 rue Saint Leu,
80039 Amiens (France)

sabine.evrard@u-picardie.fr
youssef.fares@u-picardie.fr