GENERALIZED FACTORIAL IDEALS

Jean-Luc Chabert*

Université de Picardie Jules Verne
Faculté de Mathématiques et d'Informatique
Amiens, France

الخلاصة :

باستعمال مفهوم « ترتيب ـ v » (أو الترتيب التقييمي) في الحلقات التقييمية المنفصلة ، قام « بهاركفا Bhargava » بتقديم ودراسة المثاليات العاملية المنبثقة من مجموعات جزئية لحلقات « ديدكيند Dedekind »، تعميما للمفهوم الكلاسيكي للمثالية العاملية . نوضح كيف يمتد هذا المفهوم إلى مجموعات جزئية لحلقات تقييمية ذات بُعدٍ احادي، ومن ثمّ كيف يتم تمديد مفهوم المثالية العاملية المنبثقة من مجموعات جزئية لحلقات « كرول Krull » مع الاحتفاظ تقريباً بنفس الخواص . بالإضافة إلى ذلك، نحصل على نتائج حول السلوك التقاربي لمتتالية هذه المثاليات العاملية .

ABSTRACT

Using the notion of v-ordering in discrete valuation domains, Bhargava introduced factorial ideals associated with subsets of Dedekind domains, which generalize the classical factorials. We show how v-orderings may be extended to subsets of rank-one valuation domains, and also, how factorial ideals may be generalized to subsets of Krull domains with almost the same properties. In addition, we obtain results concerning the asymptotic behavior of the sequence of these factorial ideals.

1991 *Mathematics Subject Classification.* Primary: 11B65, 13F20;
Secondary: 11B83, 13F30.

Keywords and phrases: Factorials, integer-valued polynomials, valuations.

*Address for correspondence:
Université de Picardie Jules Verne
Faculté de Mathématiques et d'Informatique
33 rue Saint Leu, 80039 Amiens Cedex 01
France
e-mail: jlchaber@worldnet.fr

GENERALIZED FACTORIAL IDEALS

INTRODUCTION

Recall first some properties of the classical factorials $n!$ [1]:

Property 1 — For each k, $l \in \mathbb{N}$,

$$\frac{(k+l)!}{k!l!} \in \mathbb{N}.$$

Property 2 — For any sequence $a_0, a_1, \ldots, a_n$ of $n+1$ integers, the product:

$$\prod_{0 \le i < j \le n} (a_j - a_i) \quad \text{is divisible by} \quad 1! \ldots n!.$$

Moreover, the product is equal to 1 for the sequence $0, 1, \ldots, n$.

Property 3 — For every monic polynomial $f \in \mathbb{Z}[X]$ of degree n,

$$d(f) = \gcd\{f(k) \mid k \in \mathbb{Z}\} \quad \text{divides} \quad n! \qquad [16].$$

Moreover, for $f = (X+1) \ldots (X+n)$, $d(f) = n!$.

Property 4 — For every integer-valued polynomial g of degree n, that is, every $g \in \mathbb{Q}[X]$ of degree n such that $g(\mathbb{Z}) \subseteq \mathbb{Z}$,

$$n!g(X) \in \mathbb{Z}[X].$$

Moreover, $\frac{1}{n!}$ is the leading coefficient of the binomial polynomial:

$$\binom{X}{n} = \frac{X(X-1)\ldots(X-n+1)}{n!}.$$

In these assertions, $\mathbb{Z}$ is considered either as a domain (divisibility in $\mathbb{Z}$), or as a set (sequences of elements in $\mathbb{Z}$). Following Bhargava [2], we will extend these properties by replacing $\mathbb{Z}$ both by a domain D and by a subset E of D. In the first section, generalizing Property 4, we define the factorial ideals with respect to any subset E of an integral domain D. In Section 2, we extend to any valuation domain the notion of v-ordering introduced by Bhargava for discrete valuation domains [2], and recall the links with integer-valued polynomials and factorial ideals. Then, in Section 3, we show that, even if there is no v-ordering, the main results concerning factorial ideals still remain valid in the case of rank-one valuation domains (Prop. 3.2, Thms 3.12 and 3.13). In Section 4, we study the asymptotic behavior of some arithmetic functions associated with the sequence of factorials ideals (Prop. 4.1 and Thm 4.2). Then, in Section 5, we globalize the previous results in the case where D is a Krull domain (Prop. 5.8 and 5.9) extending Bhargava's results for Dedekind domains [3]. Finally, in the last section, we consider some examples.

1. FACTORIALS IDEALS

Notation. Let D be an integral domain with quotient field K and let E be any subset of D. (In the three next sections, D will be a valuation domain denoted by V.)

Recall that the *ring of integer-valued polynomials on* E (with respect to D) is:

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

Definition 1.1. [6, §II.1] For each $n \in \mathbb{N}$, the *characteristic ideal* of index n of the ring $\mathrm{Int}(E, D)$ is the set $\mathfrak{I}_n(E, D)$ formed by the leading coefficients of the polynomials in:

$$\mathrm{Int}_n(E, D) = \{f \in \mathrm{Int}(E, D) \mid \deg(f) \le n\}.$$

Clearly, $\{\mathfrak{I}_n(E, D)\}_{n \in \mathbb{N}}$ is an increasing sequence of D-modules such that

$$D \subseteq \mathfrak{I}_n(E, D) \subseteq K, \quad \text{and} \quad \mathfrak{I}_0(E, D) = D.$$

One knows that (see [12] and [6, Proposition I.3.1]):

- if $n \ge card(E)$, then $\mathfrak{I}_n(E, D) = K$,
- if $n < card(E)$, then $\mathfrak{I}_n(E, D)$ is a fractional ideal of D.

In particular, if $card(E)$ is infinite, all the $\mathfrak{I}_n(E, D)$ are fractional ideals.

Recall also that, for each fractional ideal $\mathfrak{I}$ of D, the set

$$\mathfrak{I}^{-1} = \{x \in K \mid x\mathfrak{I} \subseteq D\}$$

is a fractional ideal of D called the *inverse* of $\mathfrak{I}$ (although, the inclusion $\mathfrak{I} \cdot \mathfrak{I}^{-1} \subseteq D$ may be strict and $(\mathfrak{I}^{-1})^{-1}$ may strictly contain $\mathfrak{I}$). Such an inverse is a divisorial ideal, that is, an intersection of principal fractional ideals of D (and, in this case, is equal to the inverse of its inverse). By convention, we will write $K^{-1} = (0)$ and $(0)^{-1} = K$.

The following definition extends those given by Zantema [20] in the case where D is the ring of integers of a number field and $E = D$, and by Bhargava [3] in the case where E is a subset of a Dedekind domain D.

Definition 1.2. The *factorial ideal* of index n with respect to the subset E of D is the inverse of the fractional ideal $\mathfrak{I}_n(E, D)$ and is denoted by $(n!)_E^D$ or $(n!)_E$ if the context allows us to omit D:

$$(n!)_E^D = \mathfrak{I}_n^{-1}(E, D).$$

For instance,

$$(n!)_{\mathbb{Z}}^{\mathbb{Z}} = (n!)_{\mathbb{N}}^{\mathbb{Z}} = n!\,\mathbb{Z}.$$

Here are some easy properties of these factorial ideals.

Proposition 1.3. *For each subset E of the integral domain D:*

1. $(0!)_E = D$,
2. $\{(n!)_E\}_{n \in \mathbb{N}}$ *is a decreasing sequence of entire divisorial ideals of* D,
3. $(n!)_E = (0)$ *if and only if* $n \ge card(E)$,
4. *if* $E \subseteq F \subseteq D$, *then* $(n!)_E \subseteq (n!)_F$, *and hence,* $(n!)_E \times (n!)_F^{-1} \subseteq D$.

2. GENERALIZED v-ORDERINGS

The notion of v-ordering defined by Bhargava [2] for any subset of discrete valuation domains is a very fruitful notion in the study of integer-valued polynomials and generalized factorials. We are going to see that such a notion may also be useful for some subsets of non-discrete valuation domains.

Hypothesis. Let V be a valuation domain and let E be a subset of V. We denote by K the quotient field of V, by v the corresponding valuation of K, by $\mathfrak{m}$ the maximal ideal of V, and by Γ the value group of v.

Definition 2.1. A *v-ordering* of E is a (finite or infinite) sequence $\{a_n\}_{n=0}^{N}$ of distinct elements of E such that, for $1 \leq n \leq N$, one has:

$$v\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) \leq v\left(\prod_{k=0}^{n-1}(x - a_k)\right) \quad \text{for each } x \in E.$$

Remarks 2.2.

(*a*) In the case where the valuation v is discrete, there always exist v-orderings of E with $N < card(E)$ without any assumption on E. Such sequences may be constructed inductively on n choosing any element in E for a_0.

(*b*) If v is not discrete, we have to assume, at each step n, the existence of a minimum for $v(\prod_{k=0}^{n-1}(x - a_k))$. For instance, if $E = \mathfrak{m}$ and $\mathfrak{m}$ is not principal, then $\mathrm{Int}(\mathfrak{m}, V) = V[X]$, and hence, $(n!)_E^V = V$ for each n. On the other hand, $v(a - a_0) > 0$ for all a_0, $a \in \mathfrak{m}$, while $\inf_{x \in \mathfrak{m}} v(x - a_0) = 0$. Consequently, there does not exist any v-ordering (cf. [7, § 4]).

(*c*) The existence of a minimum is obviously satisfied if the subset E is finite, or more generally, if E is compact with respect to the topology induced by v, or even, if the completion $\widehat{E}$ of E is compact [7, § 4]. In fact, weaker conditions are enough. In the particular context of topologies defined by valuations, $\widehat{E}$ is compact if and only if, for each nonzero ideal $\mathfrak{I}$ of V, E meets only finitely many cosets of V modulo $\mathfrak{I}$. We extend such a property by considering the following one.

Proposition 2.3. *Let E be an infinite subset of the valuation domain V such that, for each $\gamma \in \Gamma$ of the form $\gamma = v(x - y)$ where $x, y \in E$ and $x \neq y$, E meets only finitely many cosets of V modulo $\mathfrak{I}_\gamma = \{z \in V \mid v(z) \geq \gamma\}$. Then there exist infinite v-orderings of E.*

Proof.

First step: for each $x_0 \in E$, the map

$$x \in E \mapsto v(x - x_0) \in \Gamma \cup \{+\infty\}$$

reaches a minimum on E.

Let $\gamma = v(y_0 - x_0)$ where $y_0 \in E$, $y_0 \neq x_0$ and let $\mathfrak{I}_\gamma = \{z \in V \mid v(z) \geq \gamma\}$. Then, there are finitely many $x_1, \ldots, x_r \in E$ such that:

$$E \subseteq \cup_{k=0}^{r} \{x_k + \mathfrak{I}_\gamma\} \quad \text{and} \quad v(x_j - x_i) < \gamma \text{ for } 0 \leq i \neq j \leq r.$$

If $r = 0$, then $\inf_{x \in E} v(x - x_0) = \gamma$.

If $r \geq 1$ then, for $k \geq 1$ and $x \in x_k + \mathfrak{I}_\gamma$, $v(x - x_0) = v(x_k - x_0)$; consequently,

$$\inf_{x \in E} v(x - x_0) = \inf_{k=1}^{r} v(x_k - x_0).$$

Second step: for each $a_1, a_2, \ldots, a_n \in E$, the map:

$$x \in E \mapsto v((x - a_1)(x - a_2)\ldots(x - a_n)) \in \Gamma \cup \{+\infty\},$$

reaches a minimum on E.

First note that, from every infinite sequence of elements of Γ, we may extract either an infinite increasing sequence, or an infinite strictly decreasing sequence. Assume that $x \mapsto g(x) = v((x-a_1)\dots(x-a_n))$ does not reach a minimum. Then, there exists an infinite sequence $\{y_k\}$ of elements of E such that $\{g(y_k)\}$ is strictly decreasing. Since the subset $\{y_k \mid k \in \mathbb{N}\}$ of E has the same property of finiteness, it follows from the first step that, for every $i \in \{1,\dots,n\}$, we cannot extract from the sequence $\{v(y_k - a_i)\}$ a strictly decreasing sequence. Consequently, we may extract from the sequence $\{y_k\}$ an infinite sequence $\{z_l\}$ such that, for every i, the sequence $\{v(z_l - a_i)\}$ is increasing. This is a contradiction with the fact that $\{g(z_l)\}$ is strictly decreasing. $\square$

Example 2.4. Let k be a field, let $\mathbb{Q}^+$ be the set of positive rational numbers, and let $K = k(\{T^r \mid r \in \mathbb{Q}^+\})$. Let v be the rank-one valuation on K such that $v(\sum_{k=0}^n a_k T^{r_k}) = \inf\{r_k \mid a_k \neq 0\}$ and let V be the corresponding valuation domain. For every strictly increasing sequence $\{r_n\}_{n\in\mathbb{N}}$ of positive rational numbers and every finite subset F of k containing 0, we consider the following subset of V:

$$E = \{k_0 t^{r_0} + k_1 t^{r_1} + \dots + k_l t^{r_l} \mid l \in \mathbb{N},\ k_0, k_1, \dots, k_l \in F\}.$$

This subset E has the property assumed in Proposition 2.3, and hence, there are infinite v-orderings of E. Note that the completion $\widehat{E}$ of E cannot be compact if the sequence $\{r_n\}$ is bounded (and $F \neq \{0\}$). We may obtain a v-ordering $\{a_n\}_{n\in\mathbb{N}}$ in the following way. Let $a_0 = 0, a_1, \dots, a_{q-1}$ be the elements of F. Writing, for each $n \in \mathbb{N}$,

$$n = n_0 + n_1 q + n_2 q^2 + \dots + n_s q^s \quad \text{where} \quad 0 \le n_i \le q-1,$$

we let

$$a_n = a_{n_0} T^{r_0} + a_{n_1} T^{r_1} + \dots + a_{n_s} T^{r_s}.$$

Indeed, denoting by $v_q(n)$ the greatest integer k such that q^k divides n, for each n and $m \in \mathbb{N}$ we have:

$$v(a_n - a_m) = r_{v_q(n-m)}.$$

We then may check that

$$v\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \sum_{l=1}^{n} r_{v_q(l)}$$

$$= \sum_{k\ge 0} r_k \left(\left[\frac{n}{q^k}\right] - \left[\frac{n}{q^{k+1}}\right]\right) = r_0 n + \sum_{k>0}\left[\frac{n}{q^k}\right](r_k - r_{k-1}).$$

Consequently, for $m \ge n$,

$$v\left(\prod_{k=0}^{n-1}(a_m - a_k)\right) = \sum_{k=0}^{n-1} r_{v_q(m-k)} = \sum_{l=1}^{m} r_{v_q(l)} - \sum_{l=1}^{m-n} r_{v_q(l)}$$

$$= r_0 n + \sum_{k>0}\left(\left[\frac{m}{q^k}\right] - \left[\frac{m-n}{q^k}\right]\right)(r_k - r_{k-1}).$$

By induction on n, it follows from the previous equalities that the sequence $\{a_n\}$ is a v-ordering of E since, for every $m \ge n$,

$$\left[\frac{m}{q^k}\right] - \left[\frac{m-n}{q^k}\right] \ge \left[\frac{n}{q^k}\right].$$

Now we recall the link between v-orderings and integer-valued polynomials.

Proposition 2.5. *Let $\{a_n\}_{n=0}^N$ be a sequence of distinct elements of E. Then, $\{a_n\}_{n=0}^N$ is a v-ordering of E if and only if the polynomials*

$$f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}$$

form a basis of the V-module

$$\mathrm{Int}_N(E, V) = \{f \in K[X] \mid f(E) \subseteq V, \deg(f) \leq N\}.$$

Proof. The sequence is a v-ordering of E if and only if, for each $n \leq N$, $v(f_n(a)) \geq v(f_n(a_n))$ for each $a \in V$, that is, $f_n(E) \subseteq V$. Moreover, the f_n's form a basis of the K-vector space $K_N[X] = \{g \in K[X] \mid \deg(g) \leq N\}$. Consequently, if the f_n's are in $\mathrm{Int}(E, V)$, then they form a basis of the V-module $\mathrm{Int}_N(E, V)$ since $f_n(a_n) = 1$ for each $n \leq N$. □

Note that there may be infinitely many v-orderings of E. Nevertheless, we have the following straightforward consequence:

Corollary 2.6. [2, Prop. 2.1] *If $\{a_n\}_{n=0}^N$ is a v-ordering of E, then for each $n \leq N$, one has:*

$$(n!)_E^V = \mathfrak{I}_n(E, V)^{-1} = \prod_{k=0}^{n-1} (a_n - a_k)V,$$

and the sum

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

does not depend on the choice of the v-ordering of E.

Remark 2.7. Note that if there exists a v-ordering $\{a_n\}_{n=0}^N$ of E then, for $0 \leq n < N$, $(n!)_E^V$ is a principal ideal. It follows from Remark 2.2 (b) that $(n!)_E$ may be principal even though there does not exist any v-ordering.

Corollary 2.8. *Assume that there exists a v-ordering $\{a_k\}_{k=0}^n$ of E and let $f \in \mathrm{Int}(E, V)$ of degree $\leq n$. Denote by $c(f)$ and $f(E)$ the fractional ideals of V generated respectively by the coefficients of f and by the values of f on E, and write:*

$$f(x) = \sum_{k=0}^{n} b_k \prod_{l=0}^{k-1} \frac{X - a_l}{a_k - a_l}.$$

(1) *$c(f)(n!)_E$ is an entire ideal.*

(2) *$f(E) = (f(a_0), f(a_1), \ldots, f(a_n)) = (b_0, \ldots, b_n)$.*

(3) *$c(f)(n!)_E \subseteq f(E) \subseteq c(f)$.*

Moreover, for $f = \prod_{k=0}^{n-1}(X - a_k)$, we have $c(f) = V$ and $f(E) = (n!)_E$.

Proof.

(1) results from the equality:

$$c(f) = \left(b_0, \frac{b_1}{a_1 - a_0}, \ldots, \frac{b_n}{\prod_{k=0}^{n-1}(a_n - a_k)}\right).$$

(2) Obviously,

$$f(E) \subseteq (b_0, \ldots, b_n) \subseteq (f(a_0), \ldots, f(a_n)) \subseteq f(E).$$

(3) Clearly, $f(E) \subseteq c(f)$. The equality in the proof of assertion (1) shows that $c(f)(n!)_E$ is contained in $(b_0, b_1, \ldots, b_n)$ which by (2) is equal to $f(E)$. □

3. RANK-ONE VALUATION DOMAINS

Hypothesis. In this section, V denotes a rank-one valuation domain (Γ is a subgroup of $\mathbb{R}$).

For every ideal $\mathfrak{I}$, denote by $v(\mathfrak{I})$ the valuation of $\mathfrak{I}$, that is,

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

Definition 3.1. If v is a rank-one valuation, the *characteristic function* of $\mathrm{Int}(E, V)$ is the arithmetic function w_E defined by:

$$n \in \mathbb{N} \mapsto w_E(n) = v\left((n!)_E^V\right) = -v\left(\mathfrak{I}_n(E, V)\right) \in \mathbb{N} \cup \{+\infty\}.$$

Such a sequence $w_E(n)$ was already considered in the special case where the valuation is discrete (as in [4] and [5]) or, more generally, where there exists a v-ordering (Corollary 2.6).

The characteristic function is an increasing function. More precisely, we have the following inequality which extends Property 1 of the classical factorials (*cf.* Introduction).

Proposition 3.2. *For each k, $l \in \mathbb{N}$, one has:*

$$w_E(k) + w_E(l) \leq w_E(k + l).$$

This inequality results from the obvious inclusion:

$$\mathfrak{I}_k(E, V) \cdot \mathfrak{I}_l(E, V) \subseteq \mathfrak{I}_{k+l}(E, V).$$

We can find some computations of this function w_E in [4] and [5]. Let us return to Example 2.4 and consider the case where $k = F = \mathbb{F}_q$ and $r_k = k$, that is, $V = \mathbb{F}_q[T]_{(T)}$ and $E = \mathbb{F}_q[T]$. We then have $w_E(n) = \sum_{k>0} \left[\frac{n}{q^k}\right]$. This is a particular case of the following result.

Proposition 3.3 (Pólya [17]). *If v is discrete and if q denotes the cardinality (finite or infinite) of the residue field of v, then*

$$w_V(n) = w_q(n) = \sum_{k>0} \left[\frac{n}{q^k}\right].$$

Again we generalize the notion of v-ordering.

Definition 3.4. Let $\varepsilon \geq 0$. A *v-ordering of E modulo ε* is a sequence $\{b_n\}_{n=0}^N$ of distinct elements of E such that, for each $n \leq N$, one has:

$$v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) \leq v\left(\prod_{k=0}^{n-1}(x - b_k)\right) + \varepsilon \quad \text{for every } x \in E.$$

For $\varepsilon = 0$, we have the classical notion of v-ordering. Although v-orderings do not necessarily exist, there always exist v-orderings modulo ε for every $\varepsilon > 0$. Such sequences may be constructed inductively on n choosing any element in E for b_0. Then, the link between v-orderings and integer-valued polynomials becomes:

Lemma 3.5. *Let $N < card(E)$, let $\varepsilon > 0$, and let $\{b_n\}_{n=0}^N$ be a v-ordering of E modulo ε. Every polynomial $f \in K[X]$ of degree $\leq N$ may be written:*

$$f(X) = \sum_{n=0}^{N} c_n \prod_{k=0}^{n-1} \frac{X - b_k}{b_n - b_k} \quad \text{with } c_n \in K.$$

If $v(c_n) \geq \varepsilon$ for each $n \leq N$, then f belongs to $\mathrm{Int}(E, V)$. *Conversely, if f belongs to* $\mathrm{Int}(E, V)$, *then $v(c_n) \geq -n\varepsilon$ for each $n \leq N$.*

Proof. For each $n \leq N$, let:

$$h_n(X) = \prod_{k=0}^{n-1} \frac{X - b_k}{b_n - b_k}.$$

Then,

$$f(X) = \sum_{n=0}^{N} c_n h_n(X).$$

By definition of the sequence $\{b_n\}$, for each $n \leq N$ and for each $x \in E$, one has $v(h_n(x)) \geq -\varepsilon$. Obviously, if $v(c_n) \geq \varepsilon$, then $v(c_n h_n(x)) \geq 0$ for each $x \in E$, and hence, f belongs to $\mathrm{Int}(E, V)$.

Conversely, assuming that f belongs to $\mathrm{Int}(E, V)$, let us prove by induction on n, that $v(c_n) \geq -n\varepsilon$. First, $f(b_0) = c_0 \in V$, and hence $v(c_0) \geq 0$. Let $n \in \{1, \ldots, N\}$ and suppose that $v(c_k) \geq -k\varepsilon$ for $0 \leq k \leq n-1$. Then,

$$f(b_n) = c_0 + c_1 h_1(b_n) + \ldots + c_{n-1} h_{n-1}(b_n) + c_n h_n(b_n).$$

We have $h_n(b_n) = 1$, $v(c_k) \geq -k\varepsilon$, and $v(h_k(b_n)) \geq -\varepsilon$ for $1 \leq k \leq n-1$. Consequently,

$$v(c_n) \geq \left(\inf_{0<k<n} v(c_k)\right) - \varepsilon \geq -n\varepsilon.$$

□

As an immediate consequence we have:

Lemma 3.6. *If $b_0, b_1, \ldots, b_N$ is a v-ordering modulo ε, then for $n \leq N$:*

$$v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) - \varepsilon \leq w_E(n) \leq v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) + n\varepsilon.$$

For every subset F of E and for every $n \in \mathbb{N}$, we have $w_E(n) \leq w_F(n)$ and, if there is a v-ordering $\{a_k\}_{k=0}^n$ of E, then $w_E(n) = w_F(n)$ where $F = \{a_k \mid 0 \leq k \leq n\}$. More generally:

Proposition 3.7. *For each $n \geq 0$,*

$$w_E(n) = \inf\{w_F(n) \mid F \subseteq E,\, card(F) = n+1\}.$$

Proof. Fix an $n < card(E)$ and an $\varepsilon > 0$. Let $b_0, b_1, \ldots, b_n$ be a v-ordering of E modulo ε and let $F = \{b_0, \ldots, b_n\}$. Then, $b_0, \ldots, b_n$ is also a v-ordering of F modulo ε, thus

$$w_F(n) - n\varepsilon \leq v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) \leq w_E(n) + \varepsilon.$$

Hence, for every $\varepsilon > 0$, there is a subset F of E such that $card(F) = n+1$ and $w_F(n) \leq w_E(n) + (n+1)\varepsilon$. □

Recall that, for every polynomial $g \in K[X]$, $g(E)$ denotes the fractional ideal generated by the values of g on E and that $v(\mathfrak{I})$ denotes the valuation of the ideal $\mathfrak{I}$. In particular,

$$v(g(E)) = \inf_{x \in E} v(g(x)).$$

Lemma 3.8. *For each monic polynomial $g \in K[X]$ of degree n, $v(g(E)) \leq w_E(n)$.*

Proof. Let $y \in K$ be such that $v(y) \geq -v(g(E))$. Then yg belongs to $\mathrm{Int}(E,V)$; and hence, $y \in \mathfrak{I}_n(E,V)$. Consequently, $v(y) \geq -v(g(E))$ implies $v(y) \geq -w_E(n)$; and hence, $v(g(E)) \leq w_E(n)$. □

Proposition 3.9. *For each $n \in \mathbb{N}$, we have:*

$$w_E(n) = \sup\{v(g(E)) \mid g \in K[X],\, \deg(g) = n,\, g\,\text{monic}\},$$

$$w_E(n) = \sup\{v(g(E)) \mid g \in V[X],\, \deg(g) = n,\, g\,\text{monic}\},$$

$$w_E(n) = \sup\{v(g(E)) \mid g = \prod_{k=0}^{n-1}(X - x_k),\text{ with } x_0, \ldots, x_{n-1} \in E\}.$$

Proof. If E is finite, we may assume that $n < card(E)$. Let $\varepsilon > 0$ and let $\{b_k\}_{k=0}^n$ be a v-ordering of E modulo ε. Consider the polynomial $g = \prod_{k=0}^{n-1}(X - b_k)$. It follows from Lemma 3.6 that:

$$w_E(n) \leq v\left(\prod_{k=0}^{n-1}(b_n - b_k)\right) + n\varepsilon.$$

Consequently, by definition of a v-ordering modulo ε,

$$w_E(n) \leq \inf_{x \in E} v\left(\prod_{k=0}^{n-1}(x - b_k)\right) + (n+1)\varepsilon,$$

that is,

$$w_E(n) \leq v(g(E)) + (n+1)\varepsilon.$$

Thus, $w_E(n) \leq v(g(E))$. The other inequality follows from Lemma 3.8. □

From now on, we will omit in the proofs the condition $n < card(E)$ because, if $n \geq card(E)$, then all the equalities correspond to $+\infty = +\infty$ or $0 = 0$.

Corollary 2.6 says that, if there is a v-ordering $\{a_k\}_{k=0}^n$, then:

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

More generally, the previous proposition shows that:

Corollary 3.10. *For each $n \geq 0$, we have:*

$$w_E(n) = \sup_{x_0,\ldots,x_{n-1}\in E}\ \inf_{x\in E} v\left(\prod_{k=0}^{n-1}(x - x_k)\right).$$

With Proposition 3.7, the previous corollary leads to the following result:

Corollary 3.11. *For each $n \geq 0$, we have:*

$$w_E(n) = \inf_{x_0,\ldots,x_n\in E}\ \sup_{0\leq i\leq n} v\Big(\prod_{0\leq k\leq n,\, k\neq i}(x_i - x_k)\Big).$$

Since $(n!)_E$ is a divisorial ideal, Proposition 3.9 leads to an assertion very similar to Property 3 of the classical factorials (*cf.* Introduction).

Theorem 3.12. *For each $f \in V[X]$, let $d(f,E)$ be the* fixed divisor *of f over E, that is, the divisorial ideal of V generated by the values of f on E. Then,*

$$(n!)_E = \cap\{d(f,E) \mid f \in V[X],\ \deg(f) = n,\ f\,\text{monic}\}.$$

Finally, analogously to Property 2 of the classical factorials, we have:

Theorem 3.13. *For each $n \in \mathbb{N}$,*

$$\inf_{x_0,\ldots,x_n\in E} v\Big(\prod_{0\leq i<j\leq n}(x_j - x_i)\Big) = \sum_{k=1}^{n} w_E(k).$$

If $\{a_k\}_{k=0}^n$ is a v-ordering, then:

$$v\Big(\prod_{0\leq i,j\leq n}(a_j - a_i)\Big) = \sum_{k=1}^{n} w_E(k).$$

Proof. Let $x_0,\ldots,x_n \in E$. We first prove that:

$$v\Big(\prod_{0\leq i<j\leq n}(x_j - x_i)\Big) \geq \sum_{k=1}^{n} w_E(k).$$

The proof is the same as that given by Bhargava for discrete valuations. Let $F = \{x_0, x_1, \ldots, x_n\}$. Assume that these $n+1$ elements are reordered so that the sequence $x_0, x_1 \ldots, x_n$ is a v-ordering of F. Then,

$$v\Big(\prod_{0\leq i<j\leq n}(x_j - x_i)\Big) = \sum_{j=1}^{n} v\left(\prod_{i=0}^{j-1}(x_j - x_i)\right) = \sum_{j=1}^{n} w_F(j) \geq \sum_{j=1}^{n} w_E(j)$$

since $F \subseteq E$ (see Proposition 1.3.4). In particular, if $x_0, \ldots, x_n$ is a v-ordering of E, then we have an equality.

Conversely, let $\varepsilon > 0$ and let $\{b_k\}_{k=0}^n$ be a v-ordering of E modulo ε. It follows from Lemma 3.6 that:

$$v\Bigg(\prod_{0\le i<j\le n}(b_j-b_i)\Bigg)=\sum_{j=1}^{n} v\left(\prod_{i=0}^{j-1}(b_j-b_i)\right)\le\sum_{j=1}^{n} w_E(j)+n\varepsilon.$$

Consequently,

$$\inf_{x_0,\ldots,x_n\in E} v\Bigg(\prod_{0\le i<j\le n}(x_j-x_i)\Bigg)\le\sum_{j=1}^{n} w_E(j)+n\varepsilon,$$

that is,

$$\inf_{x_0,\ldots,x_n\in E} v\Bigg(\prod_{0\le i<j\le n}(x_j-x_i)\Bigg)\le\sum_{j=1}^{n} w_E(j).$$

□

4. ASYMPTOTIC BEHAVIOR AND VALUATIVE CAPACITY

Hypothesis. As in the previous section, K is a field with a rank-one valuation v, V denotes the corresponding domain, q the cardinality of the residue field, and E is any subset of V.

Here we study the asymptotic behavior of the arithmetic function w_E. More precisely, we show that $\frac{w_E(n)}{n}$ has a limit and that this limit is also the limit of the sequence $\delta_E(n)$ where, for $n \geq 1$:

$$\delta_E(n)=\frac{2}{n(n+1)}\inf_{x_0,\ldots,x_n\in E} v\Bigg(\prod_{0\le i<j\le n}(x_j-x_i)\Bigg).$$

This limit will be denoted by δ_E and, by analogy with the Archimedean case (see for instance [11]), δ_E is called the *valuative capacity* of E (with respect to v).

Proposition 4.1. *The sequence $\{\delta_E(n)\}_{n\in\mathbb{N}^*}$ is an increasing sequence, and hence tends to a (finite or infinite) limit $\delta_E \in \mathbb{R}_+ \cup \{+\infty\}$.*

Proof. Let $x_0, \ldots, x_n$ be elements of E. It follows from the obvious formula:

$$\Bigg(\prod_{0\le i<j\le n}(x_j-x_i)\Bigg)^{n-1}=\prod_{k=0}^{n}\Bigg(\prod_{0\le i<j\le n,\, i,j\neq k}(x_j-x_i)\Bigg),$$

and from the inequality:

$$v\Bigg(\prod_{0\le i<j\le n,\, i,j\neq k}(x_j-x_i)\Bigg)\ge\frac{(n-1)n}{2}\times\delta_E(n-1),$$

that:

$$(n-1)v\Bigg(\prod_{0\le i<j\le n}(x_j-x_i)\Bigg)=\sum_{k=0}^{n} v\Bigg(\prod_{0\le i<j\le n,\, i,j\neq k}(x_j-x_i)\Bigg)\ge(n+1)\times\frac{(n-1)n}{2}\times\delta_E(n-1).$$

Consequently,

$$(n-1)\times\frac{n(n+1)}{2}\delta_E(n)\geq(n+1)\times\frac{(n-1)n}{2}\times\delta_E(n-1). \qquad \square$$

The limit δ_E is linked to the function w_E because of the formula given by Theorem 3.13:

$$\frac{1}{2}n(n+1)\delta_E(n)=w_E(1)+\ldots+w_E(n).$$

Theorem 4.2.

$$\lim_{n\to\infty}\frac{w_E(n)}{n}=\sup_{n\geq1}\frac{w_E(n)}{n}=\delta_E.$$

Proof.

First step: $\frac{w_E(n)}{n}$ tends to $\omega_E=\sup_{n\geq1}\frac{w_E(n)}{n}$.

If ω_E is finite (resp., infinite), let m be such that $\frac{w_E(m)}{m}$ is close to ω_E (resp., is large). For $n\geq m$, write $n=km+r$ with $0\leq r<m$. It follows from Proposition 3.2 that:

$$\omega_E\geq\frac{w_E(n)}{n}=\frac{w_E(km+r)}{km+r}\geq\frac{w_E(km)}{(k+1)m}\geq\frac{k}{k+1}\frac{w_E(m)}{m}.$$

Thus, for n large, k is large, $\frac{k}{k+1}\frac{w_E(m)}{m}$ is close to $\frac{w_E(m)}{m}$, and hence, $\frac{w_E(n)}{n}$ is close to ω_E (resp., is large).

Second step: $\omega_E=\delta_E$.

From the equalities:

$$\frac{1}{2}n(n+1)\delta_E(n)=w_E(1)+\ldots+w_E(n),$$

it follows that:

$$n(n+1)\delta_E(n)-(n-1)n\delta_E(n-1)=2w_E(n);$$

that is,

$$(n+1)\delta_E(n)-(n-1)\delta_E(n-1)=2\frac{w_E(n)}{n},$$

$$n\delta_E(n-1)-(n-2)\delta_E(n-2)=2\frac{w_E(n-1)}{n-1},\ldots$$

By addition,

$$\delta_E(1)+\delta_E(2)+\delta_E(n-1)+(n+1)\delta_E(n)=2\sum_{k=1}^{n}\frac{w_E(k)}{k},$$

or,

$$\frac{1}{n}(\delta_E(1)+\delta_E(2)+\ldots+\delta_E(n-1))+\Big(1+\frac{1}{n}\Big)\delta_E(n)=\frac{2}{n}\sum_{k=1}^{n}\frac{w_E(k)}{k}.$$

By Cesàro's theorem, the first term in the left side tends to δ_E, of course the second term also tends to δ_E, while the sum in the right side tends to $2\omega_E$, both by the first step and by Cesàro's theorem. $\square$

Of course, in some sense, the larger E is, the smaller δ_E becomes.

Examples 4.3.

(1) If V is a discrete valuation domain, it follows from Pólya's formula [Proposition 3.3] that:

$$\delta_V = \frac{1}{q-1}.$$

Then, for $a \in V$ and $b \in V^*$, we have:

$$\delta(a + bV) = \frac{1}{q-1} + v(b).$$

More generally, it follows from [4, Proposition 4.4] that if E is a finite union of classes modulo a nonzero ideal bV, that is,

$$E = \cup_{i=1}^{r} \{c_i + bV\}$$

and if, moreover, $v(c_i - c_j) = h < v(b)$ for every (i,j) with $i \neq j$, then

$$\delta_E = \frac{1}{r}\left(\frac{1}{q-1} + v(b) + h(r-1)\right).$$

In particular, let p be a prime number and let $V = \mathbb{Z}_{(p)}$ (and hence, $v = v_p$). It follows from [5, Proposition 5.4] that to the containments:

$$\mathbb{Z} \setminus p\mathbb{Z} \subset \mathbb{Z} \setminus p^2\mathbb{Z} \subset \mathbb{Z}$$

correspond the following inequalities for the valuative capacities:

$$\frac{p}{(p-1)^2} > \frac{p(p^2-p+1)}{(p-1)^2(p^2+1)} > \frac{1}{p-1}.$$

(2) On the other hand, δ_E may be infinite. Let V be a rank-one valuation domain and let t be an element of its maximal ideal. Then, $\{t^n \mid n \in \mathbb{N}\}$ is a v-ordering of $E = \{t^n \mid n \in \mathbb{N}\}$, $w_E(n) = \frac{n(n-1)}{2}v(t)$ and $\delta_E = +\infty$.

(3) The valuative capacity δ_E in Example 2.4 may be finite or infinite, since:

$$\delta_E = \left(1 - \frac{1}{q}\right)\sum_{k=0}^{\infty} \frac{r_k}{q^k},$$

and $\{r_k\}$ is any strictly increasing sequence of positive rational numbers.

5. DEDEKIND AND KRULL DOMAINS

By globalization, results on discrete valuation domains may be extended to Dedekind domains. We are going to show that some of the results obtained by Bhargava [3] for Dedekind domains may also be proved for Krull domains. We first begin with some results with respect to localization.

Notation. We now denote by D an integral domain with quotient field K and by E a subset of D.

Proposition 5.1. [8, Proposition 1.2] *If D is a Mori domain then, for each multiplicative subset S of D, one has:*

$$S^{-1}\text{Int}(E, D) = \text{Int}(E, S^{-1}D).$$

Recall that a Mori domain is a domain which satisfies the ascending chain condition on divisorial ideals. In particular, Noetherian domains and Krull domains are Mori domains.

Corollary 5.2. *If D is a Mori domain then, for each multiplicative subset S of D and each $n \in \mathbb{N}$, one has:*

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

$$(n!)_E^D = \cap_{\mathfrak{m}\in \max(D)} (n!)_E^{D_\mathfrak{m}}.$$

Proof. We just have to explain the second equality, that is, why the localization of the inverse of an ideal $\mathfrak{I}$ is equal to the inverse of the localization of $\mathfrak{I}$. This is an easy consequence of the fact that in a Mori domain, for each fractional ideal $\mathfrak{I}$, there exists a finitely generated fractional ideal $\mathfrak{J}$ such that $\mathfrak{I}^{-1} = \mathfrak{J}^{-1}$ [18, Théorème 1]. □

In a Krull domain, the divisorial ideals are characterized by their localization with respect to the height-one prime ideals:

Corollary 5.3. *If D is a Krull domain then, for each $n \in \mathbb{N}$, one has:*

$$(n!)_E^D = \cap_{\mathfrak{p}\in \mathrm{Spec}(D),\, ht(\mathfrak{p})=1} (n!)_E^{D_\mathfrak{p}}.$$

For each height-one prime ideal $\mathfrak{p}$ of the Krull domain D, $D_\mathfrak{p}$ is a discrete valuation domain. Let us denote by $w_{E,\mathfrak{p}}$ the function w_E corresponding to this valuation defined in Section 3. The previous corollary may be formulated in the following way:

If D is a Krull domain then, for each $n \in \mathbb{N}$,

$$(n!)_E = \cap_{\mathfrak{p}\in \mathrm{Spec}(D),\, ht(\mathfrak{p})=1} \mathfrak{p}^{w_{E,\mathfrak{p}}(n)} D_\mathfrak{p}.$$

For Dedekind domains, we obtain the well known result [3, § 2].

Corollary 5.4. *If D is a Dedekind domain then, for each $n \in \mathbb{N}$, one has:*

$$(n!)_E^D = \prod_{\mathfrak{m}\in \max(D)} (n!)_E^{D_\mathfrak{m}} = \prod_{\mathfrak{m}\in \max(D)} \mathfrak{m}^{w_{E,\mathfrak{m}}(n)}.$$

Examples 5.5. Let D be a Dedekind domain.

1. Let E be a subset, $\mathfrak{a}$ be an ideal, and b be an element of D. Let

$$F = b + \mathfrak{a}E = \{b + ax \mid a \in \mathfrak{a},\, x \in E\}.$$

Then,

$$(n!)_F = (n!)_E \times \mathfrak{a}^n.$$

In particular, for every ideal $\mathfrak{a}$ of D:

$$(n!)_\mathfrak{a} = (n!)_D \times \mathfrak{a}^n.$$

2. For every maximal ideal $\mathfrak{m}$ of D, let $N(\mathfrak{m}) = card(D/\mathfrak{m})$. Recall that $w_q(n) = \sum_{k>0} \left[\frac{n}{q^k}\right]$. Then,

$$(n!)_D = \prod_{\mathfrak{m}\in \max(D)} \mathfrak{m}^{w_{N(\mathfrak{m})}(n)} = \prod_{q=2}^{n} \Big(\prod_{N(\mathfrak{m})=q} \mathfrak{m}^{w_q(n)} \Big).$$

For any two divisorial ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a Krull domain D, the containment $\mathfrak{a} \subseteq \mathfrak{b}$ is equivalent to $v_{\mathfrak{p}}(\mathfrak{a}) \geq v_{\mathfrak{p}}(\mathfrak{b})$ for each height-one prime ideal $\mathfrak{p}$ of D. By globalization, it then follows from inequalities of Proposition 3.2:

Proposition 5.6. *If D is a Krull domain then, for each $k, l \in \mathbb{N}$,*

$$((k+l)!)_E \subseteq (k!)_E \cdot (l!)_E.$$

In particular, $((k+l)!)_E \cdot \mathfrak{I}_k(E,D) \cdot \mathfrak{I}_l(E,D)$ is an entire ideal of D.

Corollary 5.7. [3] *If D is a Dedekind domain then, for each $k, l \in \mathbb{N}$, the ideal $(k!)_E \cdot (l!)_E$ divides the ideal $((k+l)!)_E$.*

Analogously, the equality in Theorem 3.13 leads to:

Proposition 5.8. *If $a_0, a_1, \ldots, a_n$ are $n+1$ elements of a subset E of a Krull domain D, then*

$$\prod_{0 \leq i < j \leq n} (a_j - a_i) \in (1!)_E \cdot (2!)_E \cdots (n!)_E.$$

In particular, $\prod_{0 \leq i < j \leq n} (a_j - a_i)$ is a common denominator of the fractional ideal $\mathfrak{I}_1(E,D) \cdot \mathfrak{I}_2(E,D) \cdots \mathfrak{I}_n(E,D)$.

Finally, by globalization, Corollary 2.8 leads to the following extension of [2, Theorem 2].

Proposition 5.9. *For each $g \in K[X]$, let $d(g,E)$ be the divisorial fractional ideal generated by the values of g on E. If D is a Krull domain then, for each $n \in \mathbb{N}$, one has:*

$$(n!)_E = \cap\{d(g,E) \mid g \in D[X],\ \deg(g) = n,\ g \,\text{monic}\}.$$

Proof. Let $\mathfrak{a} = \cap\{d(g,E) \mid g \in D[X],\ \deg(g) = n,\ g\,\text{monic}\}$. If $g \in D[X]$ is a monic polynomial of degree n, then $(n!)_E \subseteq d(g,E)$ since this inclusion holds locally with respect to each height-one prime ideal of D. Thus, $(n!)_E \subseteq \mathfrak{a}$. Moreover, for each prime ideal $\mathfrak{p}$ of D, there is a monic polynomial $g_{n,\mathfrak{p}} \in D[X]$ of degree n such that $d(g_{n,\mathfrak{p}},E)D_{\mathfrak{p}} = (n!)_E^{D_{\mathfrak{p}}}$. Consequently, $\mathfrak{a}_{\mathfrak{p}} \subseteq d(g_{n,\mathfrak{p}},E)D_{\mathfrak{p}} = (n!)_E^{D_{\mathfrak{p}}}$. Since $\mathfrak{a}$ is divisorial, $\mathfrak{a} \subseteq (n!)_E$, and then we have an equality. □

Remark 5.10. Denote by $\mathfrak{J}_n(E,D)$ the fractional ideal of D generated by all the coefficients of the polynomials in $\text{Int}(E,D)$ of degree n. Obviously, we have: $\mathfrak{I}_n(E,D) \subseteq \mathfrak{J}_n(E,D)$. We do not know if these two fractional ideals are equal, but if D is a Krull domain it follows from assertion 3 of Corollary 2.8 that:

$$\mathfrak{J}_n(E,D)^{-1} = \mathfrak{I}_n(E,D)^{-1} = (n!)_E^D$$

since

$$\mathfrak{J}_n(E,D) = \cup\{c(f) \mid f \in \text{Int}(E,D),\ \deg(f) = n\}.$$

In particular, if D is a Dedekind domain, then $\mathfrak{J}_n(E,D) = \mathfrak{I}_n(E,D)$.

6. EXAMPLES AND D-ORDERINGS

To end this paper, let us come back to the introduction. We recalled that, if $a_0, a_1, \ldots, a_n$ are any $n+1$ integers, then the product:

$$\prod_{0 \leq i < j \leq n} (a_j - a_i) \quad \text{is divisible by} \quad 1! \ldots n!.$$

This fine result is not so easy to obtain; Bhargava [2] gave an enlightening proof with the notion of v-ordering. In fact, this result is a very particular case of Proposition 5.8, which concerns Krull domains and is itself a globalization of Theorem 3.13. One find another interesting proof in [19]. Applying L'Hôpital's rule to the factors of the function $P(t) = \prod_{0\leq i<j\leq n} \frac{t^{a_j-a_i}-1}{t^{j-i}-1}$, we obtain:

$$\lim_{t\to 1} P(t) = \prod_{0\leq i<j\leq n} \lim_{t\to 1} \frac{(a_j-a_i)t^{a_j-a_i-1}}{(j-i)t^{j-i-1}} = \prod_{0\leq i<j\leq n} \frac{a_j-a_i}{j-i}.$$

It follows from the next proposition that this rational number is in fact an integer.

Proposition 6.1 (Sury [19]). *For any integers $a_0 < a_1 < \ldots < a_n$,*

$$P(T) = \prod_{0\leq i<j\leq n} \frac{T^{a_j-a_i}-1}{T^{j-i}-1} \in \mathbb{Z}[T].$$

Sury's proof of this last assertion needs some computation. Following Bhargava, we wish to give a more enlightening proof using the notion of v-ordering in the localizations of the Krull domain (more precisely, unique factorization domain) $\mathbb{Z}[T]$.

Lemma 6.2. *Let $D = \mathbb{Z}[T]$ and $E = \{T^n \mid n \in \mathbb{N}\}$. The sequence $\{T^n\}_{n\in\mathbb{N}}$ is a v_π-ordering of E for every irreducible element π of $\mathbb{Z}[X]$.*

Proof. Either π is a prime number p, or π is an irreducible polynomial $Q(T)$ of $\mathbb{Q}[T]$ that we may suppose to be monic. Obviously, if $v_\pi(T^n - T^m) \neq 0$ for some $n \neq m$, then $\pi = T$ or $\Phi_d(T)$ where Φ_d denotes the d-th cyclotomic polynomial and d divides $n-m$. Consequently, we just have to check that $\{T^n\}$ is a v_π-ordering for $\pi = T$ or Φ_d. For $\pi = T$, this is Example 4.3.2. Let $d > 0$ and let us prove by induction on n that $\{T^k\}_{k=0}^n$ is a v_{Φ_d}-ordering. For every $m > n$, we have:

$$v_{\Phi_d}\left(\prod_{k=0}^{n-1}(T^m - T^k)\right) = v_{\Phi_d}\left(\prod_{k=m-n+1}^{m}(T^k-1)\right),$$

while

$$v_{\Phi_d}\left(\prod_{k=0}^{n-1}(T^n - T^k)\right) = v_{\Phi_d}\left(\prod_{k=1}^{n}(T^k-1)\right).$$

These quantities are respectively equal to:

$$card\{k \mid d|k,\ m-n+1 \leq k \leq m\}$$

and

$$card\{k \mid d|k,\ 1 \leq k \leq n\},$$

that is,

$$\left[\frac{m}{d}\right] - \left[\frac{m-n}{d}\right] \quad \text{and} \quad \left[\frac{n}{d}\right].$$

Clearly, this latter quantity is less or equal to the first one. □

Proof of the proposition. Let $a_0 < a_1 < \ldots < a_n$ be integers. We may assume that $a_0 \geq 0$. Theorem 3.13 together with Lemma 6.2 says that, for each irreducible element π of $\mathbb{Z}[X]$,

$$\prod_{0\leq i<j\leq n} \frac{T^{a_j} - T^{a_i}}{T^j - T^i} \in \mathbb{Z}[T]_\pi.$$

Consequently,

$$\prod_{0\leq i<j\leq n} \frac{T^{a_j} - T^{a_i}}{T^j - T^i} \in \mathbb{Z}[T].$$

Finally, $P(T) \in \mathbb{Z}[T]$ since $a_0 + a_1 + \ldots + a_n \geq 0 + 1 + \ldots + n$. $\square$

The sequence $\{T^n\}$ in $\mathbb{Z}[T]$ is a particular case of the following:

Definition 6.3. Let D be an integral domain and let E be a subset of D. A *D-ordering of E* is a sequence $\{a_n\}_{n=0}^N$ of distinct elements of E such that, for each $n \leq N$, $\prod_{k=0}^{n-1}(a_n - a_k)$ divides $\prod_{k=0}^{n-1}(x - a_k)$ for every $x \in E$.

This notion of D-ordering is in fact the same than the notion of *special sequence* introduced by Mulay [14, § 1.6] although both definitions are distinct. It is worth noticing that Mulay's Theorem 4 (*ii*) already showed the existence of such sequences for every subset of discrete valuation domains. The following assertion is straightforward.

Proposition 6.4. *Let $a_0, a_1, \ldots, a_N$ be distinct elements of E. The sequence $\{a_n\}_{n=0}^N$ is a D-ordering of E if and only if the polynomials:*

$$f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k} \quad (0 \leq n \leq N)$$

form a basis of:

$$\mathrm{Int}_n(E, D) = \{f \in \mathrm{Int}(E, D) \mid \deg(f) \leq n\}.$$

In that case, $(n!)_E = \prod_{k=0}^{n-1}(a_n - a_k)D$ for every $n \leq N$.

If D is a Krull domain, then $\{a_n\}_{n=0}^N$ is a D-ordering of E if and only if, for each height-one prime ideal $\mathfrak{p}$ of D, $\prod_{k=0}^{n-1} \frac{x-a_k}{a_n-a_k} \in D_\mathfrak{p}$ for each $x \in E$ and $n \leq N$, that is, $\{a_n\}_{n=0}^N$ is a $v_\mathfrak{p}$-ordering of E in $D_\mathfrak{p}$. The following assertion is a particular case of Proposition 5.8.

Proposition 6.5. *If D is a Krull domain and $\{a_n\}_{n=0}^N$ is a D-ordering of E, then for every $n \leq N$ and every choice of elements $x_0, x_1, \ldots, x_n \in E$,*

$$\prod_{0\leq i<j\leq n} \frac{x_i - x_j}{a_i - a_j} \in D.$$

Examples 6.6.

(1) The sequence $\{n\}_{n\in\mathbb{N}}$ is a $\mathbb{Z}$-ordering of $\mathbb{N}$.

(2) The sequence $\{n^2\}_{n\in\mathbb{N}}$ is a $\mathbb{Z}$-ordering of $\{n^2 \mid n \in \mathbb{N}\}$.

(3) The sequence $\{T^n\}_{n\in\mathbb{N}}$ is a $\mathbb{Z}[T]$ ordering of $\{T^n \mid n \in \mathbb{N}\}$.

(4) The sequence $\{q^n\}_{n\in\mathbb{N}}$ is a $\mathbb{Z}$-ordering of $\{q^n \mid n \in \mathbb{N}\}$.

(5) The sequence $\{1, 2, 3, 5\}$ is a $\mathbb{Z}$-ordering of the polynomial closure $\mathbb{P} \cup \{\pm 1\}$ of the set $\mathbb{P}$ of prime numbers. On the other hand, there does not exist any $\mathbb{Z}$-ordering with 5 elements, although, for each $N \in \mathbb{N}$, there are prime numbers $p_0, p_1, \ldots, p_N$ such that the polynomials $\frac{1}{\pi_n} \prod_{k=0}^{n-1}(X - p_k)$ form a basis of the $\mathbb{Z}$-module $\mathrm{Int}_N(\mathbb{P}, \mathbb{Z})$ where π_n denotes a generator of $(n!)_{\mathbb{P}}$ (cf [10]).

REFERENCES

[1] M. Bhargava, "The Factorial Function ... and Generalizations", *Amer. Math. Monthly*, **107** (2000), pp. 783–799.

[2] M. Bhargava, "P-Orderings and Polynomial Functions on Arbitrary Subsets of Dedekind Rings", *J. reine angew. Math.*, **490** (1997), pp. 101–127.

[3] M. Bhargava, "Generalized Factorials and Fixed Divisors Over Subsets of a Dedekind Domain", *J. Number Theory*, **72** (1998), pp. 67–75.

[4] J. Boulanger, J.-L. Chabert, S. Evrard, and 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), pp. 161–174. New York: Dekker.

[5] J. Boulanger and J.-L. Chabert, "Asymptotic Behavior of Characteristic Sequences of Integer-Valued Polynomials", *J. Number Theory*, **80** (2000), pp. 238–259.

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

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

[8] P.-J. Cahen, S. Gabelli, and E. Houston, "Mori Domains of Integer-Valued Polynomials", *J. Pure Appl. Algebra*, **153** (2000), pp. 1–15.

[9] J.-L. Chabert, "Une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers", *Canad. Math. Bull.*, **39** (1996), pp. 402–407.

[10] J.-L. Chabert, S. Chapman, and W. Smith, "A Basis for the Ring of Polynomials Integer-Valued on Prime Numbers", in *Factorization in Integral Domains, Lecture Notes in Pure and Appl. Math.* New York: Dekker, **189** (1997), pp. 271–284.

[11] M. Fekete, "Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten", *Math. Zeitsch.*, **17** (1923), pp. 228–249.

[12] D.L. McQuillan, "Rings of Integer-Valued Polynomials Determined by Finite Sets", *Proc. Roy. Irish Acad., Sect. A*, **85** (1985), pp. 177–184.

[13] D.L. McQuillan, "On Ideals in Prüfer domains of Polynomials", *Arch. Math.*, **45** (1985), pp. 517–527.

[14] S. B. Mulay, "On Integer-Valued Polynomials", in *Zero-Dimensional Commutative Rings, Lecture Notes in Pure and Appl. Math.* New York: Dekker, **171** (1995), pp. 331–345.

[15] A. Ostrowski, "Untersuchungen zur arithmetischen Theorie der Körper", *Math. Zeitsch.*, **39** (1935), pp. 269–404.

[16] G. Pólya, "Über ganzwertige ganze Funktionen", *Rend. Circ. Mat. Palermo*, **40** (1915), pp. 1–16.

[17] G. Pólya, "Über ganzwertige Polynome in algebraischen Zahlkörpern", *J. reine angew. Math.*, **149** (1919), pp. 97–116.

[18] J. Querré, "Sur une propriété des anneaux de Krull", *Bull. Sc. Math.*, **95** (1971), pp. 341–354.

[19] B. Sury, "An Integral Polynomial", *Math. Mag.*, **68** (1995), pp. 134–135.

[20] H. Zantema, "Integer Valued Polynomials Over a Number Field", *Manuscr. Math.*, **40** (1982), pp. 155–203.

Paper Received 26 September 2000; Revised 13 March 2001; Accepted 30 May 2001.