

---

# Old problems and new questions around integer-valued polynomials and factorial sequences

Jean-Luc Chabert<sup>1</sup> and Paul-Jean Cahen<sup>2</sup>

<sup>1</sup> Université de Picardie, LAMFA CNRS-UMR 6140, Faculté de Mathématiques, 33 rue Saint Leu, 80039 Amiens Cedex 01, France

[jean-luc.chabert@u-picardie.fr](mailto:jean-luc.chabert@u-picardie.fr)

<sup>2</sup> Université Paul Cézanne Aix-Marseille III, LATP CNRS-UMR 6632, Faculté des Sciences et Techniques, 13397 Marseille Cedex 20, France

[paul-jean.cahen@univ.u-3mrs.fr](mailto:paul-jean.cahen@univ.u-3mrs.fr)

*It is but natural, in this tribute to the work of Robert Gilmer, to write a few words about him. Robert showed extremely helpful, in many ways, for our book on Integer-valued Polynomials; he made numerous useful comments and was kind enough to undertake a very scrupulous proofreading. It could also be underlined that he promoted the notation  $\text{Int}(D)$  which seems now to be universally adopted. It is thus our pleasure, to dedicate this paper to Robert.*

## 1 On Bhargava's factorials

### 1.1 Arithmetical viewpoint

The first generalization of the notion of factorials can probably be attributed to Carlitz [8]. It stems from the arithmetical analogy between the ring  $\mathbb{Z}$  of integers and the ring  $\mathbb{F}_q[T]$  of polynomials over a finite field: both rings are principal ideal domains with finite residue fields, finite group of units and an infinite number of irreducible elements. With respect to this analogy, monic polynomials correspond to natural numbers and monic irreducible polynomials to prime numbers. The construction of *Carlitz factorials* is a little mysterious. He first defines, for each positive integer  $j$ , a polynomial  $D_j$  that may be interpreted as a piece of factorial:

$$D_j = \prod_{f \text{ monic, } \deg(f)=j} f \quad (1)$$

Then, for each positive integer  $n$  with  $q$ -adic expansion:

$$n = n_0 + n_1q + \dots + n_sq^s \quad (0 \leq n_j < q), \quad (2)$$

Carlitz defines the  $n$ -th factorial by:

$$n!_{\mathcal{C}} = \prod_{j=0}^s D_j^{n_j}. \quad (3)$$

We shall clarify that this may somehow be called a factorial by relating this construction to other generalizations.

## 1.2 Number theoretical viewpoint

Here is another generalization replacing the ring  $\mathbb{Z}$  by the ring  $\mathcal{O}_K$  of integers of a number field  $K$ . We first interpret the classical factorial as a product of powers of prime numbers, the power of  $p$  being given by *Legendre's formula*:

$$n! = \prod_{p \in \mathbb{P}} p^{w_p(n)} \quad \text{where} \quad w_p(n) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor. \quad (4)$$

We then analogously define the  $n$ -th factorial with respect to  $K$  as a product of powers of maximal ideals of  $\mathcal{O}_K$ :

$$n!_{\mathcal{O}_K} = \prod_{\mathfrak{p} \in \text{Max}(\mathcal{O}_K)} \mathfrak{p}^{w_{\mathfrak{p}}(n)}, \quad (5)$$

where the power of  $\mathfrak{p}$  is linked to its norm  $q = N(\mathfrak{p}) = \text{Card}(\mathcal{O}_K/\mathfrak{p})$  by a formula very close to Legendre's formula:

$$w_{\mathfrak{p}}(n) = w_q(n) = \sum_{k \geq 1} \left\lfloor \frac{n}{q^k} \right\rfloor. \quad (6)$$

Note that here factorials are not elements, like numbers in  $\mathbb{Z}$  or polynomials in  $\mathbb{F}_q[T]$ , but ideals of the ring  $\mathcal{O}_K$ . These ideals may first be traced in Pólya's work on integer-valued polynomials in 1919 [33], although factorials were not mentioned, and later in papers by Gunji and McQuillan [25] in 1970 and by Zantema [40] in 1982.

## 1.3 Algebraic viewpoint

The previous generalization can naturally be extended with a commutative algebraic viewpoint, replacing more generally the ring  $\mathcal{O}_K$  by a Dedekind domain  $D$ . The corresponding  $n$ -th factorial ideal  $n!_D$  appears as a product of prime ideals as in (5), the power  $w_{\mathfrak{p}}(n)$  of  $\mathfrak{p}$  being given by formula (6), using the norm  $q = N(\mathfrak{p}) = \text{Card}(D/\mathfrak{p})$ . Note that, if  $q = +\infty$ , then  $w_q(n) = 0$ , so that a maximal ideal with an infinite residue field does not appear in

any factorial ideal. Factorial ideals apply in particular to rings of integers of function fields, that is, finite algebraic extensions of  $\mathbb{F}_q(T)$  (compare with  $\Gamma$ -ideals of Goss [24]).

If  $D$  is a principal ideal domain, factorials can be interpreted as elements of  $D$ . In particular, letting  $D$  be the ring  $\mathbb{F}_q[T]$ , we obtain Carlitz factorials thanks to *Sinott's formula* [24, Thm 9.1.1]:

$$n!_C = \prod_{f \text{ monic, irreducible}} f^{w_f(n)} \quad \text{where} \quad w_f(n) = \sum_{k \geq 1} \left\lfloor \frac{n}{q^k \deg(f)} \right\rfloor. \quad (7)$$

Indeed the norm of the (principal prime) ideal  $f\mathbb{F}_q[t]$  is obviously given by

$$N(f\mathbb{F}_q[t]) = \text{Card}(\mathbb{F}_q[t]/f\mathbb{F}_q[t]) = q^{\deg(f)}.$$

#### 1.4 Multiplicative viewpoint

Write the usual factorial as

$$n! = \prod_{k=0}^{n-1} (n-k).$$

If we replace the natural sequence  $0, 1, 2, 3, \dots$  by a geometrical sequence  $1, q, q^2, q^3, \dots$ , where  $q$  denotes an integer,  $q \geq 2$ , we obtain the *Jackson factorials* [27]:

$$n!_q = \prod_{k=0}^{n-1} (q^n - q^k). \quad (8)$$

This is a different kind of generalization: now it is not the ring of integers  $\mathbb{Z}$  which is replaced by a Dedekind domain  $D$  but the subset  $\mathbb{N}$  of  $\mathbb{Z}$  which is replaced by another subset  $S$  (as here  $S = \{q^n \mid n \in \mathbb{N}\}$ ). In fact, all these generalizations are particular cases of the following one.

#### 1.5 Combinatorial viewpoint

*Bhargava's factorials* were introduced in 1997 [4]. For a Dedekind domain  $D$  and a subset  $S$  of  $D$ , Bhargava defined factorial ideals by means of the following local notion of  $\mathfrak{p}$ -ordering, where  $\mathfrak{p}$  is a maximal ideal of  $D$  and  $v_{\mathfrak{p}}$  denotes the corresponding valuation.

**Definition 1.1.** A  $\mathfrak{p}$ -ordering of  $S$  is a sequence  $\{a_n\}_{n \in \mathbb{N}}$  in  $S$  such that, for each  $n > 0$ ,  $a_n$  minimizes the expression

$$v_{\mathfrak{p}} \left( \prod_{k=0}^{n-1} (a_n - a_k) \right).$$

Thus,  $a_0$  being arbitrarily chosen,

$$v_{\mathfrak{p}}(a_1 - a_0) = \inf_{s \in S} v_{\mathfrak{p}}(s - a_0)$$

and, inductively, for each  $n > 0$ ,

$$v_{\mathfrak{p}} \left( \prod_{k=0}^{n-1} (a_n - a_k) \right) = \inf_{s \in S} v_{\mathfrak{p}} \left( \prod_{k=0}^{n-1} (s - a_k) \right). \tag{9}$$

Obviously, such  $\mathfrak{p}$ -orderings always exist and are not unique. However, as we shall see in the next section, the value of (9) does not depend on the choice of the  $\mathfrak{p}$ -ordering of  $S$ . Thus, letting

$$w_{S,\mathfrak{p}}(n) = v_{\mathfrak{p}} \left( \prod_{k=0}^{n-1} (a_n - a_k) \right) \tag{10}$$

Bhargava defined the  $n$ -th factorial ideal of  $S$  with respect to  $D$  by the formula:

$$n!_S^D = \prod_{\mathfrak{p} \in \text{Max}(D)} \mathfrak{p}^{w_{S,\mathfrak{p}}(n)}. \tag{11}$$

One may check that formula (11) generalizes all previously mentioned ones. Moreover, as shown by Bhargava [5], there are many reasons that allow us to consider it a good generalization. For instance, here are 3 of its nice properties:

It is well known that	We also have
For all $k, l \in \mathbb{N}$ $k!l!$ divides $(k+l)!$ in $\mathbb{Z}$	For all $k, l \in \mathbb{N}$ $k!_S^D l!_S^D$ divides $(k+l)!_S^D$ as ideals of $D$
For all $x_0, x_1, \dots, x_n \in \mathbb{Z}$ $\prod_{0 \leq i < j \leq n} (x_j - x_i)$ is divisible by $1! \times 2! \times \dots \times n!$	For all $x_0, x_1, \dots, x_n \in S$ $\prod_{0 \leq i < j \leq n} (x_j - x_i) D$ is divisible by $1!_S^D \times 2!_S^D \times \dots \times n!_S^D$
For all $f \in \mathbb{Z}[X]$ $f$ monic, $\deg(f) = n$ the GCD of $\{f(k) \mid k \in \mathbb{Z}\}$ divides $n!$ (Pólya 1915)	For all $f \in D[X]$ $f$ monic, $\deg(f) = n$ the ideal generated by $\{f(s) \mid s \in S\}$ divides $n!_S^D$

**1.6 Last generalization: Integer-valued polynomial viewpoint**

We finally allow  $D$  to be any domain with quotient field  $K$  (not restricting ourselves to Dedekind domains,  $D$  could for instance be an order of a number field). For a subset  $S$  of  $D$  we consider the ring of *integer-valued polynomials* on  $S$  with respect to  $D$ :

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

We then set the following.

**Definition 1.2.** The  $n$ -th factorial ideal of  $S$  with respect to  $D$  is defined by:

$$n!_S^D = \{a \in D \mid af \in D[X], \forall f \in \text{Int}(S, D), \deg(f) \leq n\}.$$

Hence, the ideals  $\{n!_S^D\}_{n \in \mathbb{N}}$  form a decreasing sequence of ideals of  $D$  with  $0!_S^D = D$ .

**Proposition 1.3.** Definition 1.2 generalizes Formula (11).

*Proof.* Assume  $D$  to be a Dedekind domain. We may look at things locally since, for every maximal ideal  $\mathfrak{p}$  of  $D$ , one has (see for instance [7, 1.2.7]):

$$\text{Int}(S, D)_{\mathfrak{p}} = \text{Int}(S, D_{\mathfrak{p}}).$$

Now fix a maximal ideal  $\mathfrak{p}$  of  $D$  and consider a  $\mathfrak{p}$ -ordering  $\{a_n\}_{n \in \mathbb{N}}$  of  $D$ . It follows from the definition of  $\mathfrak{p}$ -orderings that the Lagrange polynomials

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

form a basis of the  $D_{\mathfrak{p}}$ -module  $\text{Int}(S, D_{\mathfrak{p}})$ . Consequently,  $af \in D_{\mathfrak{p}}[X]$  for every  $f \in \text{Int}(S, D)$  such that  $\deg(f) \leq n$ , if and only if,  $a$  is divisible by  $\prod_{k=0}^{n-1} (a_n - a_k)$  in  $D_{\mathfrak{p}}$ , that is,

$$n!_S^D D_{\mathfrak{p}} = \mathfrak{p}^{w_{S,\mathfrak{p}}(n)} D_{\mathfrak{p}} \quad \text{where} \quad w_{S,\mathfrak{p}}(n) = v_{\mathfrak{p}} \left( \prod_{k=0}^{n-1} (a_n - a_k) \right). \square$$

*Remark 1.4.* With Definition 1.2, it is easy to see that, for a Dedekind domain:

- 1) The function  $w_{S,\mathfrak{p}}$  defined by (10) does not depend on the choice of the  $\mathfrak{p}$ -ordering of  $S$ .
- 2) The product  $k!_S^D l!_S^D$  divides  $(k+l)!_S^D$  since the product of two integer-valued polynomials of respective degree  $k$  and  $l$  is an integer-valued polynomial of degree  $k+l$ .
- 3) If  $S \subseteq T \subseteq D$ , then  $n!_T^D$  divides  $n!_S^D$  since  $\text{Int}(T, D) \subseteq \text{Int}(S, D)$ .

## 2 Examples and questions on factorials

### 2.1 An example in non-commutative algebra: Hurwitz quaternions

In the previous definition of factorial ideals we just need to consider  $\text{Int}(S, D)$  as a  $D$ -module. This allows for instance to consider the ring  $\mathbb{H}$  of *Hurwitz quaternions*, that is,

$$\mathbb{H} = \left\{ a + bi + cj + dk \mid (a, b, c, d) \in \mathbb{Z}^4 \text{ or } \left(\mathbb{Z} + \frac{1}{2}\right)^4 \right\}$$

One knows that  $\mathbb{H}$  is a non-commutative principal ideal domain with quotient field:

$$\mathbb{H}(\mathbb{Q}) = \{a + bi + cj + dk \mid (a, b, c, d) \in \mathbb{Q}^4\}$$

Now consider the left  $\mathbb{H}$ -module of integer-valued polynomials on  $\mathbb{H}$ :

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

The corresponding factorial ideals  $n!_{\mathbb{H}}$  are left ideals of  $\mathbb{H}$ . The first ideals are:

$$0!_{\mathbb{H}} = 1!_{\mathbb{H}} = 2!_{\mathbb{H}} = 3!_{\mathbb{H}} = \mathbb{H} \text{ and } 4!_{\mathbb{H}} = \mathbb{H} \frac{1+i}{2}.$$

The value of  $4!_{\mathbb{H}}$  follows from the fact that  $\frac{1+i}{2}(X^4 - X)$  is integer-valued (Gerboud [19]).

**Question A.** Find a formula for the (principal) factorial ideals  $n!_{\mathbb{H}}$  with  $n \geq 5$ .

### 2.2 Factorials of the prime numbers and Bernoulli polynomials

Factorials of the set  $\mathbb{P}$  of prime numbers (with respect to  $\mathbb{Z}$ ) are given by the formula [12]:

$$n!_{\mathbb{P}} = \prod_{p \in \mathbb{P}} p^{\omega_p(n)} \text{ where } \omega_p(n) = \sum_{k \geq 0} \left[ \frac{n-1}{(p-1)p^k} \right]. \tag{12}$$

The first terms of this sequence are

1, 1, 2, 24, 48, 5 760, 11 520, 2 903 040, 5 806 080, 1 393 459 200, ...

If we look at *The On-line Encyclopedia of Integer sequences* [34], we find another sequence with the same first terms: Sequence A075265 defined by Paul D. Hanna as the sequence  $(d_n)_{n \in \mathbb{N}}$  such that

$$\begin{aligned} \left( -\frac{\log(1-x)}{x} \right)^m &= \left( \sum_{k=1}^{\infty} \frac{x^k}{k+1} \right)^m \\ &= 1 + \frac{m}{2} x + \frac{m(3m+5)}{24} x^2 + \dots = \sum_{n \geq 1} \frac{1}{d_n} C_n(m) x^n \end{aligned} \tag{13}$$

where  $d_n \in \mathbb{N}$  and the polynomial  $C_n(m) \in \mathbb{Z}[m]$  is primitive of degree  $n$ . Experimental checking suggests and theoretical proof [11] shows that:

$$d_n = (n+1)!_{\mathbb{P}}$$

Moreover, superseeker@research.att.com suggests (and it may be proved) that

$$(n+1)!_{\mathbb{P}} = n! \times e_n$$

where  $e_n$  is the  $n^{\text{th}}$  term of Sequence A0011898 formed by the denominators of Bernoulli polynomials. More precisely, the  $n^{\text{th}}$  Bernoulli polynomial of order  $m$ , denoted by  $B_n^{(m)}$ , is defined by:

$$\left(\frac{t}{e^t - 1}\right)^m = \sum_{n=0}^{\infty} B_n^{(m)} \frac{t^n}{n!} \quad (14)$$

and may be written:

$$B_n^{(m)} = \frac{1}{e_n} D_n(m)$$

where  $e_n \in \mathbb{N}$  and the polynomial  $D_n(m) \in \mathbb{Z}[m]$  is primitive. Thus, we have:

**Proposition 2.1.**

$$\left(\frac{t}{e^t - 1}\right)^m = \sum_{n=0}^{\infty} D_n(m) \frac{t^n}{(n+1)!_{\mathbb{P}}} \quad (15)$$

where  $D_n(m) \in \mathbb{Z}[m]$  is primitive.

Such a link with denominators of Bernoulli numbers had been previously suggested by Bhargava [5, Example 21].

**Question B.** Explain the relation between the sequence of factorials of  $\mathbb{P}$  and the sequence of denominators of either Bernoulli numbers or Bernoulli polynomials.

### 2.3 Subsets with the same factorial sequences

The following question seems to be natural:

**Question C.** Let  $S$  and  $T$  be two subsets of an integral domain  $D$ . Under which conditions the factorial sequences of  $S$  and  $T$  are equal?

These factorial sequences are obviously equal if  $S$  and  $T$  are *polynomially equivalent*, that is,  $\text{Int}(S, D) = \text{Int}(T, D)$  (see for instance [7, Chapter IV] or [15, section 2] with a new approach to polynomial closure). This is far from necessary! Indeed if  $T = uS + a = \{us + a \mid s \in S\}$  where  $a \in A$  and  $u$  is a unit of  $A$ , the factorial sequences of  $S$  and  $T$  are clearly equal.

For an infinite subset  $S$  of  $\mathbb{Z}$ , Gilmer and Smith conjectured [23] that, if  $f \in \text{Int}(S, \mathbb{Z})$  is such that  $\text{Int}(S, \mathbb{Z}) = \text{Int}(f(S), \mathbb{Z})$ , then  $\deg(f) = 1$  (see also the question following Theorem 1.6 in [15]). Fares [17] proved this conjecture by establishing that, in fact, if  $S$  and  $f(S)$  have the same factorial sequences, then  $\deg(f) = 1$ . He even recently extended this result [18] with the following:

**Proposition 2.2.** *Let  $\mathcal{O}_K$  be the ring of integers of any number field  $K$  and let  $S$  be any infinite subset of  $\mathcal{O}_K$ . If  $\varphi(X) \in K(X)$  is a rational function such that  $S$  and  $\varphi(S)$  have the same factorial sequences, then  $\varphi$  is an homographic function (i.e., a rational function of the form  $\frac{aX+b}{cX+d}$  with  $ad - bc \neq 0$ ).*

This suggests two more questions:

**Question C1.** Does Fares' result hold for ring of integers of function fields?

**Question C2.** Assume that  $S$  is an infinite subset of the ring  $\mathcal{O}_K$  of integers of a number field  $K$ . Let  $f$  and  $g \in \text{Int}(S, \mathcal{O}_K)$ . Does the equality of the factorial sequences of  $f(S)$  and  $g(S)$  imply that  $g = f \circ h$  where  $\deg(h) = 1$ ?

Even in the case of the ring  $\mathbb{Z}$ , there are nevertheless examples of subsets  $S$  and  $T$  with the same factorial sequences such that  $T$  is not of the form  $uS + a$  where  $a \in A$  and  $u$  is a unit of  $A$ :

1) when the subsets are finite: for instance, the three subsets  $S = \{0, 2, 35\}$ ,  $T = \{0, 7, 22\}$  and  $U = \{0, 10, 21\}$  have the same factorial sequences but there does not exist any polynomial  $f$  of degree 1 such that either  $T = f(S)$ , or  $U = f(S)$ , or  $U = f(T)$ .

2) when  $T$  is not assumed to be the image of  $S$  by a polynomial, as for instance:

$$S = 5\mathbb{Z} \cup (1 + 5\mathbb{Z}) \quad \text{and} \quad T = 5\mathbb{Z} \cup (2 + 5\mathbb{Z})$$

For a subset  $S$  of  $\mathbb{Z}$ , A. Crabbe [16] tried to test the factorial sequence on finite subsets. For each prime number  $p$  and each  $r \geq 1$ , set

$$S \bmod(p^r) = \{0 \leq a < p^r \mid \exists s \in S \text{ such that } s \equiv a \pmod{p^r}\}.$$

Gilmer characterized the subsets  $S$  such that  $\text{Int}(S, \mathbb{Z}) = \text{Int}(\mathbb{Z})$  as the subsets which are prime power complete, that is, such that  $S \bmod(p^r) = \{0 \leq a < p^r\}$ , for each prime  $p$  and each  $r \geq 1$  [20, Theorem 2]. More generally, it follows from [7, IV.§1 and §2] that two subsets  $S$  and  $T$  of  $\mathbb{Z}$  are polynomially equivalent if and only they have the same  $p$ -adic completion for each  $p$  and hence, if and only if  $S \bmod(p^r) = T \bmod(p^r)$  for each  $p \in \mathbb{P}$  and each  $r \geq 1$ . Crabbe asked the following question [16, Conjecture 3.3].

**Question C3.** Is the equality of the factorial sequences of two subsets  $S$  and  $T$  of  $\mathbb{Z}$  characterized by the equalities of the factorial sequences of  $S \bmod(p^r)$  and  $T \bmod(p^r)$  for each  $p \in \mathbb{P}$  and each  $r \geq 1$ ?

He proved one way: if  $S \bmod(p^r)$  and  $T \bmod(p^r)$  have the same factorial sequences, for each  $p \in \mathbb{P}$  and each  $r \geq 1$ , then  $S$  and  $T$  have the same factorial sequences. He proved the converse for  $S \subseteq T = \mathbb{Z}$ . In fact, whenever  $S \subseteq T$ , if  $S$  and  $T$  have the same factorial sequences, then  $\text{Int}(S, \mathbb{Z}) = \text{Int}(T, \mathbb{Z})$ , thus  $S \bmod(p^r) = T \bmod(p^r)$  for each  $p \in \mathbb{P}$  and each  $r \geq 1$ . A fortiori,  $S \bmod(p^r)$  and  $T \bmod(p^r)$  have the same factorial sequences.

## 2.4 Several indeterminates

Another natural question is:

**Question D.** What would be a good generalization of the notion of factorials to several indeterminates?

Let  $n$  be a positive integer,  $D$  be an integral domain with quotient field  $K$ , and  $\underline{S}$  be a subset of  $D^n$ . Denote by  $\text{Int}(\underline{S}, D)$  the ring of integer-valued polynomials in several indeterminates on  $\underline{S}$ , that is:

$$\text{Int}(\underline{S}, D) = \{f \in K[\underline{X}] \mid \forall \underline{a} \in \underline{S}, f(\underline{a}) \in D\}$$

where  $\underline{X} = (X_1, \dots, X_k)$ . For each  $\underline{k} = (k_1, \dots, k_n) \in \mathbb{N}^k$ , a definition of the  $\underline{k}$ -th factorial ideal of  $\underline{S}$  with respect to  $D$  could be:

$$\underline{k}!_{\underline{S}}^D = \{a \in D \mid \forall f \in \text{Int}(\underline{S}, D), \text{ such that } \deg_{X_j}(f) \leq k_j, af \in D[\underline{X}]\}.$$

As noticed by Ostrowski [35], if  $D = \mathbb{Z}$  and  $\underline{S} = \mathbb{Z}^n$ , then one has:

$$\underline{k}! = k_1! \cdots k_n!$$

since the products  $\binom{X_1}{k_1} \cdots \binom{X_n}{k_n}$  form a basis of the  $\mathbb{Z}$ -module  $\text{Int}(\mathbb{Z}^n, \mathbb{Z})$ . More generally, if  $D$  is a Dedekind domain and  $\underline{S}$  is of the form  $S_1 \times \cdots \times S_n$ , then (see [25] and [7, § XI.1]):

$$\underline{k}!_{\underline{S}}^D = \prod_{j=1}^n k_j!_{S_j}^D.$$

But, if  $\underline{S}$  is more general, the question is much more difficult. There are some partial studies by Mulay [30] and Bhargava [5, § 12].

### 3 Simultaneous orderings

#### 3.1 Newtonian orderings (or simultaneous $\mathfrak{p}$ -orderings)

Recall that the polynomials

$$\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!} = \prod_{k=0}^{n-1} \frac{X-k}{n-k}.$$

form a basis of the  $\mathbb{Z}$ -module  $\text{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$ . This is linked to Gregory-Newton interpolation formula ([7], Historical Introduction). More generally, the unique degree  $n$  polynomial that interpolates a function  $f$  at a given set of  $n+1$  distinct arguments  $\{a_n\}_{0 \leq n \leq N}$  can be written in different manners and, in particular, as the *Newton's interpolation polynomial* [32], that is, as a linear combination of the polynomials:

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

By analogy, we introduce the following definition.

**Definition 3.1.** Let  $D$  be a domain and  $E$  be a subset of  $D$ . A sequence  $\{a_n\}_{n \in \mathbb{N}}$  of distinct elements of  $E$  is said to be an infinite Newtonian ordering for  $E$  in  $D$ , or shortly an ordering for  $E$ , if the polynomials

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

form a basis of the  $D$ -module  $\text{Int}(E, D)$ .

It is easy to establish the following.

**Lemma 3.2.** A sequence  $\{a_n\}$  is an ordering for  $E$  in  $D$  if and only if the polynomials  $f_n$  belong to  $\text{Int}(E, D)$ .

Infinite orderings do not necessarily exist and thus, for a given integer  $N$ , one may consider orderings of length  $N$ , that is, finite sequences  $\{a_n\}_{0 \leq n < N}$  such that the interpolation polynomials  $\{f_n\}_{0 \leq n < N}$  belong to  $\text{Int}(E, D)$ .

**Question E.** [5, Quest. 30] Characterize the subsets of  $\mathbb{Z}$  which admit an infinite Newtonian ordering.

Here are some examples (see [5]):

- 1)  $0, 1, \dots, n, \dots$  is an infinite ordering for  $\mathbb{N}$ , and also for  $\mathbb{Z}$ .
- 2)  $1^2, 2^2, \dots, n^2, \dots$  is an infinite ordering for  $\{n^2 \mid n \in \mathbb{N}\}$
- 3)  $1, q, q^2, \dots, q^n, \dots$  is an infinite ordering for  $\{q^n \mid n \in \mathbb{N}\}$ .

On the other hand, there exists an infinite ordering for  $\{n^k \mid n \in \mathbb{N}\}$  or for  $\{n^k \mid n \in \mathbb{Z}\}$  if and only if  $k = 1$  or  $2$ .

Of course, one can study subsets of other rings, in particular of Dedekind domains. For instance, in line with our third example above, for every non-constant polynomial  $g \in \mathbb{F}_q[T]$ , the sequence  $1, g, g^2, \dots, g^n, \dots$  is an infinite ordering for  $\{g^n \mid n \in \mathbb{N}\}$  in  $\mathbb{F}_q[T]$ .

A few facts are relevant in the study of orderings, whether infinite or of length  $N$ , for a subset of a domain  $D$ :

- 1) Orderings are related to factorial ideals: if  $\{a_n\}$  is an infinite ordering for  $E$  in  $D$  (resp. an ordering of length  $N$ ), then each factorial ideal  $n!_E^D$  (resp. each factorial ideal up to  $N$ ) is generated by  $\prod_{k=0}^{n-1} (a_n - a_k)$  and, in particular, is principal.
- 2) Local behaviour: it follows from the containment [7, I.2.4]

$$\text{Int}(E, D) \subseteq \text{Int}(E, D_{\mathfrak{p}})$$

that if  $\{a_n\}$  is an ordering for  $E$  in  $D$  (of length  $N$  or infinite) then it is an ordering for  $E$  in  $D_{\mathfrak{p}}$  for each prime ideal  $\mathfrak{p}$  of  $D$ . Conversely if  $\mathcal{P}$  is a set of prime ideals of  $D$  such that  $D = \bigcap_{\mathfrak{p} \in \mathcal{P}} D_{\mathfrak{p}}$ , and if  $\{a_n\}$  is an ordering for  $E$  in  $D_{\mathfrak{p}}$  for all  $\mathfrak{p} \in \mathcal{P}$  then it is an ordering for  $E$  in  $D$ .

In particular, suppose that  $D$  is a Dedekind domain with finite residue fields. Then  $\{a_n\}$  is an ordering for  $E$  if and only if, for every maximal ideal  $\mathfrak{p}$  of  $D$ , it is a  $\mathfrak{p}$ -ordering of  $E$  (Def. 1.1). Following Bhargava, this is known

as a *simultaneous ordering* (note that, for a discrete valuation domain with maximal ideal  $\mathfrak{p}$  and finite residue field, a Newtonian ordering is nothing else than a  $\mathfrak{p}$ -ordering).

3) Non-uniqueness: when they exist, orderings are not necessarily unique. For instance, if  $\{a_n\}_{0 \leq n \leq N}$  is an ordering for  $D$  itself in the ring  $D$ , then, for every  $b \in D$  and every unit  $u$  of  $D$ ,  $\{ua_n + b\}$  is also an ordering for  $D$ , moreover there may also be orderings of a different type. For instance, the sequence  $\{(-1)^n \lfloor \frac{n+1}{2} \rfloor\}_{n \in \mathbb{N}}$  is an ordering for  $\mathbb{Z}$  [7, Exercise I.5] which is not linked by a linear transformation to the sequence  $0, 1, \dots, n, \dots$  of natural numbers.

4) Polynomial closure: if  $\{a_n\}$  is an ordering for  $E$  in  $D$  it is also an ordering for the *polynomial closure*  $\overline{E}$  of  $E$  in  $D$ , that is,

$$\overline{E} = \{b \in D \mid \forall f \in \text{Int}(E, D), f(b) \in D\}.$$

### 3.2 Newtonian domains

**Definition 3.3.** A domain  $D$  is said to be a Newtonian domain if there exists an infinite Newtonian ordering for  $D$  in  $D$ .

Here are some examples:

- 1)  $\mathbb{Z}$  is a Newtonian domain.
- 2) Every local domain  $D$  with infinite residue field is a Newtonian domain. Any sequence of elements in distinct residue classes is an ordering for  $D$  since  $\text{Int}(D) = D[X]$ .
- 3) Every discrete valuation domain  $V$  is a Newtonian domain. If the residue field is infinite this follows from the previous example and if the residue field is finite, a Newtonian ordering is given by a  $\mathfrak{p}$ -ordering (where  $\mathfrak{p}$  is the maximal ideal of  $V$ ). A particular case is that of a *very well distributed and well ordered sequence* [7, Definition II.2.1]. To build such a sequence [7, Proposition II.2.3], let  $t$  be a generator of the maximal ideal  $\mathfrak{p}$  and  $a_0 = 0, a_1, \dots, a_{q-1}$  be a system of representatives of  $V$  modulo  $\mathfrak{p}$  then, for each  $n \in \mathbb{N}$  with  $q$ -adic expansion (2), put

$$a_n = a_{n_0} + a_{n_1}t + \dots + a_{n_k}t^k. \quad (16)$$

From the previous examples and the Chinese remainder theorem we deduce the following.

**Proposition 3.4.** A semi-local principal ideal domain is a Newtonian domain.

Let us consider now non semi-local domains. The first question is the following.

**Question F.** Does there exist a number field  $K \neq \mathbb{Q}$  such that the ring of integers  $\mathcal{O}_K$  of  $K$  is a Newtonian domain? [5, Quest. 30]

Known results are essentially negative (Wood [38]).

**Proposition 3.5.** *The ring of integers  $\mathcal{O}_K$  of an imaginary quadratic field  $K$  is not Newtonian.*

The reason why it is easier to obtain a negative answer for imaginary quadratic fields is probably due to the fact that there are only finitely many units. Here is a positive result [14].

**Proposition 3.6.** *Let  $K$  be a number field and let  $D$  be a localization of the ring  $\mathcal{O}_K$  of integers of  $K$ . Then, the sequence  $\{n\}_{n \in \mathbb{N}}$  is a Newtonian ordering for  $D$  (and thus  $D$  is a Newtonian domain) if and only if every prime number splits completely in  $D$ .*

For instance, if  $S$  denotes the multiplicative subset generated by the prime numbers  $p$  such that  $p \equiv 1 \pmod{4}$ , then  $S^{-1}\mathbb{Z}[i]$  is a Newtonian domain. More generally, we have the following.

**Proposition 3.7.** *Let  $D$  be a Dedekind domain which is Newtonian, let  $\{a_n\}_{n \in \mathbb{N}}$  be an ordering for  $D$  and let  $R$  be an integral domain containing  $D$ . The following assertions are equivalent:*

- (i)  $\{a_n\}_{n \in \mathbb{N}}$  is an ordering for  $R$ ,
- (ii) For each  $\mathfrak{p} \in \max(D)$  with finite residue field and for each  $\mathfrak{m} \in \max(R)$  containing  $\mathfrak{p}$ , one has  $R/\mathfrak{m} \simeq D/\mathfrak{p}$  and  $\mathfrak{m}R_{\mathfrak{m}} = \mathfrak{p}R_{\mathfrak{m}}$ .

When  $R$  is Noetherian, this is also equivalent to:

- (iii) each  $\mathfrak{p} \in \max(D)$  with finite residue field such that  $\mathfrak{p}R \neq R$  splits completely in  $R$  (that is,  $\mathfrak{p}R = \prod_{i=1}^r \mathfrak{m}_i$  where the  $\mathfrak{m}_i$ 's are distinct maximal ideals of  $R$  with norm equals to the norm of  $\mathfrak{p}$ ).

The proof follows from the results given in [7, §IV.3]. See also [38, Prop. 5.1] when  $R$  is a Dedekind domain.

One may also consider the question of Newtonian domains in the context of function fields with analogous results. First of all, for each finite field  $\mathbb{F}_q$ , the polynomial ring  $\mathbb{F}_q[T]$  is a Newtonian domain. Indeed, the sequence  $\{a_n\}_{n \in \mathbb{N}}$  obtained by Formula (16) for the valuation domain  $\mathbb{F}_q[T]_{(T)}$ , that is,

$$a_n = a_{n_0} + a_{n_1}T + \dots + a_{n_k}T^k \quad (17)$$

is in fact a Newtonian ordering for the domain  $\mathbb{F}_q[T]$  itself (see [5] or [1]). Similarly to Question F, one may then ask the following.

**Question F1.** Are there algebraic extensions  $K \neq \mathbb{F}_q(T)$  of  $\mathbb{F}_q(T)$  such that the integral closure  $\mathcal{O}_K$  of  $\mathbb{F}_q[T]$  in  $K$  is a Newtonian domain?

There is a result very similar to Wood's result. Recall that the extension  $K$  of  $\mathbb{F}_q(T)$  is called an *imaginary extension* if the infinite place of  $\mathbb{F}_q(T)$ , that is the valuation associated to  $\frac{1}{T}$ , has only one extension to  $K$ . In this case the units of  $K$  are the elements of  $\mathbb{F}_q^*$ . Assume that  $q$  is odd, then a quadratic extension  $K = \mathbb{F}_q(T)[Y]/(Y^2 - D(T))$  of  $\mathbb{F}_q(T)$  is imaginary if and only if either  $\deg(D)$  is odd or the leading coefficient of  $D$  is not a square in  $\mathbb{F}_q$ .

**Proposition 3.8.** (Adam [1]) *Assume that  $q$  is odd and consider an imaginary quadratic extension  $K = \mathbb{F}_q(T)[Y]/(Y^2 - D(T))$  of  $\mathbb{F}_q(T)$ . Then the integral closure  $\mathcal{O}_K$  of  $\mathbb{F}_q[T]$  in  $K$  is not a Newtonian domain unless  $\deg(D) = 1$ .*

In fact, if  $\deg(D) = 1$ , the quadratic extension  $K$  is isomorphic to  $\mathbb{F}_q(T)$ .

More generally, we ask the following.

**Question F2.** Characterize the Dedekind domains that are Newtonian.

For a discrete valuation domain with maximal ideal  $\mathfrak{p}$  and finite residue field, Newtonian orderings and  $\mathfrak{p}$ -orderings are the same; they were characterized by Julie Yeramian [39] and correspond to the *very well ordered sequences* defined by Y. Amice [3]. By globalization, we obtain the following partial answer:

**Proposition 3.9.** *Let  $D$  be a Dedekind domain with finite residue fields. A sequence  $\{a_n\}_{n \in \mathbb{N}}$  in  $D$  is a Newtonian ordering for  $D$  if and only if, for each maximal ideal  $\mathfrak{p}$  of  $D$  with norm  $q$ , for each  $s \in \mathbb{N}$ , and for each  $k \in \mathbb{N}^*$ , the  $q^k$  following consecutive elements form a complete system of representatives of  $D$  modulo  $\mathfrak{p}^k$ :*

$$a_{sq^k}, a_{sq^k+1}, \dots, a_{(s+1)q^k-1}. \quad (18)$$

### 3.3 Schinzel orderings

The last proposition is obviously related to an old problem suggested by J. Browkin in 1965 for  $\mathbb{Q}[i]$ , which is known as Schinzel's problem [31, Problem 8].

**Schinzel's problem** (1969). Does there exist a number field  $K \neq \mathbb{Q}$  with a sequence  $\{a_n\}_{n \in \mathbb{N}}$  of elements in the ring of integers  $\mathcal{O}_K$  of  $K$  such that, for each ideal  $I$  of  $\mathcal{O}_K$  with norm  $N = N(I) = \text{Card}(\mathcal{O}_K/I)$ , the sequence  $a_0, a_1, \dots, a_{N-1}$  is a complete system of representatives of  $\mathcal{O}_K$  modulo  $I$ ?

Some results are known:  $K$  cannot be a quadratic field (Wantula, 1969),  $\mathcal{O}_K$  must be a principal ideal domain (Wasen, 1976).

More generally, we may consider a domain  $D$ . As for Newtonian orderings, good infinite sequences may not exist and hence, we may wish to restrict ourselves to finite sequences. We thus set the following.

**Definition 3.10.** *Let  $D$  be a domain.*

- (1) *A sequence  $\{a_n\}_{n \in \mathbb{N}}$  in  $D$  is called an infinite Schinzel ordering for  $D$  if, for each integer  $k$  and each ideal  $I$  of  $D$  with norm  $N(I) \geq k$ , the elements  $a_0, a_1, \dots, a_{k-1}$  are in distinct classes modulo  $I$ .*
- (2) *Given a positive integer  $N$ , a sequence  $\{a_n\}_{0 \leq n < N}$  in  $D$  is called a Schinzel ordering of length  $N$  for  $D$  if, for each  $k \leq N$  and each ideal  $I$  of  $D$  with norm  $N(I) \geq k$ , the elements  $a_0, a_1, \dots, a_{k-1}$  are in distinct classes modulo  $I$ .*
- (3) *The domain  $D$  is said to be a Schinzel domain if there exists an infinite Schinzel ordering for  $D$ .*

Here are some examples:

- (1)  $\mathbb{Z}$  is a Schinzel domain with Schinzel ordering  $\{n\}_{n \in \mathbb{N}}$ .
- (2) A discrete valuation domain with finite residue field is a Schinzel domain. The sequence constructed by means of Formula (16) is a Schinzel ordering.
- (3)  $\mathbb{F}_q[T]$  is a Schinzel domain: the Newtonian ordering for  $\mathbb{F}_q[T]$  defined by (17) is a Schinzel ordering because, for  $g \in \mathbb{F}_q[T]$  of degree  $d$ , the  $q^d$  first elements of this sequence are in distinct classes modulo  $g$ .
- (4) A local domain with an infinite residue field is (trivially) a Schinzel domain (the norm of every proper ideal is infinite and a sequence of elements in distinct classes modulo the maximal ideal is a Schinzel ordering).

The following necessary condition was communicated to us by Sophie Frisch.

**Proposition 3.11.** *Let  $D$  be a domain with finite residue rings. If  $D$  is a Schinzel domain, then  $D$  is Euclidean for the norm.*

*Proof.* For  $x \in D$ , write  $N(x)$  for the norm of the principal ideal  $xD$ . Assume there exists an infinite Schinzel ordering  $\{a_n\}_{n \in \mathbb{N}}$ . One may always assume that  $a_0 = 0$ . Then, for each  $k$ ,  $a_k$  and  $a_0$  are in the same class modulo  $a_k D$ . It follows from the definition of a Schinzel ordering that  $N(a_k) \leq k$ . Let  $x, y \in D$ , with  $x \neq 0, x$  not a unit. Set  $n = N(x)$ . As  $a_0, a_1, \dots, a_{n-1}$  form a complete system of residues modulo  $xD$ , one may write  $y = qx + r$ , with  $q \in D$  and  $r = a_k$ , for some  $k \leq n - 1$ . Clearly, one then has  $N(a_k) < N(x)$ .  $\square$

In general, the ring of integers of a number field is not a Schinzel domain. Maximal lengths of Schinzel orderings are given in [28] and [37].

It may be interesting to compare Schinzel and Newtonian orderings. In particular, we pose the following.

**Question G.** Are the classes of Newtonian and Schinzel domains distinct?

In fact, for a Dedekind domain with finite residue fields, one can list six natural properties for a sequence  $\{a_n\}_{n \in \mathbb{N}}$  in  $D$  as follows:  $\nu$  denotes the norm of any nonzero ideal  $\mathcal{I}$  of  $D$ ,  $q$  denotes the norm of any maximal ideal  $\mathfrak{p}$  of  $D$  and, ‘c.s.r.’ means ‘is a complete system of representatives of ...’

property	for all	the sequence	c.s.r.
I	$\nu = N(\mathcal{I}), r \in \mathbb{N}$	$a_r, \dots, a_{r+\nu-1}$	$D/\mathcal{I}$
I'	$q = N(\mathfrak{p}), s \in \mathbb{N}^*, r \in \mathbb{N}$	$a_r, \dots, a_{r+q^s-1}$	$D/\mathfrak{p}^s$
II	$\nu = N(\mathcal{I}), k \in \mathbb{N}$	$a_{k\nu}, \dots, a_{(k+1)\nu-1}$	$D/\mathcal{I}$
II' Newton	$q = N(\mathfrak{p}), s \in \mathbb{N}^*, k \in \mathbb{N}$	$a_{kq^s}, \dots, a_{(k+1)q^s-1}$	$D/\mathfrak{p}^s$
III Schinzel	$\nu = N(\mathcal{I})$	$a_0, \dots, a_{\nu-1}$	$D/\mathcal{I}$
III'	$q = N(\mathfrak{p}), s \in \mathbb{N}^*$	$a_0, \dots, a_{q^s-1}$	$D/\mathfrak{p}^s$

One can say that a Dedekind domain  $D$  satisfies one of these properties if there exists a sequence in  $D$  which satisfies the given property. We have the following obvious implications:

$$\begin{array}{ccccc}
 I & \longrightarrow & II & \longrightarrow & III \\
 \downarrow & & \downarrow & & \downarrow \\
 I' & \longrightarrow & II' & \longrightarrow & III'
 \end{array}$$

**Problem G1.** Discuss each reverse implication.

We list below some examples for the strongest properties (I, I' and II):

*Property I:* a) Obviously, the sequence of natural numbers satisfies I in  $\mathbb{Z}$ .

b) A discrete valuation domain with a finite residue field. A sequence  $\{a_n\}_{n \in \mathbb{N}}$  satisfies I if and only if it is a *very well distributed and well ordered* sequence [7, §II.2], that is if, for each  $n$  and  $m$ ,

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

where  $v$  denotes the valuation,  $q$  denotes the cardinality of the residue field and  $v_q(n - m)$  denotes the greatest  $k$  such that  $q^k$  divides  $n - m$ . The sequence given by Formula 16 satisfies this property.

*Property I':* a) A Dedekind domain  $D$  with characteristic 0 such that every prime number splits completely in  $D$ . Merely consider the sequence  $\{n\}_{n \in \mathbb{N}}$ .

b) A semi-local principal ideal domain  $D$  (because property I may be globalized for finitely many maximal ideals, cf. [39]).

*Property II:* The sequence given by (17) yields that  $\mathbb{F}_q[T]$  has this property.

Here is a partial answer to question G1. The domain  $\mathbb{F}_q[T]$  satisfies II, but not I' [2, Prop. 2.8]). Consequently,  $II \not\rightarrow I'$ . We may also notice that the negative results concerning the Newtonian property are generally obtained by using only the first terms of the sequences (that is, property III').

## 4 The Pólya-Ostrowski group and Pólya fields

A necessary (but not sufficient) condition for  $D$  to be a Newtonian domain is that all factorial ideals are principal. We discuss here this property.

### 4.1 The Pólya-Ostrowski group

**Definition 4.1.** Let  $D$  be a Dedekind domain.

(1) The factorial group of  $D$  is the subgroup  $\mathcal{F}act(D)$  of the group  $\mathcal{J}(D)$  of nonzero fractional ideals of  $D$  generated by the factorial ideals.

(2) The Pólya-Ostrowski group of  $D$  is the image  $\mathcal{P}o(D)$  of  $\mathcal{F}act(D)$  in the class group  $Cl(D) = \mathcal{J}(D)/\mathcal{P}(D)$  of  $D$ .

It is easy to check the following (see for instance, [10, Prop. 2.2]).

**Proposition 4.2.** Let  $D$  be a Dedekind domain. Then  $\mathcal{F}act(D)$  is a free Abelian group with a basis formed by the non trivial ideals

$$\Pi_q = \prod_{\mathfrak{p} \in \text{Max}(D), N(\mathfrak{p})=q} \mathfrak{p}.$$

Assume throughout that  $K$  is a number field and that  $\mathcal{O}_K$  denotes its ring of integers. A natural question is the following.

**Problem H.** Describe the Pólya-Ostrowski group  $\mathcal{P}o(\mathcal{O}_K)$  of the ring of integer  $\mathcal{O}_K$  of a number field  $K$ .

We have some partial answers for Galois extensions  $K/\mathbb{Q}$ , since in this case the ideals  $\Pi_q$  are the *ambige Ideale* of Hilbert.

- 1) The Pólya-Ostrowski  $\mathcal{P}o(\mathcal{O}_K)$  is generated solely by the  $\Pi_q$ 's where  $q$  is some power of a ramified prime number [35].
- 2) A description of the Pólya-Ostrowski group of a quadratic number field can be found in [26, Prop. 105 and 106] or [7, II.4.4].
- 3) The following sequence of Abelian groups is exact:

$$1 \rightarrow H^1(G, U(\mathcal{O}_K)) \rightarrow \bigoplus_{p \in \mathbb{P}} \mathbb{Z}/e_p \mathbb{Z} \rightarrow \mathcal{P}o(\mathcal{O}_K) \rightarrow 1$$

where  $e_p$  denotes the ramification index of  $p$  in the extension  $K/\mathbb{Q}$  (see [10] or [40]).

- 4) If  $K$  is the compositum of two Galois subextensions  $K_1$  and  $K_2$  of  $\mathbb{Q}$  such that  $[K_1:\mathbb{Q}]$  and  $[K_2:\mathbb{Q}]$  are relatively prime, then by [10, Prop. 3.6],

$$\mathcal{P}o(\mathcal{O}_K) \simeq \mathcal{P}o(\mathcal{O}_{K_1}) \times \mathcal{P}o(\mathcal{O}_{K_2}).$$

## 4.2 Pólya fields

**Proposition 4.3.** *Let  $D$  be a Dedekind domain. The following assertions are equivalent:*

- (i)  $\text{Int}(D)$  admits a regular basis, that is, a basis  $\{f_n\}_{n \in \mathbb{N}}$  where  $\deg(f_n) = n$ .
- (ii) The ideals  $n!_D$  are principal.
- (iii) The ideals  $\Pi_q = \prod_{N(\mathfrak{p})=q} \mathfrak{p}$  are principal.
- (iv) The Pólya-Ostrowski group of  $D$  is trivial, that is,  $\mathcal{P}o(D) \simeq \{1\}$ .

Returning to number fields, we use a definition of Zantema [40].

**Definition 4.4.** *A Pólya field is a number field  $K$  such that  $\mathcal{P}o(\mathcal{O}_K) = \{1\}$ , that is, such that  $\text{Int}(\mathcal{O}_K)$  admits a regular basis.*

Here again, we offer some answers.

- 1) Every cyclotomic field is a Pólya field.
- 2) For the characterization of the quadratic Pólya fields see [40] or [7, II.4.5].
- 3) It follows from the previous section that, if  $K_1$  and  $K_2$  are two Pólya fields such that  $[K_1:\mathbb{Q}]$  and  $[K_2:\mathbb{Q}]$  are relatively prime, then  $K_1 K_2$  is a Pólya field.

The notion of Pólya field may also be extended to function fields with some partial results. The first ones were given by Van der Linden [36]. More general results were obtained by Adam [2, Chapter 5]:

- 1) He proved that the analog of cyclotomic fields in the context of function fields are Pólya fields.

2) He characterized the analog of imaginary quadratic Kummer extensions that are Pólya fields.

Finally, let us recall the problem of *class field towers* which goes back to Kronecker and Weber. The ring of integers  $\mathcal{O}_K$  of a number field  $K$  is not necessarily a principal ideal domain. However, if  $h_K$  denotes the class number of  $K$ , that is, the order of the class group  $Cl(\mathcal{O}_K)$ , there exists a Galois extension  $H(K)$  of  $K$  of degree  $h_K$ , the *Hilbert class field* of  $K$ , such that, for every ideal  $\mathcal{I}$  of  $\mathcal{O}_K$ , its extension  $\mathcal{I}\mathcal{O}_{H(K)}$  is a principal ideal of  $\mathcal{O}_{H(K)}$  (and moreover, the Galois group  $Gal(H(K)/K)$  is isomorphic to  $Cl(\mathcal{O}_K)$ ). Again,  $\mathcal{O}_{H(K)}$  is not necessarily a principal ideal domain, so that, one may iterate the process and consider  $H(H(K))$ ,... , and so on. The question was as follows: does this construction of the Hilbert class field tower of  $K$  stops after a finite number of steps? The answer is no and was given by Golod and Shafarevich in 1964.

Analogously, we introduce the following definition:

**Definition 4.5.** *An extension of number fields  $L/K$  is called a Pólya extension if all the extended ideals  $\Pi_q(\mathcal{O}_K)\mathcal{O}_L$  are principal.*

In other words, the extension  $L/K$  is a Pólya extension if and only if the  $\mathcal{O}_L$ -module  $\text{Int}(\mathcal{O}_K, \mathcal{O}_L)$  has a regular basis. Of course, if  $K$  is a Pólya field, then every finite extension of  $K$  is a Pólya extension and, whatever the fixed number field  $K$ , there exist a Pólya extension  $L$  of  $K$  contained in the Hilbert class field  $H(K)$  of  $K$  (since  $\mathcal{P}o(\mathcal{O}_K) \subseteq Cl(\mathcal{O}_K)$ ). If this extension  $L$  is not a Pólya field, we may iterate the process. This suggests two questions:

**Question I1.** For every number field  $K$ , is there a smallest Pólya extension of  $K$  contained in the Hilbert class field  $H(K)$  of  $K$ ?

**Question I2.** For every number field  $K$ , is there a Pólya field containing  $K$ ? That is, is there a finite Pólya extension tower of  $K$ ?

## 5 Around Prüfer domains

We end our paper with a short section which, following R. Gilmer [22], is most strongly linked to multiplicative ideal theory. In the classical case of the ring of integer-valued polynomials in a global field  $K$  (i.e., a number field or a function field), the ring  $\text{Int}(\mathcal{O}_K)$  is a 2-dimensional Prüfer domain. In the case of a local field (i.e., a field which is complete for a discrete valuation with a finite residue field), if  $V$  denotes the ring of the valuation,  $\text{Int}(V)$  provides a very natural example of a 2-dimensional Prüfer domain that is completely integrally closed but not the intersection of rank-one valuation domains. This last example answers several questions which go back to Krull.

It was then natural to ask the following: for which domain  $D$  is  $\text{Int}(D)$  a Prüfer domain?

When  $D$  is Noetherian, it is necessary and sufficient that  $D$  is a Dedekind domain with finite residue fields. In general, the answer is more difficult and Gilmer's paper [21] is a seminal step for this characterization (see questions Q1 and Q2 in Section 1 of [15]). We state it in characteristic 0.

$\text{Int}(D)$  is a Prüfer domain if and only if  $D$  is an almost Dedekind domain (each localization of  $D$  with respect to a maximal ideal  $\mathfrak{p}$  is a discrete valuation domain) with finite residue fields and, for each prime number  $p$ , the following subsets are bounded:  $\{|D/\mathfrak{p}| \mid p \in \mathfrak{p}\}$  and  $\{v_{\mathfrak{p}}(p) \mid p \in \mathfrak{p}\}$  where  $v_{\mathfrak{p}}$  denotes the normalized valuation associated to  $\mathfrak{p}$  (see [9], [21] and [29]).

Recent papers deal more and more with subsets.

**Problem J.** Characterize the pairs  $(S, D)$ , where  $D$  is a domain and  $S$  is a subset of  $D$ , such that  $\text{Int}(S, D)$  is a Prüfer domain.

There are several partial answers (for instance [7, V.Exercises] or [13]), but no characterization. It is however interesting to note that subsets allow one to provide examples of Prüfer domains with arbitrarily large Krull dimensions.

Finally, recall a question from Brewer and Klinger [6] which is of great interest. It concerns the question whether, as with Dedekind domains, Prüfer domains  $D$  have the *simultaneous bases property*. This property is defined as follows: for each  $n \in \mathbb{N}^*$  and each sub- $D$ -module  $M$  of  $D^n$ , one has

- 1)  $M$  is a projective  $D$ -module of rank  $k \leq n$ ,
- 2) there exist  $n$  rank-one projective sub- $D$ -modules  $P_1, \dots, P_n$  of  $D^n$  and a decreasing sequence  $I_1 \supseteq \dots \supseteq I_k$  of ideals of  $D$  such that

$$D^n = P_1 \oplus \dots \oplus P_n, \quad M = I_1 P_1 \oplus \dots \oplus I_k P_k.$$

For a Prüfer domain, this property is equivalent to the *bcs-property* that may be formulated in the following way: for each matrix  $B \in \mathcal{M}_{n \times m}(D)$  of unit content, there exists a matrix  $C \in \mathcal{M}_{m \times l}(D)$  such that  $BC$  has unit content and rank one (recall that the content of a matrix is the ideal generated by its coefficients). The final question is as follows.

**Question K** (Brewer and Klinger). Does the very classical Prüfer domain  $\text{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$  satisfy the bcs-property?

## References

1. D. Adam, Simultaneous orderings in function fields, *J. Number Theory* **112** (2005), 287–297.
2. D. Adam, Fonctions et Polynômes à Valeurs entières en caractéristique finie, Thesis, June 2004, Amiens, France.
3. Y. Amice, Interpolation  $p$ -adique, *Bull. Soc. Math. France* **92** (1964), 117–180.
4. M. Bhargava,  $P$ -orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. reine angew. Math.* **490** (1997), 101–127.

5. M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly*, **107** (2000), 783–799.
6. J. Brewer and L. Klinger, Rings of Integer-Valued Polynomials and the bcs-Property, in *Commutative ring theory and applications*, 65–75, Lecture Notes in Pure and Appl. Math. **231**, Dekker, New York, 2003.
7. P.-J. Cahen & J.-L. Chabert, *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys and Monographs, **48**, Providence, 1997.
8. L. Carlitz, On certain functions connected with polynomials in a Galois field, *Duke Math. J.* **1** (1935), 137–168.
9. J.-L. Chabert, Integer-Valued Polynomials, Prüfer domains and Localization, *Proc. Amer. Math. Soc.* **118** (1993), 1061–1073.
10. J.-L. Chabert, Factorial Groups and Pólya Groups in Galoisian Extension of  $\mathbb{Q}$ , in *Commutative ring theory and applications, Lecture Notes in Pure and Appl. Math.* **231**, Dekker, New York, 2003.
11. J.-L. Chabert, Integer-valued polynomials on prime numbers and logarithm powers expansion, *European J. of Combinatorics*, to appear.
12. 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*, 271–284, Lecture Notes in Pure and Appl. Math. **189**, Dekker, New York, 1997.
13. P.-J. Cahen, J.-L. Chabert and K.A. Loper, High dimension Prüfer domains of integer-valued polynomials, *J. Korean Math. Soc.* **38** (2001), 915–935.
14. J.-L. Chabert and G. Gerboud, Polynômes à valeurs entières et binômes de Fermat, *Canad. J. Math.* **45** (1993), 6–21.
15. S. Chapman, V. Ponomarenko and W. W. Smith, Robert Gilmer’s contributions to the theory of integer-valued polynomials, this volume.
16. A. Crabbe, Generalized factorial functions and binomial coefficients, Honors Thesis, Trinity University, San Antonio, Texas, 2001.
17. Y. Fares, Factorial preservation, *Arch. Math* **83** (2004), 497–506.
18. Y. Fares,  $\delta$ -rings and factorial sequences preservation, *Acta Arithmetica*, to appear.
19. G. Gerboud, Polynômes à valeurs entières sur l’anneau des quaternions de Hurwitz, preprint, Amiens, 1998.
20. R. Gilmer, Sets that determine Integer-valued Polynomials, *J. of Number Theory* **33** (1989), 95–100.
21. R. Gilmer, Prüfer domains and Rings of Integer-Valued Domains, *J. of Algebra* **129** (1990), 502–517.
22. R. Gilmer, Forty years of commutative ring theory, in *Rings, modules, algebras, and abelian groups*, 229–256, Lecture Notes in Pure and Appl. Math. **236**, Dekker, New York, 2004.
23. R. Gilmer and W. Smith, On the polynomial equivalence of subsets  $E$  and  $f(E)$  of  $\mathbb{Z}$ , *Arch. Math.* **73** (1999), 355–365.
24. D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, 1998, New York.
25. H. Gunji and D.L. McQuillan, On a Class of Ideals in an Algebraic Number Field, *J. Number Theory* **2** (1970), 207–222.
26. D. Hilbert, Die Theorie der algebraischen Zahlkörper, 1897.
27. F.H. Jackson, On  $q$ -definite integrals, *Quart. J. Pure and Appl. Math.* **41** (1910), 193–203.
28. J. Latham, On sequences of algebraic integers, *Journ. London Math. Soc.* **6** (1973), 555–560.

29. K.A. Loper, A classification of all  $D$  such that  $\text{Int}(D)$  is a Prüfer domain, *Proc. Amer. math. Soc.* **126** (1998), 657–660.
30. S.B. Mulay, Integer-Valued Polynomials in Several Variables, *Comm. Algebra* **27** (1999), 2409–2423.
31. W. Narkiewicz, Some unsolved problems, *Bull. Soc. Math France, Mémoire* **25** (1971), 159–164.
32. I. Newton, *Mathematical Principles of Natural Philosophy*, 1687.
33. G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 97–116.
34. N.J.A. Sloane, *The On-Line Encyclopedia in Integer Sequences*, <http://www.research.att.com/~njas/sequences/index.html>
35. A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 117–124.
36. F.J. Van Der Linden, Integer valued polynomials over function fields, *Nederl. Akad. Wetensch. Indag. Math.* **50** (1988), 293–308.
37. R. Wasén, Remark on a problem of Schinzel, *Acta Arith.* **29** (1976), 425–426.
38. M. Wood,  $P$ -orderings: a metric viewpoint and the non-existence of simultaneous orderings, *J. Number Theory*, **99** (2003), 36–56.
39. J. Yeramian, Anneaux de Bhargava, *Comm. Algebra* **32** (2004), 3043–3069.
40. H. Zantema, Integer valued polynomials over a number field, *Manuscr. Math.* **40** (1982), 155–203.