MINIMAL GENERATING SETS FOR THE D-ALGEBRA $\mathrm{Int}(S, D)$

JACQUES BOULANGER AND JEAN-LUC CHABERT

Abstract. We are looking for minimal generating sets for the D-algebra $\mathrm{Int}(S, D)$ of integer-valued polynomials on any infinite subset S of a Dedekind domain D. For instance, the binomial polynomials $\binom{X}{p^r}$, where p is a prime number and r is any nonnegative integer, form a minimal generating set for the classical $\mathbb{Z}$-algebra $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$. In the local case, when D is a valuation domain and S is a regular subset of D, we are able to construct minimal generating sets, but we are not always able to extract from a generating set a minimal one. In particular, we prove that, in local fields, the generating set of integer-valued polynomials obtained by de Shalit and Iceland by means of Lubin-Tate formal group laws is minimal. In our proofs we make an extensive use of Bhargava's notion of p-ordering.

1. Introduction

When studying the ring $\mathrm{Int}(D)$ of integer-valued polynomials on a domain D, one of the first things we are looking for is the existence of bases of $\mathrm{Int}(D)$ as a D-module. Here, we consider $\mathrm{Int}(D)$ where D is a Dedekind domain, or more generally $\mathrm{Int}(S, D)$ where S is an infinite subset of D, as a D-algebra.

The origin of our study comes from a statement of de Shalit and Iceland [13] that we recall now. Let K be a local field and V be the corresponding valuation domain. De Shalit and Iceland obtained by a very interesting and surprising way, namely by means of Lubin-Tate formal groups, a generating set of the V-algebra of integer-valued polynomials on V, that is,

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

More precisely, if $F(t_1, t_2)$ denotes a Lubin-Tate formal group law on V, one knows that, for every $x \in V$, there is a unique power series

$$[x](t) = \sum_{n=1}^{\infty} c_n(x) t^n$$

such that $c_1(x) = x$ and $F([x](t_1), [x](t_2)) = [x](F(t_1, t_2))$. It turns out that the $c_n(x)$'s are polynomials of $\mathrm{Int}(V)$ of degree $\leq n$. Denoting by q the cardinality of the residue field of V, the authors proved [13, Thm 3.1] that the set

$$\{c_{q^m}(x) \mid m \geq 0\}$$

Date: January 31, 2018.

2010 *Mathematics Subject Classification.* Primary 13F20 ; Secondary 11B65, 11S31, 13F30.

Key words and phrases. Integer-valued polynomials, minimal generating sets, Bhargava's p-orderings, Lubin-Tate formal group laws .

is a generating set for the V-algebra $\mathrm{Int}(V)$. They also state that this set is a minimal generating set, but they did not give really a proof. Thus, the aim of this paper is to give a proof of this statement (Theorem 4.13 below). By the way, we study the question of the existence of minimal generating sets for the D-algebra of integer-valued polynomials $\mathrm{Int}(S,D)$ in a more general framework, namely, when D is a Dedekind domain and S is an infinite subset of D.

For instance, in the particular case where $K=\mathbb{Q}_p$ and $V=\mathbb{Z}_p$, following [9, §5.1], we know a minimal generating set of the $\mathbb{Z}_p$-algebra $\mathrm{Int}(\mathbb{Z}_p)$ obtained by a more direct way, namely the set formed by the polynomials $F_{p^m}(X)$ $(m\geq 0)$ defined inductively by $F_1(X)=X$, $F_p(X)=\frac{X^p-X}{p}$ and, for $m\geq 1$, $F_{p^m}(X)=F_p(F_{p^{m-1}}(X))$. In fact, the author gives no proof of minimality (which is true however, see Proposition 2.4 below).

Let us consider another example, the classical ring of integer-valued polynomials:

$$\mathrm{Int}(\mathbb{Z})=\{f(X)\in\mathbb{Q}[X]\mid f(\mathbb{Z})\subseteq\mathbb{Z}\}.$$

It is well known that the binomial polynomials

$$\binom{X}{n}=\frac{X(X-1)\dots(X-n+1)}{n!}\quad(n\geq 0)$$

form a basis of the $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$. The set $\{\binom{X}{n}\}_{n\geq 0}$ is then a generating set, and in fact a minimal generating set, for the $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$. If we try to extract from this set a minimal generating set for the $\mathbb{Z}$-algebra $\mathrm{Int}(\mathbb{Z})$, we see that there exists one and only one such subset, namely (see Proposition 5.9):

$$\left\{\binom{X}{p^k}\;\middle|\; p\in\mathbb{P},k\in\mathbb{N}\right\}.$$

We will prove below analogous results when replacing $\mathbb{Z}$ by an integral domain.

Notation. Let D denote an integral domain with quotient field K, and consider the D-algebra of *integer-valued polynomials on* D, that is,

$$\mathrm{Int}(D)=\{f(X)\in K[X]\mid f(D)\subseteq D\}.$$

More generally, for every infinite subset S of D, consider the D-algebra of *integer-valued polynomials on* S *with respect to* D, that is,

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

Recall that, for every $n\in\mathbb{N}$, the leading coefficients of the polynomials of $\mathrm{Int}(S,D)$ with degree $\leq n$ form a nonzero fractional ideal of D denoted by $\mathfrak{I}_n(S,D)$ and called the n-th *characteristic ideal* of S (cf. [5, §II.1]). We also know:

Proposition 1.1 ([5, II.1.5])**.** *Let $\mathcal{G}\subseteq\mathrm{Int}(S,D)$. If, for every $n\geq 0$, the leading coefficients of the polynomials of $\mathcal{G}$ with degree n generate the fractional ideal $\mathfrak{I}_n(S,D)$, then $\mathcal{G}$ is a generating set for the D-module* $\mathrm{Int}(S,D)$.

In the sequel, we will look for generating sets of the D-algebra $\mathrm{Int}(S,D)$ which are extracted from sets $\mathcal{G}$ obtained by this way. In particular, when the characteristic ideals are principal, there exists bases of $\mathrm{Int}(S,D)$ having one and only one polynomial of each degree. Following Pólya [19], such a basis is called a *regular basis*. Proposition 1.1 shows that there exists regular bases for the D-module $\mathrm{Int}(S,D)$ if and only if all the characteristic ideals $\mathfrak{I}_n(S,D)$ are principal.

We begin our study with the local case: in the next section, we consider first the easiest case, namely, the $\mathbb{Z}_p$-algebra $\mathrm{Int}(\mathbb{Z}_p)$. Then, in section 3, we consider generating sets for the V-algebra extracted from regular bases of the V-module $\mathrm{Int}(S,V)$ where V is any rank-one valuation domain and S any infinite subset of V. To obtain minimal generating sets with Theorem 4.8 we need to assume that the subset S is regular (we recall there the notion of regular subset). Finally, in section 5, we globalize the previous results to Dedekind domains.

2. Minimal generating sets for the $\mathbb{Z}$-algebra $\mathrm{Int}(\mathbb{Z}_p)$

Let p be a fixed prime number. We denote by $\mathbb{Q}_p$ the field of p-adic numbers, by $\mathbb{Z}_p$ the ring of p-adic integers, and by v_p the p-adic valuation on $\mathbb{Q}_p$.

2.1. Extracted from the regular basis formed by the $\binom{X}{n}$.

Lemma 2.1. *The $\mathbb{Z}_p$-algebra $\mathrm{Int}(\mathbb{Z}_p)$ admits the following generating set:*

$$\left\{ \binom{X}{p^r} \Big| r \geq 0 \right\}.$$

Proof. Assume that $n \geq 2$ is not of the form p^r with $r \geq 0$. Then, $n = mp^r$ with $m \geq 2$, and $p \not| m$. Using Legendre formula

$$v_p(n!) = \sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \quad [17]$$

we have:

$$v_p(n!) = \sum_{k=1}^{r} m \left\lfloor \frac{p^r}{p^k} \right\rfloor + \sum_{k\geq 1} \left\lfloor \frac{m}{p^k} \right\rfloor$$

$$= \sum_{k=1}^{r} \left\lfloor \frac{p^r}{p^k} \right\rfloor + \sum_{k=1}^{r} (m-1) \left\lfloor \frac{p^r}{p^k} \right\rfloor + \sum_{k\geq 1} \left\lfloor \frac{m-1}{p^k} \right\rfloor = v_p(p^r!) + v_p((m-1)p^r!)\,.$$

Consequently, $n! = u \times p^r! \times ((m-1)p^r)!$ where u is invertible in $\mathbb{Z}_p$. Thus, the degree of the polynomial $\binom{X}{n} - \frac{1}{u}\binom{X}{p^r}\binom{X}{(m-1)p^r}$ is strictly less than n. Since the polynomial $\binom{X}{n}$ is generated by the binomials $\binom{X}{m}$ where $m < n$, it may be deleted from the generating set. □

Remark 2.2. If n is of the form p^r for some $r \geq 1$, the previous reasoning does not hold since

$$\forall j \in \{1, \ldots, p^r - 1\} \quad v_p(j!) + v_p((p^r - j)!) < v_p(p^r!)\,.$$

This is a consequence of Legendre formula written in the following way:

$$v_p(n!) = \frac{n - \sigma_p(n)}{p-1} \quad [17]$$

where $\sigma_p(n)$ denotes the sum of the digits of n in base p.

$$v_p\left(\binom{p^r}{j}\right) = v_p(p^r!) - v_p(j!) - v_p((p^r-j)!) = \frac{\sigma_p(j) + \sigma_p(p^r - j) - \sigma_p(p^r)}{p-1}\,.$$

Since each carry in the addition of j and $p^r - j$ decreases the sum of the digits by $p-1$, p divides $\binom{p^r}{j}$.

We show now that the generating set given in Lemma 2.1 is minimal.

Proposition 2.3. *The set* $\left\{\binom{X}{p^r}\,\middle|\, r\geq 0\right\}$ *is a minimal generating set for the* $\mathbb{Z}_p$*-algebra* $\mathrm{Int}(\mathbb{Z}_p)$*. Moreover, it is the only minimal generating set that one may extract from* $\left\{\binom{X}{n}\,\middle|\, n\in\mathbb{N}\right\}$.

Proof. First, the polynomial $X=\binom{X}{p^0}$ cannot be delete since if we have a relation of the form

$$X = c_0 + \sum_{\underline{\alpha}\neq\underline{0}} c_{\underline{\alpha}} \binom{X}{k_1}^{\alpha_1} \dots \binom{X}{k_s}^{\alpha_s} \quad \text{where } c_{\underline{\alpha}}\in\mathbb{Z}_p \text{ and } k_i\neq 0,1\,, \tag{1}$$

the substitution of 0 and 1 for X would lead to a contradiction.

Now assume that there exists some $r\geq 1$ such that $\binom{X}{p^r}$ could be deleted, that is, that there exists a relation of the form

$$\binom{X}{p^r} = c_0 + \sum_{\underline{\alpha}\neq\underline{0}} c_{\underline{\alpha}} \binom{X}{k_1}^{\alpha_1} \dots \binom{X}{k_s}^{\alpha_s} \quad \text{where } c_{\underline{\alpha}}\in\mathbb{Z}_p \text{ and } k_i\neq 0,p^r\,. \tag{2}$$

The classical formula (see for instance [12, T. 1, Ch. 1, Ex. 23]):

$$\binom{X}{m}\binom{X}{n} = \sum_{l=\max(m,n)}^{m+n} \frac{l!}{(l-m)!(l-n)!(m+n-l)!}\binom{X}{l} \tag{3}$$

shows that the coefficient of $\binom{X}{p^r}$ in the development of the product $\binom{X}{m}\binom{X}{n}$ where $m,n\neq p^r$ is always divisible by p since if $m>p^r$, or $n>p^r$, or $m+n<p^r$, $\binom{X}{p^r}$ does not appear, and if $0<m,n<p^r$ and $m+n\geq p^r$,

$$\frac{p^r!}{(p^r-m)!(p^r-n)!(m+n-p^r)!} = \binom{p^r}{m}\binom{m}{p^r-n},$$

we may conclude with Remark 2.2.

Thus, if in the right side of Eq. (2), we replace successively all the products $\binom{X}{m}\binom{X}{n}$ by means of Eq. (3) until we obtain a sum which is linear with respect to the $\binom{X}{l}$'s then, if $\binom{X}{p^r}$ appears, its coefficient is divisible by p, and this property remains until the end of the process. So that, we will obtain an equality of the form:

$$\binom{X}{p^r} = \sum_l b_l \binom{X}{l} \quad \text{with } p|b_{p^r}\,.$$

Since, the $\binom{X}{l}$'s form a basis of the $\mathbb{Z}_p$-module $\mathrm{Int}(\mathbb{Z}_p)$, we have a contradiction.

Moreover, this is the only minimal generating subset that can be extracted from $\{\binom{X}{n}\mid n\in\mathbb{N}\}$ since $\binom{X}{p^r}$ cannot be obtained from all of the others. □

2.2. **Extracted from the basis formed by the Fermat polynomials.**

As previously said in the introduction, we know another natural basis of the $\mathbb{Z}_p$-module $\mathrm{Int}(\mathbb{Z}_p)$ constructed from the Fermat binomial

$$F_p(X) = \frac{X^p - X}{p}\,. \tag{4}$$

Consider the sequence formed by the iterates of F_p :

$$F_{p^0}(X) = F_1(X) = X \text{ and, for } k\geq 2, F_{p^k}(X) = F_p(F_{p^{k-1}}(X))\,. \tag{5}$$

Now, if n may be written $n = n_k n_{k-1} \cdots n_1 n_0$ in base p, one let

$$F_n(X) = \prod_{j=0}^{k} (F_{p^j})^{n_j} . \tag{6}$$

One knows [5, §II.2] that the set $\{F_n(X)\}_{n\geq 0}$ is a regular basis of the $\mathbb{Z}_p$-module $\mathrm{Int}(\mathbb{Z}_p)$. It follows from Eq.(6) that the polynomials F_{p^k} ($k \in \mathbb{N}$) form a generating set of the $\mathbb{Z}_p$-algebra $\mathrm{Int}(\mathbb{Z}_p)$. In fact, this generating set is minimal:

Proposition 2.4. [9, §5.1] *The polynomials F_{p^k} ($k \in \mathbb{N}$) defined by Formulas* (4) *and* (5) *form a minimal generating set for the $\mathbb{Z}_p$-algebra* $\mathrm{Int}(\mathbb{Z}_p)$.

Proof. All the relations between the F_{p^k} are generated by the following:

$$(F_{p^k})^p - F_{p^k} = p\, F_{p^{k+1}} .$$

Let $R = \mathrm{Int}(\mathbb{Z}_p)$ and $\overline{R} = R/pR$. Clearly, the images $\overline{F_{p^k}}$ of the F_{p^k}'s in R/pR generate R/pR and the relations between the $\overline{F_{p^k}}$'s are all deduced from $\overline{F_{p^k}}^p = \overline{F_{p^k}}$. Consequently, the $\overline{F_{p^k}}$'s form an irredundant set of generators of R/pR, and hence, the same assertion holds for $R = \mathrm{Int}(\mathbb{Z}_p)$. □

We find similar proofs of minimality for several sub-$\mathbb{Z}_p$-algebras of $\mathrm{Int}(\mathbb{Z}_p)$ in [11].

3. Generating sets in the local case

Hypotheses and notation for the section

Let K be a valued field. We denote by v the valuation of K and by V the corresponding valuation domain. By definition, v is a rank-one valuation, that is, $v : K^* \to \mathbb{R}$.

Let S be an infinite subset of V which is assumed to be precompact, that is, such that its completion with respect to the topology defined by v is compact.

3.1. Gaps and generating sets.

Let w_S denote the 'characteristic function' of S which is associated to the sequence of characteristic ideals of S :

$$w_S : n \in \mathbb{N} \mapsto -v(\mathfrak{I}_n(S, D)) \in \mathbb{R} .$$

The function w_S is super-additive, that is,

$$w_S(i + j) \geq w_S(i) + w_S(j) \text{ for all } i, j \geq 0$$

since clearly $\mathfrak{I}_i(S, V) \times \mathfrak{I}_j(S, V) \subseteq \mathfrak{I}_{i+j}(S, V)$. We are led to consider the indices for which the function is strictly super-additive.

Definition 3.1. The set of *indices of gaps* of w_S is defined by

$$\mathfrak{g}_V(S) = \{n > 0 \mid \forall i \in \{1, \ldots, n-1\} \;\; w_S(i) + w_S(n-i) < w_S(n)\} .$$

By definition, we always have $1 \in \mathfrak{g}_V(S)$. It follows from the previous section that, for every prime number p

$$\mathfrak{g}(\mathbb{Z}_p) = \mathfrak{g}_{\mathbb{Z}_p}(\mathbb{Z}_p) = \{p^r \mid r \geq 0\} . \tag{7}$$

Recall that the inverse of the characteristic ideals $\mathfrak{I}_n(S, V)$ is the n-th factorial ideal $(n!)_S^V$ of S as defined by Bhargava [2]. Consequently, $w_S(n) = v((n!)_S^V)$.

The following proposition is a slight generalization of [16, Prop. 4.3].

Proposition 3.2. *If* $\{g_n\}_{n\geq 0}$ *is a regular basis of* $\mathrm{Int}(S,V)$*, then the following set is a generating set for the* V*-algebra* $\mathrm{Int}(S,V)$:

$$\{\, g_n \mid n \in \mathfrak{g}_V(S) \,\}\,.$$

Proof. It follows from Proposition 1.1 that the set $\{\, g_n \mid n \geq 0 \,\}$ is a generating set of the module. We may forget $g_0 = 1$ for the generating set of the algebra. Let $n > 0$ and assume that $n \notin \mathfrak{g}_V(S)$: there exist $i > 0$ and $j > 0$ such that $i + j = n$ and $w_S(i) + w_S(j) = w_S(n)$. Denoting by $lc(g)$ the leading coefficient of every polynomial g, we have $v(lc(g_k)) = w_S(k)$ for all k. Thus, in the valuation domain V we have the relation:

$$lc(g_n) = u \times lc(g_i) \times lc(g_j) \quad \text{where } v(u) = 0\,.$$

Consequently,

$$\deg\left(g_n(X) - u g_i(X) g_j(X)\right) < n,$$

and hence, $g_n(X) - u g_i(X) g_j(X)$ is a linear combination of the g_m's where $m < n$. Thus, we may delete g_n from the generating set. □

In other words, every polynomial $f \in \mathrm{Int}(S,V)$ of degree n may be written:

$$f(X) = P(g_{i_1}(X), \ldots, g_{i_k}(X)) \text{ where } i_1, \ldots, i_k \in \mathfrak{g}_V(S) \cap \{1, \ldots, n\}$$

and $P(T_1, \ldots, T_k) \in V[T_1, \ldots, T_k]$. Moreover, the previous proof shows that we may add: the total degree of P is ≤ 2.

We will prove next that some of these generating sets are minimal generating sets for the V-algebra $\mathrm{Int}(S,V)$ if the subset S itself is sufficiently regular.

Remark 3.3. Take care that there are generating sets extracted from regular bases which do not necessarily contain all the g_n's where $n \in \mathfrak{g}_V(S)$. Indeed, consider the $\mathbb{Z}_3$-algebra $\mathrm{Int}(\mathbb{Z}_3)$ and the regular basis $\{g_n\}_{n\geq 0}$ where $g_n(X) = \binom{X}{n}$ for $n \neq 5$ and $g_5(X) = \binom{X}{5} + \binom{X}{3}$. We now that $3 \in \mathfrak{g}(\mathbb{Z}_3)$ while the $\mathbb{Z}_3$-algebra $\mathrm{Int}(\mathbb{Z}_3)$ is generated by the g_n's where $n \in \{1, 4, 5\} \cup \{3^r \mid r \geq 2\}$ since

$$\binom{X}{3} = g_5(X) - \frac{1}{5}(g_1(X) - 4) \times g_4(X)\,.$$

3.2. **Structural constants.**

As said in the introduction, the V-module $\mathrm{Int}(S,V)$ is free. Thus, if $\{f_n\}_{n\geq 0}$ denotes a basis, we may consider the corresponding structural constants $c_k(n,m)$ of the V-algebra $\mathrm{Int}(S,V)$ defined by the relations:

$$f_n(X) f_m(X) = \sum_{k\geq 0} c_k(n,m) f_k(X) \quad (m,n,k \in \mathbb{N}). \tag{8}$$

The $c_k(n,m)$ are unique and belong to V since the f_k's form a basis of the V-module $\mathrm{Int}(S,V)$. Recall the following result due to Elliott [14, Prop. 2.2] in the case where the basis is a regular basis associated to a v-ordering (see subsection 3.3):

Proposition 3.4. *Let* $\{f_n\}_{n\geq 0}$ *be a basis and consider the* $c_k(n,m)$ *defined by* (8)*. Then, all the relations between the generators* f_n *are generated by relations* (8)*.*

Proof. Let $\varphi : V[T_1, \ldots, T_n, \ldots] \to \mathrm{Int}(S,V)$ be the homomorphism of V-algebra defined by $\varphi(T_n) = f_n$. Clearly, φ is onto and $\ker(\varphi)$ contains the ideal $\mathfrak{I}$ generated by the elements $T_n T_m - \sum_{k\geq 0} c_k(n,m) T_k$. It is easy to see that every $P \in V[T_1, \ldots, T_n, \ldots]$ is congruent modulo $\mathfrak{I}$ to a linear form $\sum_{0\leq k\leq n} \lambda_k T_k$, and then,

$\varphi(P) = \sum_{k=0}^{n} \lambda_k f_k$. Moreover, this linear form is unique because of the fact that the f_k's form a basis. Consequently, the morphism $\overline{\varphi} : V[\dots, T_n, \dots]/\mathfrak{I} \to \mathrm{Int}(S,V)$ deduced from φ is a bijection. □

In order to generalize the previous results obtained for $\mathrm{Int}(\mathbb{Z}_p)$, we need a formula analogous to Eq. (3) which allowed us to say that the coefficient of $\binom{X}{p^r}$ is divisible by p. This is the hypothesis of the next lemma.

Lemma 3.5. *Fix some $l \in \mathbb{N}^*$. If for all $n, m \neq l$, either $c_l(n,m) = 0$ or $v(c_l(n,m)) > 0$, then f_l does not belong to the V-algebra generated by the f_n's where $n \in \mathbb{N} \setminus \{l\}$.*

Proof. Assume that there exists a relation of the form:

$$f_l(X) = \sum_{\underline{\alpha}} d_{\underline{\alpha}} f_{k_1}^{\alpha_1}(X) \dots f_{k_s}^{\alpha_s}(X) \text{ where } d_{\underline{\alpha}} \in V \text{ and } k_i \neq l\,.$$

Replacing successively every product of two polynomials f_{k_i} and f_{k_j}, by means of relations (8), until we obtain a linear combination of the $f_k(X)$'s, we see that, if $f_l(X)$ appears at some step, then this is always with a coefficient whose valuation is > 0, and this property is preserved at the following steps. Thus, we obtain an equality of the form:

$$f_l(X) = \sum_{k} b_k f_k(X) \text{ with } v(b_l) > 0\,.$$

We have a contradiction since the $f_k(X)$'s form a basis of the V-module $\mathrm{Int}(S,V)$. □

The following proposition is an obvious consequence of Proposition 3.2 and Lemma 3.5.

Proposition 3.6. *Let $\{f_n\}_{n\geq 0}$ be a regular basis of $\mathrm{Int}(S,V)$. If for every $l \in \mathfrak{g}_V(S)$ and for every $n, m \neq l$, either $c_l(n,m) = 0$ or $v(c_l(n,m)) > 0$, then the set $\{f_l \mid l \in \mathcal{G}_V(S)\}$ is a minimal generating set for the V-algebra $\mathrm{Int}(S,V)$. Moreover, it is the only minimal generating set that one may extract from $\{f_n \mid n \geq 0\}$.*

3.3. **Regular bases associated to v-orderings.**

Let us recall the notion of v-ordering introduced by Manjul Bhargava [2]. A *v-ordering* of the subset S is a sequence $\{a_n\}_{n\geq 0}$ of elements of S such that, for every $n \geq 1$, a_n satisfies

$$v\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \inf_{x\in S} v\left(\prod_{k=0}^{n-1}(x - a_k)\right)\,.$$

Such sequences exist thanks to the precompactness of S [7].

Clearly, if $\{a_n\}_{n\geq 0}$ is a v-ordering of S, then the following sequence of polynomials is a regular basis of $\mathrm{Int}(S,V)$ (see [4]):

$$f_0(X) = 1 \text{ and, for } n \geq 1,\ f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}\,. \tag{9}$$

Lemma 3.7. *Let $\mathcal{B} = \{f_n \mid n \geq 0\}$ be a regular basis of $\mathrm{Int}(S,V)$ constructed by means of a v-ordering $\{a_n\}_{n\geq 0}$ of S. Any subset $\mathcal{G}$ of $\mathcal{B}$ which is a generating set for the V-algebra $\mathrm{Int}(S,V)$ contains $f_1(X) = \frac{X-a_0}{a_1-a_0}$.*

Proof. Otherwise, analogously to the beginning of the proof of Proposition 2.3, we would obtain a contradiction by substituting a_0 and a_1 to X. □

Lemma 3.8. [14, Prop. 2.2] *Let $\{f_n\}_{n\geq 0}$ be a regular basis associated to a v-ordering $\{a_n\}_{n\geq 0}$ of S and consider the structural constants $c_k(n,m)$ associated to this basis. Then, for $k < \max\{n,m\}$ or $k > n+m$, $c_k(n,m) = 0$. Moreover, $c_m(0,m) = 1$ and $c_m(m,m) = 1$.*

Proof. By considering the degree, we see that $c_k(n,m) = 0$ for $k > n+m$. We may prove by induction on k that $c_k(n,m) = 0$ for $k < \max(n,m)$ since $f_k(a_h) = 0$ for $0 \leq h \leq k-1$ and $f_k(a_k) = 1$.

In particular,

$$f_m(X)f_m(X) = c_m(m,m)f_m(X) + \ldots + c_k(m,m)f_k(X) + \ldots + c_{2m}(m,m)f_{2m}(X)\,.$$

By substituting a_m to X, we obtain $c_m(m,m) = 1$. The equality $c_m(0,m) = 1$ is obvious. □

Despite Elliott's work [14] on the structural constants of the V-algebra $\mathrm{Int}(S,V)$ with respect to regular bases associated to v-orderings, we need to add an hypothesis on the subset S : we assume that S is regular in a sense which generalizes the regular compact subsets of local fields considered by Amice [1].

4. Minimal generating sets in the case of a regular subset

Hypotheses and notation for the section

Let K be a valued field, let V be the corresponding valuation domain, and let S be an infinite precompact subset of V.

For every $\gamma \in \mathbb{R}$ and every $x \in S$, consider the class in S of x modulo γ, that is, the S-ball

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

Denote by q_γ the number of classes of S modulo γ, that is, the number of distinct nonempty S-balls $S(x,\gamma)$.

The fact that S is precompact is equivalent to the fact that all the q_γ's are finite (see for instance [7, Lemma 3.1]). Moreover, there is a strictly increasing sequence of non-negative numbers $\{\gamma_k\}_{k\geq 0}$, the *critical valuations* of S, which tends to $+\infty$ such that

$$\gamma_0 = \min_{x,y\in S\,,\ x\neq y} v(x-y)$$

and

$$q_{\gamma_k} \leq q_\gamma < q_{\gamma_{k+1}} \ \Leftrightarrow\ \gamma_k \leq \gamma < \gamma_{k+1} \qquad \text{[8, Prop. 5.1].} \tag{10}$$

Note that $q_{\gamma_0} = 1$.

4.1. Regular subsets, gaps, and strong v-orderings.

Definition 4.1. The precompact subset S of the valued field K is said to be *regular* if, whatever $\gamma < \delta$, all nonempty S-balls $S(x,\gamma)$ contain the same number of S-ball $S(y,\delta)$.

Consequently, with notation (10), if S is regular there exist a sequence of positive integers $\{\alpha_k\}_{k\geq 0}$ such that each nonempty S-ball $S(x, \gamma_k)$ contains α_k non-empty distinct S-balls $S(y, \gamma_{k+1})$. In particular, for every $k \geq 0$, we have:

$$q_{\gamma_{k+1}} = \alpha_k q_{\gamma_k}\,.$$

When S is regular, the characteristic function w_S satisfies the following generalization of Legendre formula:

$$w_S(n) = n\gamma_0 + \sum_{k\geq 1} \left[\frac{n}{q_{\gamma_k}}\right](\gamma_k - \gamma_{k-1}) \qquad [10,\ \text{Thm } 1.5]. \tag{11}$$

Lemma 4.2. *If S is regular, then the indices of gaps of S are the cardinalities q_γ :*

$$\mathfrak{g}_V(S) = \{q_{\gamma_k} \mid k \geq 0\}\,.$$

Proof. Fix some $n \neq 0, 1$ which is not of the form q_{γ_k} and let r be the largest integer such that q_{γ_r} divides n. Then, $n = mq_{\gamma_r}$ where $m \geq 2$ and $\alpha_r \nmid m$. It follows from (11) that

$$w_S(n) = mq_{\gamma_r}\gamma_0 + \sum_{k=1}^{r} m\left[\frac{q_{\gamma_r}}{q_{\gamma_k}}\right](\gamma_k - \gamma_{k-1}) + \sum_{k\geq r+1}\left[\frac{mq_{\gamma_r}}{q_{\gamma_k}}\right](\gamma_k - \gamma_{k-1})$$

$$= (m-1)q_{\gamma_r}\gamma_0 + \sum_{k=1}^{r}(m-1)\left[\frac{q_{\gamma_r}}{q_{\gamma_k}}\right](\gamma_k - \gamma_{k-1}) + \sum_{k\geq r+1}\left[\frac{(m-1)q_{\gamma_r}}{q_{\gamma_k}}\right](\gamma_k - \gamma_{k-1})$$

$$+q_{\gamma_r}\gamma_0 + \sum_{k=1}^{r}\left[\frac{q_{\gamma_r}}{q_{\gamma_k}}\right](\gamma_k - \gamma_{k-1}) = w_S(n - q_{\gamma_r}) + w_S(q_{\gamma_r})\,.$$

On the other hand, consider some n of the form q_{γ_r} with $r \geq 1$. Then, for every $j \in \{1, ..., n-1\}$, we have:

$$w_S(j)+w_S(n-j) = j\gamma_0+\sum_{k=1}^{r-1}\left[\frac{j}{q_{\gamma_k}}\right](\gamma_k-\gamma_{k-1})+(n-j)\gamma_0+\sum_{k=1}^{r-1}\left[\frac{n-j}{q_{\gamma_k}}\right](\gamma_k-\gamma_{k-1})$$

$$\leq n\gamma_0 + \sum_{k=1}^{r-1}\left[\frac{n}{q_{\gamma_k}}\right](\gamma_k - \gamma_{k-1}) < w_S(n)\,.$$

The strict inequality follows from the fact that $\left[\frac{n}{q_{\gamma_r}}\right](\gamma_k - \gamma_{k-1}) = \gamma_k - \gamma_{k-1}$ is missing. □

We also know that:

Proposition 4.3. [10, Theorem 1.5] *Any regular subset S admits* strong v-orderings*, that is, sequences $\{a_n\}_{n\geq 0}$ of elements of S such that, for every $k \geq 0$, $\{a_n\}_{n\geq k}$ is a v-ordering of S.*

For instance, the sequence $\{0, 1, 2, \ldots\}$ is a strong p-ordering of $\mathbb{Z}_p$.

4.2. **Minimal generating sets associated to strong v-orderings.**

Both following lemmas show clearly why regular subsets allow a generalization of what happens for $\mathbb{Z}_p$.

Lemma 4.4. *Assume that $\{a_n\}_{n\geq 0}$ is a strong v-ordering of S and let $\{f_n\}_{n\geq 0}$ be the regular basis of $\mathrm{Int}(S,V)$ associated to this strong v-ordering. Then, for every $l \in \mathfrak{g}_V(S)$ and every $k \in \{1,\ldots,l-1\}$, one has $v(f_k(a_l)) > 0$.*

Proof.

$$f_k(a_l) = \prod_{j=0}^{k-1} \frac{a_l - a_j}{a_k - a_j} = \frac{\prod_{j=0}^{l-1}(a_l - a_j)}{\prod_{j=0}^{k-1}(a_k - a_j)\prod_{j=k}^{l-1}(a_l - a_j)}\,.$$

Since, the sequence $\{a_n\}$ is a strong v-ordering, we have

$$v\left(\prod_{j=k}^{l-1}(a_l - a_j)\right) = v\left(\prod_{j=0}^{l-k-1}(a_l - a_j)\right) = w_S(l-k)\,.$$

Finally, $l \in \mathfrak{g}_V(S)$ implies:

$$v(f_k(a_l)) = w_S(l) - w_S(k) - w_S(l-k) > 0\,.$$

□

Lemma 3.8 may be completed by the following:

Lemma 4.5. *Let $\{f_n\}_{n\geq 0}$ be a regular basis associated to a strong v-ordering $\{a_n\}_{n\geq 0}$ of the regular subset S and let $c_k(n,m)$ be the corresponding structural constants. Then, for every $l \in \mathfrak{g}_V(S)$:*

$$[\,n\cdot m \neq 0 \text{ and } (n,m)\neq(l,l)\,] \;\Rightarrow\; [\,c_l(n,m) = 0 \;\text{ or }\; v(c_l(n,m)) > 0\,]\,.$$

Proof. By Lemma 3.8, we may assume that $1 \leq n \leq m \leq l \leq n+m$. Thus we have:

$$f_n(X)f_m(X) = c_m f_m(X) + \ldots + c_l f_l(X) + \ldots + c_{n+m} f_{n+m}(X)\,.$$

Consequently,

$$f_n(a_l)f_m(a_l) = c_m f_m(a_l) + \ldots + c_{l-1} f_{l-1}(a_l) + c_l\,.$$

If $n < l$, it follows from Lemma 4.4 that $v(c_l) > 0$. □

It follows from Lemma 4.5 that we may apply Proposition 3.6 and obtain:

Theorem 4.6. *Let K be a valued field, V be its valuation domain, and S be a precompact and regular subset of V. Let $\mathfrak{g}_V(S)$ denote the set of indices of gaps, that is, the set formed by the cardinalities q_γ of the subsets S mod γ. Let $\{a_n\}_{n\geq 0}$ be a strong v-ordering of S and let $\mathcal{B} = \{f_n\}_{n\geq 0}$ be the regular basis of the V-module $\mathrm{Int}(S,V)$ associated to this strong v-ordering, that is, defined by $f_n(X) = \prod_{k=0}^{n-1} \frac{X-a_k}{a_n-a_k}$. Then, there is one and only one subset $\mathcal{G}$ of $\mathcal{B}$ which is a minimal generating set of $\mathrm{Int}(S,V)$ as a V-algebra, namely*

$$\mathcal{G} = \{f_n \mid n \in \mathfrak{g}_V(S)\}\,.$$

4.3. **Other minimal generating sets when S is a regular subset.**

To extend Theorem 4.6 to other regular bases, we are looking for conditions which will allow us to use Lemma 4.5:

Proposition 4.7. *Let $\{a_n\}_{n\geq 0}$ be a strong v-ordering of the regular subset S, let $\{g_n\}_{n\geq 0}$ be a regular basis of $\mathrm{Int}(S, V)$, and let $l \in \mathfrak{g}_V(S)$. If $v(g_n(a_l) - g_n(a_0)) > 0$ for all $n > l$ then, $g_l(X)$ does not belong to the V-algebra generated by the g_n's where $n \in \mathbb{N} \setminus \{l\}$.*

Proof. If $\{f_n\}_{n\geq 0}$ denotes the regular basis associated to the strong v-ordering $\{a_n\}_{n\geq 0}$, for every $g(X) = \sum_{k=0}^{n} d_k f_k(X) \in \mathrm{Int}(S, V)$, we have

$$g(a_l) = g(a_0) + \sum_{k=1}^{l-1} d_k f_k(a_l) + d_l,$$

and hence, by Lemma 4.4, $v(d_l - (g(a_l) - g(a_0)) > 0$.

Consequently, by hypothesis, for every $n > l$, if $g_n(X) = \sum_{k=0}^{n} d_{n,k} f_k(X)$, then $v(d_{n,l}) > 0$. Assume now that we have

$$g_l(X) = \sum_{\underline{\alpha}} c_{\underline{\alpha}} g_{k_1}^{\alpha_1}(X) \dots g_{k_s}^{\alpha_s}(X) \text{ where } c_{\underline{\alpha}} \in V \text{ and } k_i \neq l\,.$$

Replacing the g_{k_i}'s by the f_k's in the right hand side by means of the equality $g_{k_i} = \sum_k d_{k_i,k} f_k$, we note that if f_l appears in a monomial the valuation of the corresponding coefficient is > 0. Then, we compute all the products of the f_k's by means of Lemma 4.5 and we obtain in the right hand side a sum of the form $\sum_k b_k f_k$ where $v(b_l) > 0$, that is, we obtain an equality of the form:

$$g_l(X) = \sum_k b_k f_k(X) \text{ with } v(b_l) > 0\,.$$

We have a contradiction since the f_k's and the g_h's form regular bases of the V-module $\mathrm{Int}(S, V)$. □

Now, we are able to state and prove our main theorem in the local case.

Theorem 4.8. *Let K be a valued field, V be its valuation domain, and S be a precompact and regular subset of V. Let $\mathfrak{g}_V(S)$ denote the set of indices of gaps and let $\{a_n\}_{n\geq 0}$ denote a strong v-ordering of S. Let $\mathcal{B} = \{g_n \mid n \geq 0\}$ be a regular basis of the V-module $\mathrm{Int}(S, V)$ such that*

$$\forall l \in \mathfrak{g}_V(S)\ \forall n > l \quad v(g_n(a_l) - g_n(a_0)) > 0\,. \tag{12}$$

Then, there is one and only one subset $\mathcal{G}$ of $\mathcal{B}$ which is a minimal generating set of $\mathrm{Int}(S, V)$ as a V-algebra, namely $\mathcal{G} = \{g_n \mid n \in \mathfrak{g}_V(S)\}$.

Proof. By Proposition 3.2, $\mathcal{G}$ is a generating set. The fact that this is a minimal generating set and that this is the only minimal generating set that can be extracted from $\mathcal{B}$ is an obvious consequence of Proposition 4.7. □

Remark 4.9. Condition (12) is not necessary to be able to extract a minimal generating set, as shown by the following corollary, but it is useful for us to be sure that this is the unique extracted minimal set as shown by the example of Remark 3.3.

Corollary 4.10. *Let K be a valued field, V be its valuation domain, and S be a precompact and regular subset of V. Let $\{a_n\}_{n\geq 0}$ denote a strong v-ordering of S. For each $k \in \mathfrak{g}_V(S)$, let g_k be a polynomial of $\mathrm{Int}(S,V)$ of degree k such that the valuation of its leading coefficient is equal to $-w_S(k)$. If*

$$\forall\, k, l \in \mathfrak{g}_V(S)\ \ [\, l < k\ \Rightarrow\ v(g_k(a_l) - g_k(a_0)) > 0\,]\,, \tag{13}$$

then $\{\, g_n \mid n \in \mathfrak{g}_V(S)\,\}$ is a minimal generating set of $\mathrm{Int}(S,V)$ as a V-algebra.

Proof. Let $\{f_n\}_{n\geq 0}$ be the regular basis associated to the strong v-ordering $\{a_n\}_{n\geq 0}$. For every $n \geq 0$, let $h_n = g_n$ if $n \in \mathfrak{g}_V(S)$ and $h_n = f_n$ if $n \notin \mathfrak{g}_V(S)$. Then, $\{h_n\}_{n\geq 0}$ is a regular basis which satisfies Eq. (12) of Theorem 4.8. □

Remark 4.11. Condition (13) is not necessary to have a minimal generating set: for instance, by Proposition 2.4, $\{F_{p^k} \mid k \in \mathbb{N}\}$ is a minimal generating set of $\mathrm{Int}(\mathbb{Z}_p)$ while $\mathfrak{g}(\mathbb{Z}_3) = \{3^k \mid k \geq 0\}$, $\{n\}_{n\geq 0}$ is a strong p-ordering of $\mathbb{Z}_p$, and $3 \nmid F_{3^3}(3)$.

This remark leads us to suppose that the following conjecture could be true.

Conjecture. For every regular subset S of V and every regular basis $\{f_n\}_{n\geq 0}$ of $\mathrm{Int}(S,V)$, the generating set $\{f_n \mid n \in \mathfrak{g}(S)\}$ is minimal.

4.4. **The generating set associated to a Lubin-Tate formal group law.**

In the particular case where $S = V$ is a discrete valuation domain, Corollary 4.10 becomes:

Proposition 4.12. *Let V be the ring of a discrete valuation v with uniformizer π and finite residue field of cardinality q. Let $\{f_{q^m}(X) \mid m \geq 0\}$ be a set of polynomials of $\mathrm{Int}(V)$ such that $\deg(f_{q^m}) = q^m$ and the valuation of the leading coefficient of f_{q^m} is equal to $-\frac{q^m-1}{q-1}$. If for every $m > l \geq 1$ $v(f_{q^m}(\pi^l) - f_{q^m}(0)) > 0$, then the f_{q^m}'s form a minimal generating set of the V-algebra $\mathrm{Int}(V)$.*

Proof. Recall first how we can construct a strong v-ordering $\{a_n\}_{n\geq 0}$ of V (cf. [5, §II.2]): let $\{a_0 = 0, a_1, \ldots, a_{q-1}\}$ be a system of representatives of the residue field of V then, for $n = n_r q^r + \ldots + n_1 q + n_0$ where $0 \leq n_j < q$, let $a_n = a_{n_r}\pi^r + \ldots a_{n_1}\pi + a_{n_0}$. We then have $w_V(n) = \sum_{k>0} \left\lfloor \frac{n}{q^k} \right\rfloor$, and hence, $\mathfrak{g}(V) = \{q^m \mid m \geq 0\}$. □

Assume now that the discrete valuation domain V is the ring of integers of a local field K, that is, K is complete with respect to the topology defined by the valuation v and the residue field of V is finite with cardinality q. Recall that a commutative formal group law over V is a formal power series $F(X,Y) \in V[[X,Y]]$ with the following properties:

$F(X,Y) \equiv X + Y \pmod{\deg 2}$,
$F(X, F(Y,Z)) = F(F(X,Y), Z)$,
$F(X,Y) = F(Y,X)$.

The formal group law F is said to be a Lubin-Tate formal group law if it admits an endomorphism f, that is a power series $f(T) \in V[[T]]$ such that

$f(F(X,Y)) = F(f(X), f(Y))$,

which satisfies

$f(T) \equiv \pi T \pmod{\deg 2}$,
$f(T) \equiv T^q \pmod{\pi}$,

Theorem 4.13. *Let V be the valuation domain of a local field K, whose residue field has cardinality q, and let F be a Lubin-Tate formal group law on V associated to a power series f. For each $x \in V$, let $[x](T) = \sum_{n\geq 1} c_n(x)T^n$ be the unique power series such that $c_1(x) = x$ and $f \circ [x] = [x] \circ f$. Then, for each $n \geq 1$, $c_n(x)$ is an integer-valued polynomial of degree $\leq n$. Moreover, for $m \geq 0$, the $c_{q^m}(x)$'s are integer-valued polynomials on V with degree exactly q^m which form a minimal generating set of* $\mathrm{Int}(V)$.

Proof. That the $c_n(x)$ are polynomials of degree $\leq n$ follows from the formula

$$[x](T) = \exp_F(x \log_F(T)) \tag{14}$$

and that they are integer-valued follows clearly from the fact that $[x](T) \in V[[T]]$. That the c_{q^m}'s are of degree q^m and form a generating set for the V-algebra $\mathrm{Int}(V)$ is already proved by de Shalit and Iceland [13, Theorem 3.1]. That this is a minimal generating set follows easily from Proposition 4.12: we just have to verify that, denoting by π a uniformizer such that $f(T) \equiv \pi T \pmod{\deg 2}$, we have:

$$\forall\, m > l \geq 1 \quad c_{q^m}(\pi^l) \equiv c_{q^m}(0) \pmod{\pi}.$$

First, it follows from (14) and $\exp_F(T) \equiv T \pmod{\deg 2}$ that $[0](T) = 0$ and $c_n(0) = 0$ for every n. Moreover, it is known that $[x] \circ [y] = [xy]$ for all $x, y \in V$, and that $[\pi] = f$. Finally, since by definition $f \equiv T^q \pmod{\pi}$, we have $[\pi^l](T) = f(T) \circ \cdots \circ f(T) \equiv T^{q^l} \pmod{\pi}$, and hence, $c_{q^m}(\pi^l) \equiv 0 \pmod{\pi}$.

□

5. Globalization when D is a Dedekind domain

In this section, we assume that D is a Dedekind domain and S is an infinite subset of D. Recall that, in a Dedekind domain, every ideal $\mathfrak{I}$ is generated by two elements, moreover the first generator may be any nonzero element of $\mathfrak{I}$. Noticing that, for every n, $X^n \in \mathrm{Int}(S,D)$, we then have:

Proposition 5.1. *If, for every $n \geq 0$, the polynomial $g_n \in \mathrm{Int}(S,D)$ of degree n is chosen in such a way that its leading coefficient generates with 1 the fractional ideal $\mathfrak{I}_n(S,D)$, then the set $\{X^n \mid n \in \mathbb{N}\} \cup \{g_n \mid n \in \mathbb{N}^*\}$ is a generating set for the D-module* $\mathrm{Int}(S,D)$, *and the set $\{X\} \cup \{g_n \mid n \in \mathbb{N}^*\}$ is a generating set for the D-algebra* $\mathrm{Int}(S,D)$.

To obtain minimal generating subsets, we begin by deleting some generators that are useless. To do this we have to consider the 'gaps' of the factorial ideals of S.

5.1. The factorial ideals and their gaps.

Bhargava ([2], [3], [4]) associate to the subset S of the Dedekind domain D a sequence of ideals called *factorial ideals of S*, denoted by $n!_S^D$ (or $n!_S$) which could be defined by:

$$n!_S^D = \mathfrak{I}_n(S,D)^{-1} \quad (n \geq 0).$$

The ideals $n!_S^D$ are entire ideals (for instance, $n!_{\mathbb{Z}} = n!\,\mathbb{Z}$). They form a decreasing sequence for the inclusion and satisfy:

$$0!_S = D \quad \text{and} \quad n!_S \times m!_S \text{ divides } (n+m)!_S\,.$$

Remark 5.2. One could think that, analogously to Definition 3.1, the gaps of the factorial ideals of S with respect to D should correspond to integers n such that, for every $j \in \{1, \ldots, n-1\}$, $j!_S \times (n-j)!_S \neq n!_S$. With such a definition, the gaps of the factorials of $\mathbb{Z}$ would correspond to all nonnegative integers since $j(n-j) \neq 0$ implies $\frac{n!}{j!(n-j)!} = \binom{n}{j} \neq 1$. The following equality shows that this definition would be too extensive in view of a global statement of Theorem 4.8:

$$\binom{X}{6} = X\binom{X}{5} + \binom{X}{2}\binom{X}{4} - \binom{X}{3}^2 + \binom{X}{3} - 6\binom{X}{4} + 5\binom{X}{5}.$$

Thus, the set $\left\{\binom{X}{n}\right\}_{n\geq 0}$ is not a minimal generating set for the $\mathbb{Z}$-algebra $\mathrm{Int}(\mathbb{Z})$. We are then led to consider the following definition which in fact extends also Definition 3.1.

Definition 5.3. The set of *indices of gaps* of the factorial ideals $n!_S^D$ is

$$\mathfrak{g}_D(S) = \{n \geq 1 \mid n!_S^D \neq \cap_{1\leq j\leq n-1} \left(j!_S^D \times (n-j)!_S^D\right)\}.$$

In other words, the index n corresponds to a gap if the ideal $n!_S^D$ is not the least common multiple of the ideals $j!_S^D(n-j)!_S^D$ for $1 \leq j \leq n-1$. Equivalently,

$$n \in \mathfrak{g}_D(S) \;\Leftrightarrow\; \exists \mathfrak{m} \in \mathrm{Max}(D)\; \forall j \in \{1, \ldots, n-1\}\; [\, w_{\mathfrak{m}}(n) > w_{\mathfrak{m}}(j) + w_{\mathfrak{m}}(n-j)\,].$$

Consequently,

$$\mathfrak{g}_D(S) = \cup_{\mathfrak{m}\in \mathrm{Max}(D)}\; \mathfrak{g}_{D_{\mathfrak{m}}}(S).$$

5.2. **Localization and globalization.**

Recall that, since D is Noetherian, for each maximal ideal $\mathfrak{m}$ of D [5, §I.2] :

$$\mathrm{Int}(S, D)_{\mathfrak{m}} = \mathrm{Int}(S, D_{\mathfrak{m}}). \tag{15}$$

These equalities allow us to globalize the previous results obtained in the local case. In view of this globalization the following proposition will be useful.

Proposition 5.4. *Let $\{h_j\}_{j\in J}$ be a set of elements of $\mathrm{Int}(S, D)$. The set $\{h_j \mid j \in J\}$ is a generating set for the D-algebra $\mathrm{Int}(S, D)$ if and only if, for every $\mathfrak{m} \in \mathrm{Max}(D)$, this set is a generating set for the $D_{\mathfrak{m}}$-algebra $\mathrm{Int}(S, D_{\mathfrak{m}})$.*

Proof. Clearly, it follows from Formula (15) that the condition is necessary. Conversely, assume that $\{h_j\}_{j\in J}$ is a generating set for all the localizations and consider some $g(X) \in \mathrm{Int}(S, D)$. By hypothesis, for every maximal ideal $\mathfrak{m}$ of D, there exists a polynomial $P_{\mathfrak{m}} \in D_{\mathfrak{m}}[T_j \mid j \in J]$ such that $g = P_{\mathfrak{m}}((h_j)_{j\in J})$. Let $s_{\mathfrak{m}} \in D \setminus \mathfrak{m}$ be such that $s_{\mathfrak{m}} P_{\mathfrak{m}} \in D[T_j \mid j \in J]$. As the $s_{\mathfrak{m}}$'s generate the ideal D, there exist finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_l$ and elements $t_1, \ldots, t_l \in D$ such that $t_1 s_{\mathfrak{m}_1} + \ldots + t_l s_{\mathfrak{m}_l} = 1$. Consequently,

$$g(X) = \sum_{i=1}^{l} t_i\, s_{\mathfrak{m}_i}\, g(X) = \sum_{i=1}^{l} t_i\; \left(s_{\mathfrak{m}_i}\, P_{\mathfrak{m}_i}((h_j)_{j\in J})\right).$$

Let

$$Q(T_{j_1}, \ldots, T_{j_r}) = \sum_{i=1}^{l} t_i\; \left(s_{\mathfrak{m}_i}\, P_{\mathfrak{m}_i}((T_j)_{j\in J})\right).$$

Then,

$$g(X) = Q(h_{j_1}(X), \ldots, h_{j_r}(X)) \quad \text{where} \quad Q \in D[T_{j_1}, \ldots, T_{j_r}].$$

□

Corollary 5.5. *If the factorial ideals $n!_S$ are principal, that is, if $\mathrm{Int}(S,D)$ admits a regular basis $\{g_n\}_{n\geq 0}$, the set $\{\, g_n \mid n \in \mathfrak{g}_D(S)\,\}$ is a generating set for the D-algebra $\mathrm{Int}(S,D)$.*

This is an obvious consequence of Propositions 3.2 and 5.4.

Remark 5.6. If $\{g_j \mid j \in J\}$ is a generating set for the D-algebra $\mathrm{Int}(S,D)$, then the characteristic ideal $\mathfrak{I}_1(S,D)$ is generated as a fractional ideal by the leading coefficients of the polynomials g_j of degree 1. Thus, if $\mathfrak{I}_1(S,D)$ is not principal, a generating set of $\mathrm{Int}(S,D)$ necessarily contains two polynomials of degree 1 (as in the following example).

Example 5.7. Let $K = \mathbb{Q}(\sqrt{-5})$, $D = \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Then, $3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$ where $\mathfrak{p} = (3, 1+\sqrt{-5})$ and $\mathfrak{q} = (3, 1-\sqrt{-5})$. We consider $\mathrm{Int}(\mathfrak{p}, \mathbb{Z}[\sqrt{-5}])$. The characteristic ideal $\mathfrak{I}_1(\mathfrak{p}, \mathbb{Z}[\sqrt{-5}])$ is equal to $\mathfrak{p}^{-1} = (1, \frac{1-\sqrt{-5}}{3})$ and is not principal. Consequently, any generating set of $\mathrm{Int}(\mathfrak{p}, \mathbb{Z}[\sqrt{-5}]$ contains two polynomials of degree 1, for instance X and $\frac{1-\sqrt{-5}}{3}X$.

Remark 5.8. Why do we assume that S is infinite? Because, if S is finite, there does no exist in general any minimal generating set for the D-algebra $\mathrm{Int}(S,D)$.

Let us look for instance to the $\mathbb{Z}$-algebra $\mathrm{Int}(\{0\},\mathbb{Z}) = \mathbb{Z} + X\mathbb{Q}[X]$. Let $\{h_j\}_{j\in J}$ be the elements of degree one of a generating set of the $\mathbb{Z}$-algebra $X\mathbb{Q}[X]$. By Remark 5.6, there exist $j_1, \ldots, j_r \in J$ such that $X \in \sum_{i=1}^{r} Dh_{j_i}$. Noticing that, if $h = \frac{a}{b}X$ with $(a,b) = 1$, then there exist $u, v \in \mathbb{Z}$ such that $\frac{1}{b}X = uh + vX$, it is easy to see that every h_{j_0} where $j_0 \in J \setminus \{j_1, \ldots, j_r\}$ belongs to the $\mathbb{Z}$-module generated by the h_j's where $j \in J \setminus \{j_0\}$, and hence, that no generating set can be minimal.

On the other hand, if S is empty, there may exist minimal generating sets for the D-algebra $\mathrm{Int}(\emptyset, D) = K[X]$ as shown by the set $\{\frac{1}{p} \mid p \in \mathbb{P}\} \cup \{X\}$ for the $\mathbb{Z}$-algebra $\mathbb{Q}[X]$.

5.3. **Classical examples.**

Proposition 5.9. *The following set of polynomials is a generating set for the $\mathbb{Z}$-algebra $\mathrm{Int}(\mathbb{Z})$:*

$$\binom{X}{p^r} \quad \text{where } p \in \mathbb{P} \text{ and } r \geq 0\,.$$

Moreover, it is the only subset of $\left\{ \binom{X}{n} \mid n \in N \right\}$ which is a minimal generating set.

This is a consequence of Propositions 2.3 and 5.4. We may also note that the $\binom{X}{n}$'s are constructed by means of the sequence $\{n\}_{n\geq 0}$ which is a strong p-ordering for every p. With respect to Fermat polynomials, next theorem follows from Propositions 2.4 and 5.4, and also from the fact that, if $p \neq p'$, the polynomials $F_{p'^k}$ belong to $\mathbb{Z}_{(p')}[X]$ and then are useless to generate $\mathrm{Int}(\mathbb{Z}_{(p)})$.

Proposition 5.10. *The set of polynomials $\{F_{p^k} \mid p \in \mathbb{P}, k \in \mathbb{N}\}$ where $F_1 = X$, $F_p = \frac{X^p - X}{p}$ and, for $k \geq 2$, $F_{p^k} = F_p(F_{p^{k-1}})$ is a minimal generating set for the $\mathbb{Z}$-algebra $\mathrm{Int}(\mathbb{Z})$.*

With respect to subsets, the following result shows that a generating set for the $\mathbb{Z}$-module $\mathrm{Int}(S,\mathbb{Z})$ can be, just by deleting 1, a minimal generating set for the Z-algebra $\mathrm{Int}(S,\mathbb{Z})$.

Proposition 5.11. *Let q be an integer ≥ 2 and let $S = \{q^n \mid n \geq 0\}$. The set of polynomials*

$$\left[\begin{array}{c} X \\ n \end{array}\right]_q = \prod_{k=0}^{n-1} \frac{X-q^k}{q^n-q^k} \quad (n \geq 1)$$

is a minimal generating set of the $\mathbb{Z}$-algebra $\mathrm{Int}(S,\mathbb{Z})$.

Proof. It is well known that the polynomials $\left[\begin{array}{c} X \\ n \end{array}\right]_q$ $(n \geq 1)$ form with 1 a regular basis of the $\mathbb{Z}$-module $\mathrm{Int}(S,\mathbb{Z})$ (cf. [5, Exercise II.15]) since the sequence $\{q^n\}_{n\geq 0}$ is a simultaneous ordering of S. In particular, $\mathfrak{I}_n(S,\mathbb{Z})^{-1} = \prod_{k=0}^{n-1}(q^n - q^k)\mathbb{Z} = q^{\frac{n(n-1)}{2}} \prod_{h=1}^{n}(q^h-1)\mathbb{Z}$, and hence, $\mathcal{G}(S) = \mathbb{N}^*$ since, for every prime p dividing q, $w_{p,S}(n) = -v_p(\mathfrak{I}_n(S,\mathbb{Z})) = \frac{n(n-1)}{2} v_p(q)$. The proposition is then a consequence of Proposition 3.6 thanks to the following result due to Elliott, Adams, DeMoss, Freaney and Mostowa: □

Proposition 5.12. [14, Theorem 1.5] *For all $m, n \in \mathbb{N}$*

$$\left[\begin{array}{c} X \\ m \end{array}\right]_q \left[\begin{array}{c} X \\ n \end{array}\right]_q = \sum_{l=\max(m,n)}^{m+n} q^{(l-m)(l-n)} \binom{l}{l-m, l-n, m+n-l} \left[\begin{array}{c} X \\ l \end{array}\right]_q$$

5.4. **Globalization of the sets given by Lubin-Tate formal group laws.**

At the end of their paper [13, § 4.2], de Shalit and Iceland described a globalization to number fields of their results in local fields. This globalization works in particular for number fields of class number one. We recall here this globalization with some slight changes so that it works in a more general framework, namely for Pólya fields.

Recall that a number field K is called a *Pólya field* [20] if $\mathrm{Int}(\mathcal{O}_K)$ admits a regular basis. It is known [5, II.3.9] that this is equivalent to the fact that the Pólya group of $\mathcal{O}_K$ is trivial where the *Pólya group* $\mathcal{P}o(D)$ of a Dedekind domain D is the subgroup of the class group generated by the classes of the ideals $\Pi_q(D)$ where $\Pi_q(D)$ denotes the product of all the prime ideals $\mathfrak{p}$ of D with the same norm q :

$$\Pi_q(D) = \prod_{\mathfrak{p}\in \mathrm{Max}(D),\, |D/\mathfrak{p}|=q} \mathfrak{p}\,.$$

Now, let K be a number field with ring of integers $\mathcal{O}_K$. Let T be a finite (possibly empty) set of primes such that the Pólya group of $R = \mathcal{O}_{K,T} = \cap_{\mathfrak{p}\notin T}\mathcal{O}_{K,\mathfrak{p}}$ is trivial. Denote by $\mathcal{Q}$ the set of integers $\{q \mid q = N_{K/\mathbb{Q}}(\mathfrak{p}), \mathfrak{p} \notin T\}$ and, for each $q \in \mathcal{Q}$, let π_q be a generator of the principal ideal $\Pi_q(R)$. Now, consider the formal Dirichlet series

$$L(s) = \prod_{q\in\mathcal{Q}} \frac{1}{1-\frac{1}{\pi_q N_{K/\mathbb{Q}}(\Pi_q(R))^s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}\,, \tag{16}$$

Clearly, $a_1 = 1$, $a_n \in K$, and, for every $\mathfrak{p} \notin T$ with norm q, the Dirichlet series $(1-\pi_q^{-1}N_{K/\mathbb{Q}}(\Pi_q(R))^{-s})\,L(s)$ has $\mathfrak{p}$-integral coefficients. [This is exactly de Shalit and Iceland's proof where the set $\{\mathfrak{p} \mid \mathfrak{p} \notin T\}$ is replaced by the set $\{\Pi_q \mid q \in \mathcal{Q}\}$.]

Consider the formal power series

$$f(X) = \sum_{n=1}^{\infty} a_n X^n \tag{17}$$

and the group law

$$F(X, Y) = f^{-1}(f(X) + f(Y)) \tag{18}$$

for which f is a logarithm. A priori F is defined over K, let us show that it is defined over R.

Let $\mathfrak{p} \notin T$ with norm q. Letting $N_{K/\mathbb{Q}}(\Pi_q(R)) = q^g = l$, one has:

$$(1 - \pi_q^{-1} N_{K/\mathbb{Q}}(\Pi_q(R))^{-s})\, L(s) = \sum_{n \geq 1} \left(a_n - \frac{1}{\pi_q} a_{\frac{n}{l}} \right) \frac{1}{n^s} \tag{19}$$

where $a_{\frac{n}{l}} = 0$ when $l \nmid n$. From the fact that the Dirichlet series (19) has $\mathfrak{p}$-integral coefficients, it follows that the corresponding power series has $\mathfrak{p}$-integral coefficients:

$$g(X) = f(X) - \frac{1}{\pi_q} f(X^l) \in \mathcal{O}_{K,\mathfrak{p}}[[X]]\,. \tag{20}$$

Now Hazewinkel's functional equation lemma [15, I.2.2 (i)] implies that the coefficients of the formal group law F defined by (18) are also in $\mathcal{O}_{K,\mathfrak{p}}$, and hence, in $R = \cap_{\mathfrak{p} \notin T} \mathcal{O}_{K,\mathfrak{p}}$.

Furthermore, by [15, I.8.3.6], F is a Lubin-Tate formal group law associated with the prime π_q and the corresponding power series $[\pi]_F = f^{-1}(\pi f(X))$. Then, for every $x \in \mathcal{O}_{K,\mathfrak{p}}$, $[x]_F(t) = f^{-1}(x f(t)) \in \mathcal{O}_{K,\mathfrak{p}}[[t]]$. Finally,

$$\forall x \in R \quad [x]_F(t) = \sum_{n=1}^{\infty} c_n(x) t^n \in R[[t]]\,, \tag{21}$$

and the $c_n(x)$'s belongs to $\mathrm{Int}(R)$. In the particular case where K is a Pólya field, we may state the following:

Proposition 5.13. *Let K be a Pólya field. Consider the Dirichlet series (16) where $\mathcal{Q}$ denotes the set formed by the norms of all the primes of K and the formal group law on $\mathcal{O}_K$ defined by means of equations (17) and (18). Then the functions $c_n(x)$ defined by (21) belong to $\mathrm{Int}(\mathcal{O}_K)$ and the subset $\{c_n(x) \mid n \in \mathfrak{g}(R)\}$ where $\mathfrak{g}(R) = \{q^m \mid q \in \mathcal{Q}, m \in \mathbb{N}\}$ is a generating set for the $\mathcal{O}_K$-algebra $\mathrm{Int}(\mathcal{O}_K)$.*

But we do not know whether this generating set is minimal.

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, Generalized Factorials and Fixed Divisors over Subsets of a Dedekind Domain, *J. Number Theory* **72** (1998), 67–75.

[4] M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly* **107** (2000), 783-799.

[5] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys and Monographs, **48**, Providence, 1997.

[6] P.-J. Cahen and J.-L. Chabert, What's New About Integer-Valued Polynomials on a Subset?, in *Non Noetherian Commutative Ring Theory*, Kluwer Academic Press, Dordrecht, 2000, 75–96.

[7] P.-J. Cahen and J.-L. Chabert, On the ultrametric Stone-Weierstrass theorem and Mahler's expansion, *J. Théor. Nombres de Bordeaux* **14** (2002), 43–57.
[8] J.-L. Chabert, Integer-valued polynomials in valued fields with an application to discrete dynamical systems, in *Commutative Algebra and Applications*, de Gruyter, Berlin, 2009, pp. 103-134.
[9] J.-L. Chabert, Integer-Valued Polynomials: Looking for regular Bases (a Survey), in *Commutative Algebra: Recent Advances in Commutative Rings, Integer-Valued Polynomials, and Polynomial Functions*, pp. 83–111, Springer, 2014.
[10] J.-L. Chabert, S. Evrard and Y. Fares, Regular Subsets of valued Fields and Bhargava's v-orderings, *Math. Zeitchrift* **274** (2013), 263–290.
[11] F. Clarke and S. Whitehouse, Algebraic properties of stably numerical polynomials, *J. Pure and Appl. Alg.* **207** (2006), 607–617.
[12] L. Comtet, *Analyse combinatoire*, Presses Universitaires de France, Paris, 1970.
[13] E. De Shalit and E. Iceland, Integer valued polynomials and Lubin-Tate formal groups, *J. Number Theory* **129** (2009), 632–639.
[14] J. Elliott, Newton basis relations and applications to integer-valued polynomials and q-binomial coefficients, *Integers* **14** (2014), # A38.
[15] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978.
[16] K. Johnson, Super-additive sequences and algebras of polynomials, *Proc. Amer. math. Soc.* **139** (2011), 3431–3443.
[17] A.-M. Legendre, *Essai sur la théorie des nombres*, 2nd ed., Courcier, Paris, 1808.
[18] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 117–124.
[19] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 97–116.
[20] H. Zantema, Integer valued polynomials over a number field, *Manuscr. Math.* **40** (1982), 155–203.

LAMFA CNRS-UMR 7352, Université de Picardie, 80039 Amiens, France
E-mail address: jaboulanger@wanadoo.fr

LAMFA CNRS-UMR 7352, Université de Picardie, 80039 Amiens, France
E-mail address: jean-luc.chabert@u-picardie.fr