The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: https://www.tandfonline.com/loi/uamm20

What You Should Know About Integer-Valued Polynomials

Paul-Jean Cahen & Jean-Luc Chabert

To cite this article: Paul-Jean Cahen & Jean-Luc Chabert (2016) What You Should Know About Integer-Valued Polynomials, The American Mathematical Monthly, 123:4, 311-337

To link to this article: https://doi.org/10.4169/amer.math.monthly.123.4.311

What You Should Know About Integer-Valued Polynomials

Paul-Jean Cahen and Jean-Luc Chabert

Abstract. The authors wish to celebrate the centenary of Pólya's paper *Ueber ganzwertige ganze funktionen* where first explicitly appeared the term "integer-valued polynomials." This survey is focused on the emblematic example of the ring $\mathrm{Int}(\mathbb{Z})$ formed by the polynomials with rational coefficients taking integer values on the integers. This ring has surprising algebraic properties, often obtained by means of analytical properties. Yet, the article mentions also several extensions, either by considering integer-valued polynomials on a subset of $\mathbb{Z}$, or by replacing $\mathbb{Z}$ by the ring of integers of a number field.

1. INTRODUCTION. In 2000, to *Polynomial rings and ideals* in item 13F20 of the AMS Mathematics Subject Classification were added the words *rings of integer-valued polynomials*. But what are these rings?

By *integer-valued polynomial* we mean a polynomial taking integral values on the rational integers (although we shall later give various generalizations). Such a polynomial has not necessarily integral coefficients as shown by $\frac{1}{2}X(X-1)$. More generally, for every prime number p, $\frac{1}{p}(X^p - X)$ is integer-valued, thanks to Fermat's little theorem, and so is, for every integer $n \geq 2$, the binomial polynomial

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

The set of integer-valued polynomials is denoted by $\mathrm{Int}(\mathbb{Z})$; that is

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

The sum, the difference, and the product of two integer-valued polynomials are clearly again integer-valued. Here is thus our first *ring of integer-valued polynomials*!

However, the interest for the ring structure of $\mathrm{Int}(\mathbb{Z})$ arose only in the last quarter of the previous century. Yet it was at least well known at the time of Pólya that every integer-valued polynomial f of degree n may be uniquely written as a linear combination:

$$f(X) = \sum_{k=0}^{n} c_k \binom{X}{k}, \tag{1}$$

with the convention $\binom{X}{0} = 1$ and $\binom{X}{1} = X$, and the coefficients c_k recursively given by the formula

$$c_k = f(k) - \sum_{i=0}^{k-1} c_i \binom{k}{i}. \tag{2}$$

http://dx.doi.org/10.4169/amer.math.monthly.123.4.311
MSC: Primary 13F20

In fact, (1) evokes the Gregory–Newton formula dating back to the seventeenth century:

$$f = \sum_{k=0}^{n} \Delta^k f(0) \binom{X}{k}. \tag{3}$$

Here Δf is the finite difference $\Delta f = f(X+1) - f(X)$ and $\Delta^k f$ is recursively defined by $\Delta^k f = \Delta(\Delta^{k-1} f)$. Formula (3) is easily obtained, using Pascal's triangle property: $\Delta\binom{X}{n} = \binom{X}{n-1}$.

As early as 1919, two papers by Georg Pólya [**49**] and Alexander Ostrowski [**47**], both titled "Über ganzwertige polynome in algebraischen Zahlkörpern," considered polynomials with coefficients in a number field K taking the ring of integers $\mathcal{O}_K$ into itself. This was already leading to more rings of integer-valued polynomials! Yet they only tried to generalize (1) and the celebrated earlier paper of Pólya *Ueber ganzwertige ganze funktionen* [**48**] was in fact of an analytical nature.

More generalizations, and a genuine interest for the ring structure, came in the 1970s, considering integer-valued polynomials on a domain D, with quotient field K. These polynomials form a ring denoted by $\mathrm{Int}(D)$:

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

As in more recent developments, one can even consider integer-valued polynomials on a subset E of D:

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

In this paper we nevertheless largely focus on $\mathbb{Z}$, at least in the first sections. The classical ring $\mathrm{Int}(\mathbb{Z})$ has, indeed, many interesting properties and we start with them in section 2. In a way, it behaves much better than the ring $\mathbb{Z}[X]$ of polynomials with integer coefficients. For instance, it has nice interpolation properties, as the Gregory–Newton formula may suggest. But let us immediately emphasize a negative property: it is probably the most natural and simplest algebraic example of a non-Noetherian ring (that is, having ideals which are not finitely generated).

Polynomials are known to be continuous functions. As integer-valued polynomials have their coefficients in $\mathbb{Q}$, it is natural to consider them as continuous in the p-adic topology. We recall the definition of this topology and develop this aspect in section 3. One main feature is a p-adic analogue of the theorem of Stone–Weierstrass. These analytical tools allow us to prove many algebraic results, and this is precisely what we do in section 4. For instance, we can describe the prime spectrum of $\mathrm{Int}(\mathbb{Z})$ and then show that $\mathrm{Int}(\mathbb{Z})$ is a Prüfer domain (Prüfer domains generalize Dedekind domains in the non-Noetherian case; their definition will be recalled later).

In section 5 we turn to integer-valued polynomials on a subset. Aside from some generalities, we mostly consider subsets of $\mathbb{Z}$. An interesting problem is to determine for which subsets one can generalize formula (1) with a sequence $\{a_n\}_{n\geq 0}$ replacing the nonnegative integers. Significant progress was obtained thanks to the notion of p-ordering introduced by Bhargava around 2000. This leads to Bhargava's generalized factorials. We also state some open problems.

Only in section 6 do we generalize to integer-valued polynomials on a domain. Yet we focus on the ring of integers of a number field. Most algebraic properties of $\mathrm{Int}(\mathbb{Z})$ extend to this case. Yet, as seen by Pólya and Ostrowski in 1919, there is in general

no *regular basis*, as in formula (1) (that is, with one polynomial of each degree). We end this section with the ring $\mathbb{F}_q[T]$ of polynomials with coefficients in a finite field, which in every respect compares better with $\mathbb{Z}$.

In a very short final section, we quickly evoke a few more aspects of this vast theory, such as polynomials that are integer-valued together with their derivatives, finite differences, or divided differences. Our list is far from exhaustive.

Some proofs are detailed, mostly for the results dealing with $\mathrm{Int}(\mathbb{Z})$, some are just sketched and then are so indicated. Some results are given without proof and we send the interested reader to [**16**] and [**46**].

2. ALGEBRAIC PROPERTIES.

Interpolation. By Lagrange interpolation, one may find a polynomial with coefficients in a field K assigning arbitrary values to a given finite set of arguments in K. Note that the same is not true for polynomials with integral coefficients: for $f \in \mathbb{Z}[X]$, if the integers a and b are congruent modulo some integer n, then $f(a)$ and $f(b)$ must be likewise congruent. However, interpolation is possible with integer-valued polynomials. To assign arbitrary values to a finite set of arguments contained in some interval $[a, b]$, the trick is to do better and to even assign arbitrary values to *every* integer argument ranging from a to b.

Proposition 1. *There exists one and only polynomial* $f \in \mathrm{Int}(\mathbb{Z})$ *with* $\deg(f) \leq n$, *assigning arbitrary integer values to a given set of* $n+1$ *consecutive arguments in* $\mathbb{Z}$.

Proof. First, with k ranging from 0 to n, there is a unique degree n polynomial such that $f(k) = b_k$ for each k, namely $f = \sum_{k=0}^{n} c_k \binom{X}{k}$, with the coefficients c_k given as in (2). Similarly, one can assign arbitrary values to any set of $n+1$ consecutive arguments in $\mathbb{Z}$, considering the change of variable $g(X) = f(X-h)$. ∎

For sake of reference, let us also record the following.

Corollary 2. *A degree n polynomial with rational coefficients is integer-valued if and only if it takes integral values on* $n+1$ *consecutive relative integers.*

Remark 1. If interpolation is possible, then for every pair (a, b) of elements, there is a fortiori a polynomial f with $f(a) = 0$ and $f(b) = 1$, we then say that f *separates a from b*. Conversely this is the key: a product of such separating polynomials takes the value 0 on n arguments, 1 on a last one and interpolation follows by linear combination of such products. This is how one argues in Lagrange interpolation. To separate a from b in $K[X]$ is always possible with the (unique) degree one polynomial $f = \frac{X-a}{b-a}$, this is why Lagrange interpolation on $n+1$ arguments is always possible, as every student knows, with a polynomial of degree at most n, and why it fails in $\mathbb{Z}[X]$ (where there is no way to separate 0 from 2). But now note that Proposition 1, somewhat similar to Lagrange interpolation, deals only with the specific case of $n+1$ *consecutive* arguments. Indeed, if $a, b \in \mathbb{Z}$ are such that $|b-a| > 1$, the polynomial $f = \frac{X-a}{b-a}$ is not integer-valued. To separate a from b thus requires an integer-valued polynomial of degree more that one. In fact, Proposition 1 allows us to bound this degree by $|b-a|$. In particular, $\binom{X}{n}$ separates 0 from n. Yet, there may exist a separating polynomial of degree less than n; for instance the degree 3 polynomial $f = \frac{X(X-5)(X-7)}{6}$ is integer-valued and separates 0 from 6. The discussion of the degree of interpolation polynomials can be addressed, as in [**30**].

The ring of integer-valued polynomials is not Noetherian. A ring is said to be *Noetherian* if every ideal is finitely generated. One is obviously finitely many, thus $\mathbb{Z}$ is Noetherian, being a principal ideal domain and the same is true of $K[X]$ for every field K. By Hilbert's basis theorem, if R is Noetherian, then so is $R[X]$. In particular, $\mathbb{Z}[X]$ is Noetherian, and by iteration, so are the rings $\mathbb{Z}[X_1, X_2, \ldots, X_n]$ and $K[X_1, X_2, \ldots, X_n]$ of polynomials in several indeterminates. A somewhat ad hoc counterexample is given by the ring of polynomials in infinitely many indeterminates, but probably the most natural and simplest example is our friend $\mathrm{Int}(\mathbb{Z})$. Indeed, consider the following ideal of $\mathrm{Int}(\mathbb{Z})$:

$$\mathfrak{M}_{2,0} = \{f \in \mathrm{Int}(\mathbb{Z}) \mid f(0) \text{ is even}\}.$$

Proposition 3. *The ideal $\mathfrak{M}_{2,0}$ is not finitely generated.*

Proof. By way of contradiction, suppose that $g_1, \ldots, g_s$ generate $\mathfrak{M}_{2,0}$. Finding a common denominator, write $g_1 = f_1/2^k d, \ldots, g_s = f_s/2^k d$ with d an odd integer and $f_i \in \mathbb{Z}[X]$. Each g_i is in $\mathfrak{M}_{2,0}$, that is, $g_i(0)$ is even, hence $f_i(0)$ is a multiple of 2^{k+1} and so is $f_i(2^{k+1})$ (for congruence reasons), therefore $g_i(2^{k+1})$ is even. Each $g \in \mathfrak{M}_{2,0}$ being a linear combination $g = \sum_{i=1}^{s} h_i g_i$, with $h_i \in \mathrm{Int}(\mathbb{Z})$, is then also such that $g(2^{k+1})$ is even. We obtain a contradiction: the binomial $g = \binom{X}{2^{k+1}}$ is in $\mathfrak{M}_{2,0}$, since $g(0) = 0$, but $g(2^{k+1}) = \binom{2^{k+1}}{2^{k+1}} = 1$. ∎

Although $\mathrm{Int}(\mathbb{Z})$ is not Noetherian, Gilmer and Smith proved [**33**] that every finitely generated ideal of $\mathrm{Int}(\mathbb{Z})$ may be generated by two elements. In that respect, $\mathrm{Int}(\mathbb{Z})$ compares favorably to $\mathbb{Z}[X]$ for which the number of generators required to generate an ideal can be arbitrary large. (Considering the maximal ideal $\mathfrak{m} = (p, X)$, we can see that $\mathfrak{m}^n = (p^n, p^{n-1}X, \ldots, pX^{n-1}, X^n)$ needs at least $n + 1$ generators once we interpret the quotient $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ as a vector space of dimension $n + 1$ over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p elements.)

Also, a ring is Noetherian if and only if it satisfies the *ascending chain condition* on its ideals. A weaker property is the *ascending chain condition on principal ideals*, and one may easily verify that $\mathrm{Int}(\mathbb{Z})$ satisfies this property [**16**, Proposition VI.2.9].

Skolem property. If two polynomials f and g generate $\mathbb{Z}[X]$, that is, if one can write $uf + vg = 1$ with $u, v \in \mathbb{Z}[X]$, then, for each $n \in \mathbb{Z}$, $u(n)f(n) + v(n)g(n) = 1$, hence $f(n)$ and $g(n)$ are relatively prime. But what about the converse?

In 1936, Skolem [**52**] gave a counterexample with $f = 3$ and $g = X^2 + 1$: for each $n \in \mathbb{Z}$, 3 and $n^2 + 1$ are relatively prime, but one cannot write $3u + (X^2 + 1)v = 1$, with $u, v \in \mathbb{Z}[X]$. Indeed, considering complex numbers, this would imply $3u(i) = 1$, with $u(i)$ a Gaussian integer, that is, $u(i) = a + ib$, with $a, b \in \mathbb{Z}$. But this is clearly not the case! Yet he showed that f and g generate $\mathrm{Int}(\mathbb{Z})$, writing explicitly

$$(X^2 + 1)(X^2 - 6X + 10) - 3\left(8\binom{X}{4} + 3\right) = 1.$$

In fact, he established a general property of $\mathrm{Int}(\mathbb{Z})$ that is now referred as the *Skolem property* [**16**, chapter VII].

Theorem 4 (Skolem). *If $g_1, \ldots, g_k$ are integer-valued polynomials such that, for each $n \in \mathbb{Z}$, $g_1(n), \ldots, g_k(n)$ are relatively prime, then there exist integer-valued polynomials $u_1, \ldots, u_k$ such that $u_1 g_1 + \cdots + u_k g_k = 1$.*

Let us rephrase this property. If $\mathfrak{A}$ is an ideal of $\mathrm{Int}(\mathbb{Z})$ then, for each $n \in \mathbb{Z}$,

$$\mathfrak{A}(n) = \{g(n) \mid g \in \mathfrak{A}\}$$

is clearly an ideal of $\mathbb{Z}$, quite naturally called the *ideal of values* of $\mathfrak{A}$ at n. The Skolem property states that, if $\mathfrak{A}$ is a *finitely generated* ideal of $\mathrm{Int}(\mathbb{Z})$ such that, for each n, $\mathfrak{A}(n) = \mathbb{Z}$, then $\mathfrak{A} = \mathrm{Int}(\mathbb{Z})$. But then, why stop at the special case where the ideals of values are the whole ring $\mathbb{Z}$? In fact, Brizolis [**13**] proved a stronger property, referred as the *strong Skolem property* [**16**, chapter VII].

Theorem 5 (Brizolis). *If two finitely generated ideals* $\mathfrak{A}$ *and* $\mathfrak{B}$ *of* $\mathrm{Int}(\mathbb{Z})$ *have the same ideals of values, that is, for each* $n \in \mathbb{Z}$, $\mathfrak{A}(n) = \mathfrak{B}(n)$, *then* $\mathfrak{A} = \mathfrak{B}$.

As for the (non) Noetherian property, analytical tools will shed some light on these questions [Corollaries 16 and 18].

Factorization properties. Recall that an element x of a domain D is said to be *irreducible* if it is not a unit (that is, is not invertible) and is divisible only by elements of the form u or ux where u is a unit. For instance the degree one polynomials of the form $X - a$ are clearly irreducible in $\mathrm{Int}(\mathbb{Z})$. But let us give a more interesting collection of examples.

Proposition 6. *For each* $n \geq 1$, *the binomial polynomial* $\binom{X}{n}$ *is irreducible in* $\mathrm{Int}(\mathbb{Z})$.

Proof. Suppose that $\binom{X}{n} = gh$, with $\deg(g) = r, \deg(h) = s$. It follows from the expansion of g and h as linear combination of binomials that $r!\,g$ and $s!\,h$ are in $\mathbb{Z}[X]$. Thus $r!\,s!\binom{X}{n} \in \mathbb{Z}[X]$. Looking at the leading coefficient, we have $\frac{r!\,s!}{n!} \in \mathbb{Z}$. But then $\binom{n}{r} = \frac{n!}{r!\,s!} = 1$. Hence $r = 0$ or $r = n$. Say $r = 0$, then g is a constant, thus $g \in \mathbb{Z}$ and $n!\,h \in \mathbb{Z}[X]$. The leading coefficient of $n!\binom{X}{n} = g(n!\,h)$ being 1, we can conclude that $g = \pm 1$; that is, g is a unit. ∎

If a domain D satisfies the ascending chain condition on principal ideals, as does $\mathrm{Int}(\mathbb{Z})$, then every nonzero nonunit element is a product of irreducible elements. But it may happen that an element be decomposed in products of irreducibles of different lengths, that is, $x = p_1 \cdots p_n = q_1 \cdots q_m$ with $m > n$. The upper bound of the ratio $\frac{m}{n}$, considering every element of D, is called the *elasticity* of the domain D [**54**]. Our friend $\mathrm{Int}(\mathbb{Z})$ provides a fairly simple example of infinite elasticity [**15**].

Theorem 7. *The elasticity of* $\mathrm{Int}(\mathbb{Z})$ *is infinite.*

Proof. We just saw that each binomial $\binom{X}{n}$ is irreducible. Now, look at the equality:

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

There are two irreducible factors on the right-hand side, whereas the number n, on the left-hand side, may be chosen to have an arbitrary number of prime factors. ∎

3. ANALYTIC PROPERTIES. Back in 1915, the main result in Pólya's celebrated paper [**48**] was already of an analytical nature, giving a sufficient condition for an entire function to be a polynomial.

Theorem 8. *If $f : \mathbb{C} \to \mathbb{C}$ is an entire function such that*

$$f(\mathbb{N}) \subseteq \mathbb{Z} \quad \textit{and} \quad \limsup_{r\to+\infty} \frac{\ln |f|_r}{r} < \ln 2, \quad \textit{where} \quad |f|_r = \sup_{|z|\le r} |f(z)|,$$

then f is a polynomial, and hence, belongs to $\mathrm{Int}(\mathbb{Z})$. *Moreover, the transcendental function 2^z shows that the bound* $\ln 2$ *is sharp.*

In this section we shall however adopt another point of view and consider integer-valued polynomials as continuous functions in the p-adic topology rather than with respect to the classical Archimedean absolute value.

The *p*-adic ultrametric topology. Given a prime number p and a nonzero integer x, the highest power of p that divides x is called the *p-adic valuation* of x and is denoted by $v_p(x)$. For two nonzero integers x, y, we have

$$v_p(x+y) \ge \inf\{v_p(x), v_p(y)\} \ \text{ and } \ v_p(xy) = v_p(x) + v_p(y).$$

With the conventions $v_p(0) = \infty$ and $p^{-\infty} = 0$, one then defines the *p-adic absolute value* $|x|_p = p^{-v_p(x)}$, and the *p-adic distance* between x and y by $|x-y|_p$. Hence, the higher the power of p dividing $(x-y)$, the closer is x to y. This distance is in fact an *ultradistance*: $|x-z|_p \le \max\{|x-y|_p, |y-z|_p\}$, and we say that $\mathbb{Z}$ is an *ultrametric space*. With such a distance, every ball is a *clopen* (that is, open and closed) subset. For every positive integer h, the set

$$p^h\mathbb{Z} = \{x \in \mathbb{Z} \mid v_p(x) \ge h\} = \{x \in \mathbb{Z} \mid |x|_p \le p^{-h}\}$$

is the clopen ball of center 0 and radius p^{-h}. Finally $\mathbb{Z}$ is the disjoint union of the p^h clopen balls $U_i = i + p^h\mathbb{Z}$ with $0 \le i < p^h$.

The p-adic valuation and the ultrametric p-adic distance can be extended to the field $\mathbb{Q}$ of rational numbers (letting $v_p(a/b) = v_p(a) - v_p(b)$). The p-adic completion of $\mathbb{Q}$ is a field, called the field of *p-adic numbers* and denoted by $\mathbb{Q}_p$, it is a transcendental extension of $\mathbb{Q}$. The completion of $\mathbb{Z}$, that is, the topological closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$ and called the ring of *p-adic integers*. It is worth emphasizing that $\mathbb{Z}_p$ is compact. The closure of $\mathbb{Z}$ in $\mathbb{Q}$ is the ring $\mathbb{Z}_{(p)}$ formed by the rational fractions a/b such that, in reduced form, b is not a multiple of p. (About p-adic numbers and p-adic analysis, see for instance [**50**, Chap. 1].)

Uniform continuity. An integer-valued polynomial can be viewed as a function from $\mathbb{Z}$ to $\mathbb{Z}$. The following shows it is uniformly continuous in a rather precise way.

Proposition 9. *Let f be an integer-valued polynomial. If* $\deg(f) < p^h$, *then*

$$v_p\big(f(b) - f(a)\big) \ge v_p(b-a) - h + 1; \ \textit{that is}, \ |f(b) - f(a)|_p \le p^{h-1}\,|b-a|_p.$$

Proof. Replacing $f(X)$ by $f(a+X) - f(a)$, we assume that $a = 0$ and $f(0) = 0$, and wish to prove that $v_p\big(f(b)\big) \ge v_p(b) - h + 1$. In fact, as f is a linear combination

of binomials, we need only to prove this implication for $f_n = \binom{X}{n}$, with $n < p^h$. The result is obvious for $\binom{X}{0} = 1$ and $\binom{X}{1} = X$. For $n \geq 2$ we write

$$f_n = \binom{X}{n} = \frac{X}{n} g \quad \text{where} \quad g = \frac{\prod_{i=1}^{n-1}(X-i)}{(n-1)!}.$$

Thus $n\, f_n(b) = b\, g(b)$ and hence $v_p\big(f_n(b)\big) = v_p(b) + v_p\big(g(b)\big) - v_p(n)$. The result follows since, on the one hand, $v_p(n) \leq h-1$ (as $n < p^h$) and, on the other, $v_p\big(g(b)\big) \geq 0$ (as g is integer-valued: its degree is $n-1$ and it takes integral values on the n consecutive integers ranging from 1 to n). ∎

In other words, following the formulation of R. Gilmer and W. Smith [**33**, Theorem 2.8], an integer-valued polynomial f with degree $< p^h$ is periodic modulo p^m with period p^{m+h-1} if

$$f(a + p^{m+h-1}) \equiv f(a) \pmod{p^m} \quad \text{for each } a \in \mathbb{Z}.$$

Since integer-valued polynomials are uniformly continuous functions, they can be extended to the p-adic completion of $\mathbb{Z}$. In other words, $\mathrm{Int}(\mathbb{Z})$ is contained in the ring $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ of continuous functions from $\mathbb{Z}_p$ to $\mathbb{Z}_p$. This leads us to the following.

The *p*-adic version of the Stone–Weierstrass theorem. According to the well-known Stone–Weierstrass theorem, for any compact subset F of $\mathbb{R}$, the polynomial ring $\mathbb{R}[X]$ is dense in the ring $\mathcal{C}(F, \mathbb{R})$ of real continuous functions endowed with the uniform convergence topology. As early as 1944, Dieudonné similarly proved that the polynomial ring $\mathbb{Q}_p[X]$ is dense in the ring $\mathcal{C}(F, \mathbb{Q}_p)$ of continuous functions on a compact subset F of $\mathbb{Q}_p$ [**27**, Theorem 4]. As $\mathbb{Z}_p$ is compact and $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, it follows that $\mathbb{Q}[X]$ is dense in $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$, and hence (restricting to functions with values in $\mathbb{Z}_p$) that $\mathrm{Int}(\mathbb{Z})$ is dense in $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$. Mahler established independently an effective version of this result in 1958, writing explicitly the expansion of a continuous function as a series of binomials [**41**, Thm 1].

We give here some insight into these results. We first show how to approximate some specific characteristic functions, but only modulo p. This may seem quite restrictive but Mahler's theorem follows easily and moreover the proof of this very particular case is the most interesting part!

Lemma 10. *For each h, and each i, $0 \leq i < p^h$, the characteristic function φ_i of the clopen ball $U_i = i + p^h\mathbb{Z}_p$ can be approximated modulo p by a linear combination of the binomials $\binom{X}{k}$, $0 \leq k < p^h$.*

Proof. By Proposition 9, for $k < p^h$ the binomials $\binom{X}{k}$ are constant modulo p in each U_i. As $\mathbb{Z}_p$ is the disjoint union of these clopen balls, each $\binom{X}{k}$ is thus modulo p a linear combination of the characteristic functions φ_i. We obtain p^h relations

$$\binom{X}{k} = \sum_{0 \leq i < p^h} \binom{i}{k} \varphi_i + p\delta_k, \text{ with } \delta_i \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p).$$

We can summarize these relations in a matrix identity

$$\Xi = M\Phi + p\Delta,$$

where Ξ, Φ, and Δ are column matrices whose entries are respectively the binomials $\binom{X}{k}$, the characteristic functions φ_i, and the functions δ_k, and where M is the square matrix with entry $\binom{i}{k}$ on line k column i. In fact, M is an upper triangular matrix with entries equal to 1 on the diagonal. Thus M is invertible and its inverse M^{-1} is a square matrix with integral entries $\alpha_{i,k}$. We then have the matrix identity

$$\Phi = M^{-1}\Xi - pM^{-1}\Delta,$$

giving rise to the proposed approximation for each characteristic function φ_i:

$$\varphi_i = \sum_{0\le k<p^h} \alpha_{i,k}\binom{X}{k} + p\gamma_i, \text{ with } \gamma_i \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p). \qquad \blacksquare$$

Every continuous function $\varphi \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ can be likewise approximated; as φ is uniformly continuous, it is constant modulo p in each $U_i = i + p^h\mathbb{Z}_p$ for some h. Thus φ can be approximated modulo p by a linear combination of the corresponding characteristic functions φ_i, and hence by an integer-valued polynomial, since it is so for each φ_i by Lemma 10:

$$\varphi = f_0 + p\gamma_1, \text{ with } f_0 \in \mathrm{Int}(\mathbb{Z}) \text{ and } \gamma_1 \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p).$$

Applying the same procedure to γ_1 we have

$$\varphi = f_0 + pf_1 + p^2\gamma_2, \text{ with } f_1 \in \mathrm{Int}(\mathbb{Z}) \text{and } \gamma_2 \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p).$$

Iterating this procedure, we obtain an approximation modulo p^{n+1}:

$$\varphi = f_0 + pf_1 + \cdots + p^n f_n + p^{n+1}\gamma_{n+1}.$$

The series of functions $\sum_{n=0}^{\infty} p^n f_n$ is therefore uniformly convergent and its sum is φ. We thus obtain the p-adic Stone–Weierstrass theorem.

As each f_n is integer-valued, and hence a linear combination of binomials, we also obtain Mahler's result, expanding $\varphi \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ as a series of binomials with coefficients in $\mathbb{Z}_p$. In fact, Mahler even expands every function $\varphi \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ as a series of binomials with coefficients in $\mathbb{Q}_p$. Indeed, as $\mathbb{Z}_p$ is compact, $p^k\varphi \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$, for some k, and the expansion of φ is immediately derived from that of $p^k\varphi$.

Theorem 11 (Mahler [41]). *Every function $\varphi \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$ can be written*

$$\varphi(x) = \sum_{k=0}^{\infty} c_k\binom{x}{k} \text{ where } c_k \in \mathbb{Q}_p \text{ and } \lim_{k\to\infty}\big(v_p(c_k)\big) = +\infty, \tag{4}$$

where the c_k's are given by the recursive formulae

$$c_k = \varphi(k) - \sum_{i=0}^{k-1} c_i\binom{k}{i}, \text{ or } c_k = \Delta^k\varphi(0). \tag{5}$$

Moreover,

$$\|\varphi\| := \max_{x\in\mathbb{Z}_p} |\varphi(x)|_p = \max_{n\ge 0} |c_n|_p. \tag{6}$$

It is immediate that the coefficients in (5) are given by the same formulae as in (2) or (3) (Gregory–Newton's formula) and we leave (6) to the reader.

One says that the $\binom{X}{n}$'s form an *orthonormal basis* of the Banach space $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$. Formulas (4) and (6) are characteristic of such bases in p-adic analysis. (See [**50**, Chap. 3] for the definition of orthonormal and details.)

4. BACK TO THE RING STRUCTURE. Analytical tools allow us to derive easily many properties seen in section 2. But first we can now describe the prime spectrum.

Prime spectrum. If $\mathfrak{P}$ is a prime ideal of $\mathrm{Int}(\mathbb{Z})$, then the intersection $\mathfrak{P} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and there are two cases: either $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p, $\mathfrak{P}$ is then said to be *above* p, or $\mathfrak{P} \cap \mathbb{Z} = (0)$, $\mathfrak{P}$ is then said to be *above* (0).

One can see (using localization) that the prime ideals above (0) are in one-to-one correspondence with the prime ideals of $\mathbb{Q}[X]$, just as in the case of $\mathbb{Z}[X]$: they are obtained by intersection with $\mathrm{Int}(\mathbb{Z})$ of the prime ideals of $\mathbb{Q}[X]$. Nothing special there, but standard commutative algebra. The prime ideals above p are much more interesting and, in fact, easier to deal with. We gave above an example, for $p = 2$, with the ideal $\mathfrak{M}_{2,0} = \{f \in \mathrm{Int}(\mathbb{Z}) \mid f(0) \text{ is even}\}$. More generally, we could consider $\mathfrak{M}_{p,a} = \{f \in \mathrm{Int}(\mathbb{Z}) \mid f(a) \text{ is a multiple of } p\}$ for each prime p, and each $a \in \mathbb{Z}$. But why stop at $\mathbb{Z}$?

Lemma 12. *For each prime number p and each $\alpha \in \mathbb{Z}_p$ the set*

$$\mathfrak{M}_{p,\alpha} = \{f \in \mathrm{Int}(\mathbb{Z}) \mid v_p\big(f(\alpha)\big) \geq 1\}$$

is a maximal ideal of $\mathrm{Int}(\mathbb{Z})$ *with residue field isomorphic to the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.*

Proof. It is obvious that $\mathfrak{M}_{p,\alpha}$ is an ideal. That its residue field is isomorphic to $\mathbb{F}_p$, and hence that $\mathfrak{M}_{p,\alpha}$ is maximal, follows from the fact that, for each $f \in \mathrm{Int}(\mathbb{Z})$, $f(\alpha) - k$ is a multiple of p for some $k \in \{0, 1, \ldots, p-1\}$. ∎

It follows obviously from the Stone–Weierstrass theorem that these primes are all distinct. A spectacular consequence is that the set of primes above p is uncountable (since $\mathbb{Z}_p$, just like $\mathbb{R}$, is uncountable), so is a fortiori the spectrum of $\mathrm{Int}(\mathbb{Z})$. Another major difference with $\mathbb{Z}[X]$! It turns out there are no other prime ideals above p (we prove this below). We can then summarize the description of the spectrum of $\mathrm{Int}(\mathbb{Z})$.

Theorem 13.

(i) *The prime ideals of* $\mathrm{Int}(\mathbb{Z})$ *above a prime p are in one-to-one correspondence with the elements of $\mathbb{Z}_p$: to $\alpha \in \mathbb{Z}_p$ corresponds the maximal ideal*

$$\mathfrak{M}_{p,\alpha} = \{f \in \mathrm{Int}(\mathbb{Z}) \mid f(\alpha) \in p\mathbb{Z}_p\}.$$

(ii) *The nonzero prime ideals of* $\mathrm{Int}(\mathbb{Z})$ *above* (0) *are in one-to-one correspondence with the irreducible monic polynomials of $\mathbb{Q}[X]$: to the irreducible polynomial q corresponds the prime ideal*

$$\mathfrak{P}_q = q\mathbb{Q}[X] \cap \mathrm{Int}(\mathbb{Z}).$$

(iii) *The ideal $\mathfrak{P}_q$ is contained in the maximal ideal $\mathfrak{M}_{p,\alpha}$ if and only if $q(\alpha) = 0$.*

(iv) *The maximal ideals of* $\mathrm{Int}(\mathbb{Z})$ *are the ideals $\mathfrak{M}_{p,\alpha}$.*

Proof. (Sketch) We only really prove (i). By Lemma 12, it remains to show that every prime $\mathfrak{P}$ above p is an $\mathfrak{M}_{p,\alpha}$. The short proof we give here is due to Sophie Frisch [**31**]. Suppose otherwise; for each $\alpha \in \mathbb{Z}_p$, there is $f_\alpha \in \mathfrak{M}_{p,\alpha}$ such that $f_\alpha \notin \mathfrak{P}$. By continuity there is a neighborhood U_α of α such that $v_p\big(f_\alpha(x)\big) \geq 1$ for all $x \in U_\alpha$. As $\mathbb{Z}_p$ is compact, it can be covered by a finite number of these neighborhoods, say $U_1, \ldots, U_s$, with corresponding integer-valued polynomials $f_1, \ldots, f_s$, none of them in $\mathfrak{P}$. Now consider the product $f = \prod_{i=1}^{s} f_i$. As the U_i's cover $\mathbb{Z}_p$, f is such that $v_p\big(f(x)\big) \geq 1$ everywhere. Thus $g = f/p$ is integer-valued. As $p \in \mathfrak{P}$, it follows that $f = pg \in \mathfrak{P}$. We obtain a contradiction since $\mathfrak{P}$ is prime, $f = \prod_{i=1}^{s} f_i$, and no f_i is in $\mathfrak{P}$.

(ii) Is easily obtained by localization [**16**, Corollary V.1.2].

(iii) It is immediate that $q(\alpha) = 0$ implies $\mathfrak{P}_q \subset \mathfrak{M}_{p,\alpha}$. The converse can be proved using an analytical argument [**16**, Prop. V.2.5].

(iv) One can show that every irreducible polynomial q has a root in $\mathbb{Z}_p$ for some p (in fact infinitely many) [**16**, Proposition V.2.8]. It then follows from (iii) that the corresponding prime $\mathfrak{P}_q$ is not maximal. ∎

Corollary 14. *For every proper finitely generated ideal* $\mathfrak{A}$ *of* $\mathrm{Int}(\mathbb{Z})$, *there is a prime number* p *and an open set* U *of* $\mathbb{Z}_p$ *such that* $\mathfrak{A}$ *is contained in* $\mathfrak{M}_{p,\beta}$ *for each* $\beta \in U$. *(In particular* $\mathfrak{A}$ *is contained in infinitely many maximal ideals* $\mathfrak{M}_{p,\beta}$.*)*

Proof. Let $\mathfrak{A} = (g_1, \ldots, g_s)$ be a proper finitely generated ideal. $\mathfrak{A}$ is contained in some maximal ideal $\mathfrak{M}_{p,\alpha}$, thus $v_p\big(g_i(\alpha)\big) \geq 1$ for each i. By continuity, $v_p\big(g_i(\beta)\big) \geq 1$ for each β in some neighborhood U of α. Thus $\mathfrak{A}$ is contained in $\mathfrak{M}_{p,\beta}$ for each $\beta \in U$. ∎

We derive the following, generalizing Theorem 3.

Corollary 15. *None of the nonzero prime ideals of* $\mathrm{Int}(\mathbb{Z})$ *is finitely generated.*

Proof. Each $\mathfrak{M}_{p,\alpha}$ is contained in only one maximal ideal (itself!). For a given p, each $\mathfrak{P}_q$ is contained in only finitely many $\mathfrak{M}_{p,\alpha}$'s, since q has finitely many roots in $\mathbb{Z}_p$. ∎

We can also derive an easy proof of the Skolem property [Theorem 4].

Corollary 16. $\mathrm{Int}(\mathbb{Z})$ *satisfies the Skolem property.*

Proof. Let $\mathfrak{A}$ be a proper finitely generated ideal. As $\mathfrak{A}$ is contained in $\mathfrak{M}_{p,\beta}$ for each β in some open set U of $\mathbb{Z}_p$ and as $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, $\mathfrak{A}$ is contained in $\mathfrak{M}_{p,a}$ for some $a \in \mathbb{Z}$. Equivalently $\mathfrak{A}(a) \subseteq p\mathbb{Z}$. ∎

Invertible ideals and Prüfer domains. Recall that the *inverse* of a nonzero ideal $\mathfrak{A}$ of a domain D, with quotient field K, denoted by $\mathfrak{A}^{-1}$, is the *conductor* of $\mathfrak{A}$ in D:

$$\mathfrak{A}^{-1} = [D : \mathfrak{A}] = \{x \in K \mid \forall y \in \mathfrak{A}, xy \in D\}.$$

$\mathfrak{A}^{-1}$ is a *fractional ideal* of D. By definition, the product $\mathfrak{A}\,\mathfrak{A}^{-1}$ is contained in D. One says that $\mathfrak{A}$ is *invertible* if actually, $\mathfrak{A}\,\mathfrak{A}^{-1} = D$. This is the case in particular of every nonzero principal $\mathfrak{A} = xD$ (with inverse $\mathfrak{A}^{-1} = x^{-1}D$). It is recorded in every basic

commutative algebra textbook (and easy to prove) that an invertible ideal is finitely generated (for instance, [**35**, Theorem 58]). A domain such that every (nonzero) finitely generated ideal is invertible is called a *Prüfer domain* (equivalently the localization at every maximal ideal is a valuation domain).

Theorem 17. $\mathrm{Int}(\mathbb{Z})$ *is a Prüfer domain.*

Proof. (Sketch) Let $\mathfrak{A} = (f_1, \ldots, f_r)$ be a finitely generated nonzero ideal of $\mathrm{Int}(\mathbb{Z})$. To show that $\mathfrak{A}\,\mathfrak{A}^{-1} = \mathrm{Int}(\mathbb{Z})$, we show that $\mathfrak{A}\,\mathfrak{A}^{-1}$ is not contained in any maximal ideal. Picking a prime p and $\alpha \in \mathbb{Z}_p$, we show it is not contained in $\mathfrak{M}_{p,\alpha}$. We set

$$n = \inf_{f \in \mathfrak{A}} \left\{ v_p\big(f(\alpha)\big) \right\}.$$

We pass on the fact that we can assume that $\mathfrak{A}$ contains a nonzero constant (this is easy but technical, see [**16**, Lemma VI.1.2]). We can thus assume that n is finite. For each generator f_i of $\mathfrak{A}$, we have $v_p\big(f_i(\alpha)\big) \geq n$. By continuity, there is a neighborhood U of α such that, for each $f \in \mathfrak{A}$:

$$\text{for } x \in U,\ v_p\big(f(x)\big) \geq n, \quad \text{for } x \notin U,\ v_p\big(f(x)\big) \geq 0.$$

(The second inequality holds simply because f is integer-valued.) By the Stone–Weierstrass theorem, there is a polynomial $h \in \mathrm{Int}(\mathbb{Z})$ (approximating a suitable continuous function) such that

$$\text{for } x \in U,\ v_p\big(h(x)\big) = 0, \quad \text{for } x \notin U,\ v_p\big(h(x)\big) = n.$$

Hence, for each $f \in \mathfrak{A}$, the product $(h/p^n)\,f$ is integer-valued. By definition we thus have $h/p^n \in \mathfrak{A}^{-1}$. By the choice of n, there is $f_0 \in \mathfrak{A}$ such that $v_p\big(f_0(\alpha)\big) = n$. Hence $v_p\big((h/p^n)\,f_0(\alpha)\big) = 0$, that is, $(h/p^n)\,f_0 \notin \mathfrak{M}_{p,\alpha}$. But $(h/p^n)\,f_0 \in \mathfrak{A}^{-1}\,\mathfrak{A}$. We can conclude that $\mathfrak{A}^{-1}\,\mathfrak{A}$ is not contained in $\mathfrak{M}_{p,\alpha}$. ∎

Corollary 18. $\mathrm{Int}(\mathbb{Z})$ *satisfies the strong Skolem property.*

Proof. (Sketch) Let $\mathfrak{A}$ and $\mathfrak{B}$ be two finitely generated ideals with same ideals of values. As $\mathrm{Int}(\mathbb{Z})$ is a Prüfer domain, $\mathfrak{B}$ is invertible. We can assume that $\mathfrak{A} \subseteq \mathfrak{B}$ (if need be replacing $\mathfrak{B}$ by $\mathfrak{A} + \mathfrak{B}$), hence that $\mathfrak{A}\,\mathfrak{B}^{-1} \subseteq \mathfrak{B}\,\mathfrak{B}^{-1} = \mathrm{Int}(\mathbb{Z})$. With a little bit of work, one can show that $\mathfrak{A}\,\mathfrak{B}^{-1}$ and $\mathfrak{B}\,\mathfrak{B}^{-1}$ have the same ideals of values [**16**, proof of Proposition VII.1.14]: $\forall n \in \mathbb{Z}$, $\mathfrak{A}\,\mathfrak{B}^{-1}(n) = \mathfrak{B}\,\mathfrak{B}^{-1}(n) = \mathbb{Z}$. The Skolem property then implies $\mathfrak{A}\,\mathfrak{B}^{-1} = \mathrm{Int}(\mathbb{Z})$, hence $\mathfrak{A}\,\mathfrak{B}^{-1} = \mathfrak{B}\,\mathfrak{B}^{-1}$, and finally $\mathfrak{A} = \mathfrak{B}$. ∎

5. INTEGER-VALUED POLYNOMIALS ON A SUBSET. Although we shall mostly focus on subsets of $\mathbb{Z}$, we start with some generalities. We first let E be a subset of a domain D, with quotient field K, and consider

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

Finite subsets. Let us first consider the case where E has a single element and, for simplicity, let it be 0. Then $\mathrm{Int}(\{0\}, D)$ is formed by the polynomials with constant term in D. In other words, $\mathrm{Int}(\{0\}, D)$ is a *pullback*:

$$\mathrm{Int}(\{0\}, D) = D + XK[X].$$

More generally, let $E = \{a_0, \ldots, a_n\}$. Each $f \in K[X]$ can be written

$$f = h + (X - a_0) \cdots (X - a_n)g \quad \text{with } g \in K[X] \text{ and } \deg(h) \leq n.$$

Then f and h have the same values on E. By Lagrange interpolation, we thus have

$$\mathrm{Int}(E, D) = \sum_{j=0}^{n} D \prod_{i \neq j} \frac{X - a_i}{a_j - a_i} + (X - a_0)(X - a_1) \cdots (X - a_n)K[X].$$

This being said, we shall from here on assume E to be infinite.

Characteristic ideals. As in the case of the binomials $\binom{X}{n}$ for $\mathrm{Int}(\mathbb{Z})$, one may ask if there is a basis of the D-module $\mathrm{Int}(E, D)$, formed by a sequence $\{f_n\}_{n \geq 0}$ of polynomials with $\deg(f_n) = n$ for each n. Such a basis is called a *regular basis*. The answer is positive in the case of $\mathrm{Int}(E, \mathbb{Z})$, because $\mathbb{Z}$ is a principal ideal domain. For the sake of further reference, we give here a more general result.

We let $\mathfrak{I}_n(E, D)$ be the set formed by the leading coefficients of the degree n polynomials in $\mathrm{Int}(E, D)$ to which we adjoin 0. Each $\mathfrak{I}_n(E, D)$ is clearly a D-module. Moreover it follows by Lagrange interpolation that, for any set $\{a_0, \ldots, a_n\}$ of distinct arguments in E, every degree n polynomial $f \in \mathrm{Int}(E, D)$ is such that $df \in D[X]$, where $d = \prod_{i \neq j}(a_j - a_i)$, and hence, $d\mathfrak{I}_n(E, D) \subseteq D$. Therefore each $\mathfrak{I}_n(E, D)$ is a *fractional ideal* of D.

The ideals $\mathfrak{I}_n(E, D)$ are called the *characteristic ideals* of $\mathrm{Int}(E, D)$. We simply denote by $\mathfrak{I}_n(D)$ the characteristic ideals of $\mathrm{Int}(D)$. Finally, we note that, for each n, $\mathfrak{I}_n(E, D) \subseteq \mathfrak{I}_{n+1}(E, D)$. Indeed, if f is a degree n polynomial in $\mathrm{Int}(E, D)$, then Xf is a degree $n + 1$ polynomial in $\mathrm{Int}(E, D)$.

The following is not very difficult and we state it without proof [**16**, Prop. II.1.4].

Proposition 19. *Let E be an infinite subset of the domain D. The D-module $\mathrm{Int}(E, D)$ admits a regular basis if and only if all the fractional ideals $\mathfrak{I}_n(E, D)$ are principal. Moreover, in this case, a sequence $\{f_n\}_{n \geq 0}$ of polynomials in $\mathrm{Int}(E, D)$, where $\deg(f_n) = n$, forms a regular basis if and only if, for each n, the leading coefficient of f_n generates $\mathfrak{I}_n(E, D)$.*

Newton sequences. In fact, the basis formed by the binomials $\binom{X}{n}$ is much more than a regular basis of $\mathrm{Int}(\mathbb{Z})$. It is linked with the property that the first $n + 1$ integers (more generally, $n + 1$ consecutive integers) form a test set for integer-valued polynomials. Can we find such nice bases for $\mathrm{Int}(E, D)$?

Given a sequence $\{a_n\}_{n \geq 0}$ of distinct elements of E, we define the *generalized binomials* $\binom{X}{a_n}$ by

$$\binom{X}{a_0} = 1 \text{ and, for } n \geq 1, \ \binom{X}{a_n} = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}.$$

Proposition 20. *Let E be an infinite subset of D and $\{a_n\}_{n \geq 0}$ be a sequence of distinct elements of E. Then, the following assertions are equivalent.*

(*i*) *The generalized binomials $\binom{X}{a_n}$ are integer-valued on E.*

(*ii*) *The generalized binomials $\binom{X}{a_n}$ form a basis of the D-module $\mathrm{Int}(E, D)$.*

(*iii*) *A polynomial* $f \in K[X]$ *of degree at most* n *is integer-valued on* E *if and only if it is integer-valued on the first* $n+1$ *terms of the sequence* $\{a_n\}_{n\geq 0}$.

Proof. As in the classical case, $\binom{X}{a_n}$ is the unique degree n polynomial in $K[X]$ such that $f(a_k) = 0$, for $k \leq n-1$, and $f(a_n) = 1$. Thus, as in formulas (1) and (2) in the introduction, a degree n polynomial f with coefficients in K can be expressed as a sum

$$f_n(X) = \sum_{k=0}^{n} c_k \binom{X}{a_k} \text{ with } c_k = f(a_k) - \sum_{j=0}^{k-1} c_j \prod_{i=0}^{j-1} \frac{a_k - a_i}{a_j - a_i}.$$

If the binomials $\binom{X}{a_n}$ are integer-valued and if f takes integer-values on the first $n+1$ terms of the sequence $\{a_n\}_{n\geq 0}$, it follows that $c_k \in D$ for each k, and hence that $f \in \mathrm{Int}(E, D)$. This shows also that the binomials $\binom{X}{a_n}$ form a basis of the D-module $\mathrm{Int}(E, D)$. We have shown that (i) implies (ii) and (iii). That (ii) implies (i) is obvious. Finally, if (iii) holds, then $\binom{X}{a_n}$ is integer-valued on E as it takes only the value 0 or 1 on the first $n+1$ terms of the sequence $\{a_n\}_{n\geq 0}$. ∎

When it exists, a sequence that satisfies the equivalent conditions of Proposition 20 is called a *Newton sequence*. It may be there is no such sequence, but for subsets of $\mathbb{Z}$ one can at least obtain one *locally*. Let us explain what we mean by that.

Local study: *p*-orderings. The very simple but fruitful notion of p-ordering was introduced by Manjul Bhargava [**6, 7, 8**]. Considering a subset E of $\mathbb{Z}$ and choosing a prime number p, let us play in his own terms, as in [**8**], the *game called p-ordering*:

- choose any element $a_0 \in E$;
- choose an element $a_1 \in E$ that minimizes the highest power of p dividing $a_1 - a_0$;
- choose an element $a_2 \in E$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$;

and so on.

Denoting by $v_p(x)$ (as in section 3) the highest power of p dividing x, we can say that a *p-ordering of E* is a sequence $\{a_n\}_{n\geq 0}$ of elements of E such that

$$\forall n \geq 1,\ v_p\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \min_{x\in E} v_p\left(\prod_{k=0}^{n-1}(x - a_k)\right).$$

Let $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$ be the ring formed by the rational numbers a/b such that, in reduced form, b is not a multiple of p. If $\{a_n\}_{n\geq 0}$ is a p-ordering, for each $n \geq 0$ and each $x \in E$, we have, by definition, $\prod_{k=0}^{n-1} \frac{x-a_k}{a_n-a_k} \in \mathbb{Z}_{(p)}$. In other words, the corresponding generalized binomials $\binom{X}{a_n}$ belong to $\mathrm{Int}(E, \mathbb{Z}_{(p)})$. A p-ordering is thus nothing else than a Newton sequence of E considered as a subset of $\mathbb{Z}_{(p)}$!

As noted by J. Yeramian [**56**], p-orderings in the case of $\mathbb{Z}$ are nothing else than the *very well distributed sequences* introduced by Y. Amice [**5**] back in 1964: a sequence $\{a_n\}_{n\geq 0}$ is a p-ordering of $\mathbb{Z}$ if and only if for each k, and each s, the p^k consecutive terms $\{a_{sp^k}, a_{sp^k+1}, \ldots, a_{(s+1)p^k-1}\}$ form a complete system of representatives of $\mathbb{Z}$ modulo p^k. Amice even considered subsets but had to restrict herself to the so called *regular subsets* [see Example 2 below]. The beauty of p-orderings is that it applies to any subset. Where Amice generalized Mahler's theorem only for regular compact subsets, p-orderings allowed Bhargava and Kedlaya [**11**] to consider any compact subset.

Theorem 21. *Let E be a compact subset of $\mathbb{Z}_p$. For every p-ordering $\{a_n\}_{n\geq 0}$ of E, the binomials $\binom{X}{a_n}$ form an orthonormal basis of the Banach space $\mathcal{C}(E, \mathbb{Q}_p)$.*

The *p*-sequence. Given a p-ordering $\{a_n\}_{n\geq 0}$, we set

$$w_{E,p}(n) = v_p\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \sum_{k=0}^{n-1} v_p(a_n - a_k). \tag{7}$$

Clearly, p-orderings are far from unique, since there may be a choice at each step, which we see as follows.

Proposition 22. *The sequence $\{w_{E,p}(n)\}_{n\geq 0}$ depends only on E and p.*

Proof. Having a Newton sequence, the binomials $\binom{X}{a_n}$ form a regular basis of Int $(E, \mathbb{Z}_{(p)})$. The leading coefficient $\left(\prod_{k=0}^{n-1}(a_n - a_k)\right)^{-1}$ is thus a generator of the characteristic ideal $\mathfrak{I}_n(E, \mathbb{Z}_{(p)})$. Obviously this ideal does not depend on the choice of the p-ordering! The largest power of p dividing $\prod_{k=0}^{n-1}(a_n - a_k)$ is thus the same for every p-ordering. ∎

The sequence $\{w_{E,p}(n)\}_{n\geq 0}$ is called the *p-sequence of E*.

Remark 2. Note that each difference $a_n - a_k$ as in formula (7) is divisible by only finitely many primes. One can thus show that $w_{E,p}(n) = 0$ for almost every p.

Examples 23.

1. The sequence $\{n\}_{n\geq 0}$ is a p-ordering of $\mathbb{Z}$ (for every p). From Legendre's formula [**38**], one then has

$$w_{\mathbb{N},p}(n) = v_p(n!) = \sum_{k\geq 1}\left\lfloor \frac{n}{p^k} \right\rfloor.$$

2. Let E be a subset of $\mathbb{Z}$ and q_k be the number of classes modulo p^k met by E. The subset E is said to be *regular with respect to p* in Amice's sense [**5**] if, for each k, in each class modulo p^k met by E, E meets the same number of classes modulo p^{k+1}. In this case q_k divides q_{k+1}. Building a very well distributed sequence, Amice then established *Legendre's generalized formula*:

$$w_{E,p}(n) = \sum_{k\geq 1}\left\lfloor \frac{n}{q_k} \right\rfloor. \tag{8}$$

   Conversely S. Evrard and Y. Fares [**28**] showed that if $w_{E,p}(n) = \sum_{k\geq 1}\left\lfloor \frac{n}{q_k} \right\rfloor$ then the p-adic topological closure of E is a regular subset and that this is the case if and only if E admits a very well distributed sequence.

3. Let $E = \mathbb{Z} \setminus p\mathbb{Z}$ be the set of integers not divisible by p, then

$$w_{E,p}(n) = \sum_{k\geq 0}\left\lfloor \frac{n}{(p-1)p^k} \right\rfloor. \tag{9}$$

Note that E is regular and that $w_{E,p}(n)$ fits with Legendre's generalized formula. A p-ordering of E is given by the sequence of positive integers that are not divisible by p [**12**].

Globalization: simultaneous orderings. A sequence $\{a_n\}_{n\geq 0}$ is a p-ordering of E for each prime p if and only if the corresponding generalized binomials $\binom{X}{a_n}$ are in $\mathrm{Int}(E, \mathbb{Z}_{(p)})$ for each p, hence if and only if they are in $\mathrm{Int}(\mathbb{Z})$, since $\mathbb{Z} = \bigcap_{p\in\mathbb{P}} \mathbb{Z}_{(p)}$. Such a sequence, often called a *simultaneous p-ordering*, is therefore in fact nothing else than a Newton sequence.

Examples 24. A sequence is said to be *self-simultaneously ordered* if it is a Newton sequence of the subset formed by its own elements. The following sequences are self-simultaneously ordered:

$$\left\{(-1)^n \left[\tfrac{n}{2}\right]\right\}_{n\geq 1}, \quad \{n^2\}_{n\geq 0}, \quad \left\{\tfrac{n(n+1)}{2}\right\}_{n\geq 0},$$

$$\{q^n\}_{n\geq 0}\ (q \neq 0, 1, -1), \quad \{F_n = 2^{2^n} + 1\}_{n\geq 0}.$$

Denoting by $\mathbb{N}^2 = \{n^2 \mid n \geq 0\}$ the set of square numbers, it follows for instance that the binomials $\prod_{k=0}^{n-1} \frac{X-k^2}{n^2-k^2}$ form a regular basis of $\mathrm{Int}(\mathbb{N}^2, \mathbb{Z})$, and that a degree n polynomial is integer-valued on all squares if and only if it is so up to n^2. We have similar statements for each of these sequences.

Observe that the sequence $\{F_n = 2^{2^n} + 1\}_{n\geq 0}$ of Fermat numbers is the orbit of 3 under the iteration of the quadratic polynomial $f = X^2 - 2X + 2$. In fact, the last two examples follow from a general property [**4**, Proposition 18].

Proposition 25. *If f is a nonconstant polynomial of $\mathbb{Z}[X]$, distinct from $\pm X$, then every infinite orbit $\{b, f(b), f(f(b)), \ldots\}$, for $b \in \mathbb{Z}$, is self-simultaneously ordered.*

Question. It is easy to see that if $\{a_n\}_{n\geq 0}$ is self-simultaneously ordered, then so is the sequence $a\{a_n + b\}_{n\geq 0}$ $(a, b \in \mathbb{Z}, a \neq 0)$. Are there any other self-simultaneously ordered sequences aside the sequences obtained by such an affine transformation from the sequences listed above or by iteration of a polynomial? Note for instance that $\{n^k\}_{n\geq 0}$ is not self-simultaneously ordered, for $k \geq 3$ [**4**].

An algorithm to construct a regular basis. Starting with $f_0 = 1$, assume we have the first terms $f_0, f_1, \ldots, f_{n-1}$ of a regular basis of $\mathrm{Int}(E, \mathbb{Z})$. We show how to obtain f_n, using p-orderings.

For each prime p such that $w_{E,p}(n) \neq 0$, we let $\{a_{p,k}\}_{k\geq 0}$ be a p-ordering of E. By Remark 2 there are finitely many such primes and the Chinese remainder theorem provides $n + 1$ integers $b_{n,k}$, $0 \leq k \leq n$, such that, for each such p and each k,

$$v_p(b_{n,k} - a_{p,k}) > w_{E,p}(n).$$

Finally let

$$f_n = \frac{1}{\prod_{p\in\mathbb{P}} p^{w_{E,p}(n)}} \prod_{k=0}^{n-1} (X - b_{n,k}).$$

Keep the product $\prod_{p\in\mathbb{P}} p^{w_{E,p}(n)}$ in mind for what comes next (it looks like an infinite product, but $p^{w_{E,p}(n)} = 1$ for almost every p). For every prime p, $f_0, f_1, \ldots, f_n$ are the

first terms of a regular basis of $\mathrm{Int}(E, \mathbb{Z}_{(p)})$. If $w_{E,p}(n) \neq 0$, this is because, replacing $a_{p,k}$ by $b_{n,k}$ for $0 \leq k \leq n$, we still have a p-ordering, otherwise this is because the leading coefficient of f_n is a unit in $\mathbb{Z}_{(p)}$. It is easy to conclude that $f_0, f_1, \ldots, f_n$ are the first terms of a regular basis of $\mathrm{Int}(E, \mathbb{Z})$.

Remark 3. This algorithm provides a regular basis but not a Newton sequence, and this is for two reasons; the integers $b_{n,k}$ are not necessarily in E. Moreover they depend on the degree n, as there are more and more primes such that $w_{E,p}(n) \neq 0$ as n increases. Also they do not form a test set of arguments, even for the polynomials of degree at most n, that is, it is not enough that a polynomial of degree $m \leq n$ takes integer-values on the first $m + 1$ of terms of the sequence $b_{n,0}, b_{n,1}, \ldots, b_{n,n}$ to be integer-valued (as opposed to assertion (iii) in Proposition 20).

Bhargava's factorials. Observing that $n! = \prod_{p \in \mathbb{P}} p^{w_{\mathbb{Z},p}(n)}$ (by Legendre's formula), Bhargava proposed, in [**8**] (entitled *The factorial Function and Generalizations*), to define similarly the *factorial function of a subset E* as

$$n!_E = \prod_{p \in \mathbb{P}} p^{w_{E,p}(n)}.$$

And yes, $\prod_{p \in \mathbb{P}} p^{w_{E,p}(n)}$ is the product encountered in the previous algorithm! In other words, $\frac{1}{n!_E}$ is the leading coefficient of f_n in the regular basis we constructed above. Equivalently, by Proposition 19, $\frac{1}{n!_E}$ is a generator of the characteristic ideal $\mathfrak{I}_n(E, \mathbb{Z})$.

Bhargava then described several fine properties (generalizing classical factorials).

1. For every two nonnegative integers m and n, $(m + n)!_E$ is a multiple of $m!_E\, n!_E$.
2. If f is a primitive polynomial of degree at most n, then $n!_E$ is a multiple of the *fixed divisor* $d(f, E) = \gcd\{f(a) \mid a \in E\}$ of f in E.
3. Let $a_0, a_1, \ldots, a_n \in E$. Then the product $\prod_{0 \leq i < j \leq n}(a_j - a_i)$ is a multiple of $1!_E\, 2!_E \cdots n!_E$.
4. The number of polynomial functions from E to $\mathbb{Z}/n\mathbb{Z}$ (that is, functions induced by a polynomial of $\mathbb{Z}[X]$) is equal to $\prod_{k=0}^{n-1} \frac{n}{\gcd(n, k!_E)}$ (a generalization of Kempner's formula [**36**]).

The beauty of integer-valued polynomials is to allow one to prove easily most of these properties. For instance, the first one follows immediately from the fact that the product of two integer-valued polynomials respectively of degree n and m is an integer-valued polynomial of degree $n + m$. We invite the reader to read Bhargava's proofs, having integer-valued polynomials in mind, and using an extra property [**8**, Lemma 13] that follows immediately from the containment $\mathrm{Int}(F, \mathbb{Z}) \subseteq \mathrm{Int}(E, \mathbb{Z})$ if $E \subseteq F$:

5. If E, F are two subsets such that $E \subseteq F$, then $n!_E$ is a multiple of $n!_F$.

In particular, for every subset E of $\mathbb{Z}$, $n!_E$ is a multiple of $n!$.

Factorials and Newton sequences. If E admits a simultaneous ordering $\{a_n\}_{n \geq 0}$, that is, a Newton sequence, the leading coefficient of the generalized binomial $\binom{X}{a_n}$ is $\frac{1}{\prod_{k=0}^{n-1}(a_n - a_k)}$. We thus simply have

$$n!_E = \left| \prod_{k=0}^{n-1} (a_n - a_k) \right|.$$

Examples 26. • $E = \{an + b \mid n \geq 0\},\ n!_E = a^n n!$;
• $E = \{n^2 \mid n \geq 0\},\ n!_E = \dfrac{(2n)!}{2}$; • $E = \{\frac{n(n+1)}{2} \mid n \geq 0\},\ n!_E = \dfrac{(2n)!}{2^n}$;
• $E = \{q^n \mid n \geq 0\}, n!_E = q^{\frac{n(n-1)}{2}}(q^n - 1)(q^{n-1} - 1)\cdots(q - 1)$;
(Jackson's factorials).

Bhargava raises several questions in [**8**]. For instance whether there is a combinatorial interpretation of $n!_E$, observing that the generalized binomial coefficients

$$\binom{n}{k}_E = \frac{n!_E}{k!_E (n_k)!_E}$$

are integers by property 1 above. He also asks about analogues of the Stirling or exponential functions. Some answers have been given in this last case [**42**]. The generalized exponential

$$\exp_E(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!_E}$$

converges everywhere, since $n!$ divides $n!_E$. The generalized Euler number

$$e_E = \sum_{n=0}^{\infty} \frac{1}{n!_E}$$

is such that $1 < e_E \leq e$ and never rational. For instance, for $\mathbb{N}^{(2)} = \{n^2 \mid n \geq 0\}$, $\exp_{\mathbb{N}^{(2)}}(x) = 2\cosh\sqrt{|x|}$ and $e_{\mathbb{N}^{(2)}} = e + \frac{1}{e}$ is transcendental.

Questions. • When is $e_E = \sum_{n=0}^{\infty} \frac{1}{n!_E}$ a transcendental number?
• Mingarelli [**42**] noticed there cannot be three equal consecutive terms in the sequence $\{n!_E\}_{n\geq 0}$, whatever the subset E. Indeed, $k!_E = (k+1)!_E = (k+2)!_E$ would imply $2!_E = 1$ (since $(k+2)!_E$ is a multiple of $2!_E\, k!_E$). He then raised the question: is there a subset E such that $n!_E = (n+1)!_E$ for infinitely many n?

Polynomially equivalent subsets. It is clear that $\mathrm{Int}(\mathbb{N}, \mathbb{Z}) = \mathrm{Int}(\mathbb{Z})$, as it follows immediately from Corollary 2 that a degree n polynomial is in $\mathrm{Int}(\mathbb{Z})$ as soon as it takes integer-values on $n+1$ consecutive nonnegative integers. R. Gilmer devoted a paper on *Sets that determine integer-valued polynomials* [**32**]. More generally, one can ask under which conditions two subsets E and F are such that $\mathrm{Int}(E, \mathbb{Z}) = \mathrm{Int}(F, \mathbb{Z})$. We start with some definitions given in all generality for subsets of a domain D.

- If two subsets E and F are such that $\mathrm{Int}(E, D) = \mathrm{Int}(F, D)$, we say that E and F are *polynomially equivalent*.
- For each subset E, $\overline{E} = \{x \in K \mid \forall f \in \mathrm{Int}(E, D),\ f(x) \in D\}$ is clearly the largest subset of D polynomially equivalent to E. We say that $\overline{E}$ is the *polynomial closure* of E.
- If $\overline{E} = E$, we say that E is *polynomially closed* and, if $\mathrm{Int}(E, D) = \mathrm{Int}(D)$, we say that E is *polynomially dense* in D.

Analytical tools allow us to settle the question of (polynomially) equivalent and dense subsets of $\mathbb{Z}$.

Proposition 27. (i) *Two subsets of $\mathbb{Z}$ are polynomially equivalent if and only if, for every prime p, they have the same p-adic closure in $\mathbb{Z}_p$.*

(ii) *A subset is polynomially dense in $\mathbb{Z}$ if and only if, for every prime p, it is topologically dense in $\mathbb{Z}$ in the p-adic topology.*

(iii) *The polynomial closure of a subset is the intersection of its p-adic closures in $\mathbb{Z}$.*

Proof. (i) Two subsets E and F, have the same p-adic completion, if and only if $\mathrm{Int}(E, \mathbb{Z}_p) = \mathrm{Int}(F, \mathbb{Z}_p)$. This condition is necessary by continuity, it is sufficient by the p-adic analogue of the Stone–Weierstrass theorem. The result follows using the fact that $\mathrm{Int}(E, \mathbb{Z}) = \mathbb{Q}[X] \bigcap_{p\in\mathbb{P}} \mathrm{Int}(E, \mathbb{Z}_p)$. (ii) and (iii) follow immediately from (i). ∎

The subset $\mathbb{P}$. Let us finally pay a particular attention to the subset $\mathbb{P}$ formed by the prime numbers. By Dirichlet's theorem on primes in arithmetical progression, the p-adic closure of $\mathbb{P}$ in $\mathbb{Z}$ is $\{p\} \cup (\mathbb{Z} \setminus p\mathbb{Z})$. The polynomial closure of $\mathbb{P}$ is thus

$$\overline{\mathbb{P}} = \mathbb{P} \cup \{-1, +1\}.$$

From formula (9) in Examples 23, we derive

$$w_{\mathbb{P},p}(n) = \sum_{k\geq 0} \left\lfloor \frac{n-1}{(p-1)p^k} \right\rfloor \quad [\mathbf{25}]. \tag{10}$$

We then obtain the factorial

$$n!_{\mathbb{P}} = \prod_{p\in\mathbb{P}} p^{\sum_{k\geq 0}\left\lfloor \frac{n-1}{(p-1)p^k}\right\rfloor}. \tag{11}$$

The sequence $\{n!_{\mathbb{P}}\}_{n\geq 0} = \{1, 1, 2, 24, 48, 5760, 11520, \ldots\}$ is sequence A053657 in *The On-Line Encyclopedia of Integer Sequences* (but not sequence A002552 which begins with the same seven first terms). There are links with Bernoulli numbers, as already described by Bhargava [**8**, Example 21] (see also [**23**, §4] for more details), but also with Bernoulli polynomials $B_n^{(m)}$. Let us recall that the $B_n^{(m)}$'s are defined by $\left(\frac{z}{e^z-1}\right)^m = \sum_{n=0}^{\infty} B_n^{(m)} \frac{z^n}{n!}$, and it turns out that $(n+1)!_{\mathbb{P}} B_n^{(m)}$ is a primitive polynomial in $\mathbb{Z}[X]$ (that is, the gcd of its coefficients is 1) [**24**, §2].

These factorials appear also in other contexts. First in group theory: $(n+1)!_{\mathbb{P}}$ is equal to the nth Minkowski number, that is, the least common multiple of the orders of all finite subgroups of $GL_n(\mathbb{Q})$ (cf. Minkowski [**43**] and Schur [**51**]). And also in algebraic topology: following Johnson [**34**], they are the denominators of the Laurent polynomials forming a regular basis for the Hopf algebroid of stable cooperations for complex K-theory.

Using the algorithm described above to construct a regular basis, the $b_{n,k}$'s may be chosen in $\mathbb{P}$ (thanks to Dirichlet's theorem). For instance, for $n = 5$, we may choose 1, 2, 3, 5, 79 [**25**] (1 is not really a prime, but it is in the polynomial closure of $\mathbb{P}$). We obtain a basis of $\mathrm{Int}(\mathbb{P}, \mathbb{Z})$ starting with

$$1,\ (X-1),\ \frac{(X-1)(X-2)}{2},\ \frac{(X-1)(X-2)(X-3)}{24},$$
$$\frac{(X-1)(X-2)(X-3)(X-5)}{48},\ \frac{(X-1)(X-2)(X-3)(X-5)(X-79)}{5760}.$$

Finally, we have the following test for the polynomials of degree at most n [**22**]:

$$f \in \mathrm{Int}(\mathbb{P}, \mathbb{Z}) \iff \begin{cases} \text{for } p \in \mathbb{P},\ p \leq n+1,\ f(p) \in \mathbb{Z} \\ \text{for } k \in \mathbb{N},\ k \leq 2n-1,\ k^{2n-5} f(k) \in \mathbb{Z}. \end{cases} \tag{12}$$

Question. If a subset E admits a Newton sequence, the polynomials of degree at most n can be tested on $n+1$ elements. In general, is there a test set of $\varphi(n)$ elements, with some control on $\varphi(n)$? Or at least a finite test of some sort as in (12) for integer-valued polynomials on the prime numbers?

6. NUMBER FIELDS AND MORE. We now turn to the study of integer-valued polynomials in number fields, as initiated by Pólya in [**49**] and Ostrowski in [**47**]. We shall use localization and first consider this standard tool of commutative algebra in the more general frame of a domain D, with quotient field K.

Localization. A *multiplicative subset* S of the domain D is a subset stable under multiplication, with $0 \notin S$ and $1 \in S$. The *localization of D with respect to S*, denoted by $S^{-1}D$, is the set of fractions

$$S^{-1}D = \{a/s \in K \mid a \in A, s \in S\}.$$

This set is an overring of D. In particular, the complement $S = D \setminus \mathfrak{p}$ of a prime ideal $\mathfrak{p}$ is a multiplicative subset. The corresponding localization is called the *localization with respect to* $\mathfrak{p}$ and is denoted by $D_{\mathfrak{p}}$. The ring $D_{\mathfrak{p}}$ has only one maximal ideal (namely, the extension $\mathfrak{p}D_{\mathfrak{p}}$ of the prime $\mathfrak{p}$). One says that $D_{\mathfrak{p}}$ is a *local* ring (some people say *quasi-local* in the non-Noetherian case). Local rings are often simpler to deal with.

Lemma 28. *Let S be a multiplicative subset of the domain D with quotient field K. If a polynomial $f \in K[X]$ is such that $f(D) \subseteq S^{-1}D$, then $f(S^{-1}D) \subseteq S^{-1}D$.*

Proof. Sketch: the result is trivial for a constant. By induction on the degree, if f is of degree n, to show that $f(a/s) \in S^{-1}D$, one considers the polynomial of lesser degree $g(X) = s^n f(X) - f(sX)$. ■

As S can also be considered as a multiplicative subset of $\mathrm{Int}(D)$, one can easily derive the containment $S^{-1}\mathrm{Int}(D) \subseteq \mathrm{Int}(S^{-1}D)$. It is not too difficult to show that this containment is an equality in the Noetherian case [**16**, Theorem I.2.3]. In particular, we have the following.

Proposition 29. *Let D be a Noetherian domain. For each prime ideal $\mathfrak{p}$ of D, one has*

$$\mathrm{Int}(D)_{\mathfrak{p}} = \mathrm{Int}(D_{\mathfrak{p}}).$$

Remark 4. As already noted above, if $f \in \mathrm{Int}(D)$ is of degree n, it follows from Lagrangian interpolation that, for every set of arguments $\{a_0, a_1, \ldots, a_n\}$, $df \in D[X]$ where $d = \prod_{i \neq j}(a_i - a_j)$. If $D/\mathfrak{p}$ is infinite, in particular, if $\mathfrak{p}$ is not maximal, these arguments can be chosen in distinct classes modulo $\mathfrak{p}$, thus $d \notin \mathfrak{p}$, and so one has the containment $\mathrm{Int}(D) \subseteq D_{\mathfrak{p}}[X]$, and the equalities $\mathrm{Int}(D)_{\mathfrak{p}} = \mathrm{Int}(D_{\mathfrak{p}}) = D_{\mathfrak{p}}[X]$.

When there is such a nonzero prime ideal $\mathfrak{p}$ with an infinite residue ring, many of the beautiful properties of $\mathrm{Int}(\mathbb{Z})$ are then lost: for instance, $\mathrm{Int}(D)$ cannot be a Prüfer domain since the overring $D_{\mathfrak{p}}[X]$ is not Prüfer; moreover, $\mathrm{Int}(D_{\mathfrak{p}})$ is not dense in

$\mathcal{C}(\widehat{D_\mathfrak{p}}, \widehat{D_\mathfrak{p}})$, where $\widehat{D_\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic completion of $D_\mathfrak{p}$. Also, the prime ideals of $\mathrm{Int}(D)$ above $\mathfrak{p}$ are obtained by intersection of $\mathrm{Int}(D)$ with the primes of $D_\mathfrak{p}[X]$ above $\mathfrak{p}$, and there is nothing special to them, as in the case of the primes above (0) in $\mathrm{Int}(\mathbb{Z})$ [Theorem 13 (ii)]. This is why the study of integer-valued polynomials is focused on domains for which every nonzero prime ideal is maximal with finite residue field, and such are precisely the rings of integers of number fields.

Number fields and valuations. Recall that a number field K is a finite extension of $\mathbb{Q}$, that its ring of integers $\mathcal{O}_K$ is formed by the elements of K which are roots of monic polynomials with integral coefficients, and that the quotient field of $\mathcal{O}_K$ is K itself. We shall see that $\mathrm{Int}(\mathcal{O}_K)$ has algebraic properties like those of $\mathrm{Int}(\mathbb{Z})$. The reason is that we can use very similar analytical tools, replacing p-adic valuations by $\mathfrak{m}$-adic valuations.

Given a maximal ideal $\mathfrak{m}$ of the ring of integers $\mathcal{O}_K$ of a number field K and a nonzero element x, the highest power of $\mathfrak{m}$ such that x belongs to $\mathfrak{m}^n$ is called the $\mathfrak{m}$-*adic valuation* of x and is denoted by $v_\mathfrak{m}(x)$. It can be extended to the number field K, letting $v_\mathfrak{m}(a/b) = v_\mathfrak{m}(a) - v_\mathfrak{m}(b)$.

More generally a *discrete valuation* on a field K is a map $v : K^\star \to \mathbb{Z}$ such that, alike the p-adic valuation, for two nonzero elements x, y:

$$v(x + y) \geq \inf\{v(x), v(y)\} \text{ and } v(xy) = v(x) + v(y).$$

One also sets $v(0) = \infty$. With the convention $e^{-\infty} = 0$, one defines an absolute value $|x| = e^{-v(x)}$, and a distance by $d(x, y) = |x - y|$ on K. The set $V = \{x \in K \mid v(x) \geq 0\}$ is a ring called the *ring of the valuation* v: it is a principal ideal domain with a single maximal ideal $\mathfrak{m} = \{x \in K \mid v(x) > 0\}$. One can consider the completion $\widehat{V}$ of V (and the completion of K), as we considered $\mathbb{Z}_p$ (and $\mathbb{Q}_p$).

The ring of the $\mathfrak{m}$-adic valuation is the localization $(\mathcal{O}_K)_\mathfrak{m}$, and the residue field of this discrete valuation domain, isomorphic to $\mathcal{O}_K/\mathfrak{m}$, is finite. By Proposition 29, we have $(\mathrm{Int}(\mathcal{O}_K))_\mathfrak{m} = \mathrm{Int}((\mathcal{O}_K)_\mathfrak{m})$. To study $\mathrm{Int}(\mathcal{O}_K)$, we may thus first consider integer-valued polynomials over a valuation domain V with finite residue field.

We can consider integer-valued polynomials on V as continuous functions from the completion $\widehat{V}$ into itself. Since the residue field of V is finite, $\widehat{V}$ is compact and we have the analogue of the Stone–Weierstrass theorem: $\mathrm{Int}(V)$ is dense in $\mathcal{C}(\widehat{V}, \widehat{V})$. We can easily derive, as for $\mathrm{Int}(\mathbb{Z})$ that the prime ideals of $\mathrm{Int}(V)$ above the maximal ideal of V are in one-to-one correspondence with the elements of $\widehat{V}$ and that $\mathrm{Int}(V)$ is a Prüfer domain. By globalization we obtain similar results for the ring $\mathcal{O}_K$ of integers of a number field, and more generally, for a *Dedekind* domain D with finite residue fields, that is, a Noetherian domain such that $D_\mathfrak{m}$ is a discrete valuation domain for each maximal ideal $\mathfrak{m}$.

Theorem 30. *Let D be a Dedekind domain with finite residue fields.*

(i) *For each maximal ideal $\mathfrak{m}$ of D, the prime ideals of* $\mathrm{Int}(D)$ *above* $\mathfrak{m}$ *are in one-to-one correspondence with the elements of the completion $\widehat{D}_\mathfrak{m}$ of $D_\mathfrak{m}$:*

$$\alpha \in \widehat{D}_\mathfrak{m} \mapsto \mathfrak{M}_{\mathfrak{m},\alpha} = \{f \in \mathrm{Int}(D) \mid f(\alpha) \in \mathfrak{m}\widehat{D}_\mathfrak{m}\} \in \mathrm{Max}(\mathrm{Int}(D)).$$

(ii) $\mathrm{Int}(D)$ *is is a Prüfer domain.*

Moreover, in the case where $D = \mathcal{O}_K$ the ring of integers of a number field K,

(iii) *the maximal ideals of* $\mathrm{Int}(\mathcal{O}_K)$ *are the ideals* $\mathfrak{M}_{\mathfrak{m},\alpha}$,

(iv) $\mathrm{Int}(\mathcal{O}_K)$ *satisfies the strong Skolem property.*

Remark 5. Properties (iii) and (iv) hold in case $D = \mathcal{O}_K$, the ring of integers of a number field, as for $\mathrm{Int}(\mathbb{Z})$, with very similar proofs, but fail to hold in general for a Dedekind domain. For instance, both properties always fail to hold for a local domain, Dedekind or not for that matter. Indeed, if m is a nonzero element of the unique maximal ideal of a local domain D, the irreducible polynomial $q = 1 + mX$, is then such that $q(a) = 1 + am$ is a unit for each $a \in D$. Yet the principal ideal generated by q is a proper ideal of $\mathrm{Int}(D)$, thus down goes the Skolem property, let alone the strong Skolem property! Also to q corresponds a prime ideal $\mathfrak{P}_q$ above (0) that is maximal.

***v*-orderings.** Pólya and Ostrowski studied the additive structure of the ring $\mathrm{Int}(\mathcal{O}_K)$. But unlike the previous algebraic properties, this structure is quite different from the case of $\mathrm{Int}(\mathbb{Z})$: there is no Newton sequence, and thus no way to test a degree n polynomial on $n + 1$ elements. Sometimes there is even no regular basis! Once again, life is easier in the local case; that is, considering $\mathrm{Int}((\mathcal{O}_K)_{\mathfrak{m}})$ rather than $\mathrm{Int}(\mathcal{O}_K)$. And once again, we may as well first consider a discrete valuation domain V with finite residue field, denoting by v the corresponding valuation, $\mathfrak{m}$ its maximal ideal, and q the cardinality of $V/\mathfrak{m}$ (when one considers $\mathcal{O}_K$, q is the *norm* of $\mathfrak{m}$, denoted by $N(\mathfrak{m})$, that is, the cardinality of $\mathcal{O}_K/\mathfrak{m}$).

Generalizing the notion of p-ordering, it is possible to build a sequence $\{a_n\}_{n\geq 0}$, choosing a_0 arbitrarily, and then inductively a_n such that

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

Such a sequence is called a *v-ordering*. By these choices, the generalized binomials $\binom{X}{a_n} = \prod_{k=0}^{n-1} \frac{X-a_k}{a_n-a_k}$ are integer-valued, hence $\{a_n\}_{n\geq 0}$ is a Newton sequence of V. The binomials $\binom{X}{a_n}$ form a regular basis of $\mathrm{Int}(V)$ and a degree n polynomial in $K[X]$ belongs to $\mathrm{Int}(V)$ if and only if it takes integral values on the $n + 1$ terms of the sequence $\{a_n\}_{n\geq 0}$ (see [Proposition 20]).

As for p-orderings, v-orderings are far from unique but the valuation of the product $\prod_{k=0}^{n-1}(a_n - a_k)$ depends only on n and on the ring V. In fact, it depends only on n and q, as we see next, building explicitly a v-ordering. We thus denote it by $w_q(n)$.

Choose a set of representatives $a_0 = 0, a_1, \ldots, a_{q-1}$ of $V/\mathfrak{m}$ and choose π in V such that $v(\pi) = 1$. Then, writing every integer n in its base q expansion, that is,

$$n = n_0 + n_1 q + \cdots + n_r q^r$$

with $0 \leq n_i < q$ for each n_i, set

$$a_n = a_{n_0} + a_{n_1}\pi + \cdots + a_{n_r}\pi^r. \tag{13}$$

If $v_q(n - m)$ denotes the largest h such that q^h divides $n - m$, it is easy to see that

$$v_{\mathfrak{m}}(a_n - a_m) = v_q(n - m). \tag{14}$$

It follows that, for each k, the q^k first terms of the sequence $\{a_n\}_{n\geq 0}$ form a complete set of representatives of $V/\mathfrak{m}^k$. One can derive that the sequence $\{a_n\}_{n\geq 0}$ is a v-ordering [**16**, Lemma II.2.6] and a formula for $w_q(n)$ [**16**, Lemma II.2.4]:

$$w_q(n) = v\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \sum_{k=0}^{n-1} v(a_n - a_k) = \sum_{l=1}^{n} v_q(l) = \sum_{k\geq 1}\left[\frac{n}{q^k}\right].$$

Note that the formula $w_q(n) = \sum_{k\geq 1}\left[\frac{n}{q^k}\right]$ is similar to Legendre's formula.

Remark 6. Formula (14) shows that for each h, the truncated sequence $\{a_n\}_{n\geq h}$ keeps the same nice properties. One says it is a *strong v-ordering*: analogously to the sequence of integers in the case of $\mathbb{Z}$, a polynomial is integer-valued on V if and only if it is so on $n+1$ consecutive terms of this sequence.

Globalization. Back to number fields, as $\mathrm{Int}(O_K)_{\mathfrak{m}} = (\mathrm{Int}(\mathcal{O}_K))_{\mathfrak{m}}$ for each maximal ideal $\mathfrak{m}$, the characteristic ideals $\mathfrak{I}_n(\mathcal{O}_K)$ are such that $(\mathfrak{I}_n(\mathcal{O}_K))_{\mathfrak{m}} = \mathfrak{I}_n((\mathcal{O}_K)_{\mathfrak{m}})$. As in the case of a subset of $\mathbb{Z}$, we define the nth *factorial ideal* of $\mathcal{O}_K$ as the inverse of the fractional ideal $\mathfrak{I}_n(\mathcal{O}_K)$. We thus have

$$n!_{\mathcal{O}_K} = \prod_{\mathfrak{m}\in \mathrm{Max}(\mathcal{O}_K)} \mathfrak{m}^{w_{N(\mathfrak{m})}(n)} \quad \text{where} \quad w_q(n) = \sum_{k\geq 1}\left[\frac{n}{q^k}\right]. \tag{15}$$

The factorial ideal $n!_{\mathcal{O}_K}$ is principal if and only if its inverse $\mathfrak{I}_n(\mathcal{O}_K)$ is principal. By Proposition 19 we have the following.

Proposition 31. *Let $\mathcal{O}_K$ be the ring of integers of a number field. Then* $\mathrm{Int}(\mathcal{O}_K)$ *admits a regular basis if and only if, for each n, $n!_{\mathcal{O}_K}$ is a principal ideal of $\mathcal{O}_K$.*

One could be more greedy and ask for a Newton sequence, equivalently a sequence that would be simultaneously a $v_{\mathfrak{m}}$-ordering for each maximal ideal $\mathfrak{m}$. But that may be asking too much.

Conjecture. $\mathbb{Q}$ is the only number field for which there is a Newton sequence.

Wood [**55**, Thm. 5.2] proved the conjecture holds for imaginary quadratic number fields, Adam and Cahen [**3**] that it fails for at most finitely many real quadratic fields.

Remark 7. Newton sequences are related to the *Schinzel problem* [**45**, Problem 8]: is there a sequence in $\mathcal{O}_K$ such that, for every ideal $\mathcal{I}$ with norm $N = \mathrm{Card}(\mathcal{O}_K/\mathcal{I})$, the first N terms of the sequence form a set of representatives modulo $\mathcal{I}$? So is the sequence of nonnegative integers in $\mathbb{Z}$. As for Newton sequences, the answer is conjectured to be negative for every number field but $\mathbb{Q}$. At least one could build finite sequences $\{a_n\}_{n=0}^{N}$ with this property for the ideals with norm up to N. Similarly, one could build finite sequences to be used as test sets for integer-valued polynomials of degree up to N. See [**3**] for a computation of the maximal length of such sequences in quadratic number fields (for both the Schinzel and Newton problem).

Pólya groups and Pólya fields. Following Zantema [**57**], a number field K is called a *Pólya field* if $\mathrm{Int}(\mathcal{O}_K)$ admits a regular basis. This is certainly the case if $\mathcal{O}_K$ is a principal ideal domain, as is in particular the ring $\mathbb{Z}[i]$ of Gaussian integers, yet this is asking too much.

Recall that the *class group* of K is the quotient $\mathcal{C}l(\mathcal{O}_K) = \mathcal{I}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K)$ of the group $\mathcal{I}(\mathcal{O}_K)$ of nonzero fractional ideals of $\mathcal{O}_K$ by the subgroup $\mathcal{P}(\mathcal{O}_K)$ of nonzero

principal ideals. As a measure of the obstruction for $\mathrm{Int}(\mathcal{O}_K)$ to have a regular basis, the *Pólya group* $\mathcal{P}o(\mathcal{O}_K)$ is the subgroup of the class group generated by the classes of the factorial ideals: K is a Pólya field if and only if the Pólya group is trivial.

As $n!_{\mathcal{O}_K} = \prod_{\mathfrak{m}\in \mathrm{Max}(\mathcal{O}_K)} \mathfrak{m}^{w_{N(\mathfrak{m})}(n)}$, the Pólya group is also generated by the classes of the products $\Pi_q(\mathcal{O}_K) = \prod_{\mathfrak{m}\in Max(\mathcal{O}_K),\, N(\mathfrak{m})=q} \mathfrak{m}$ (where q is such there is some maximal ideal with norm q) [**16**, Prop. II.3.9]. For a Galoisian extension of $\mathbb{Q}$, as noticed by Ostrowski [**47**], the ideal Π_q is principal unless q is a power of a ramified prime. Consequently we have the following.

Proposition 32. *If $K/\mathbb{Q}$ is Galoisian, the Pólya group $\mathcal{P}o(\mathcal{O}_K)$ is generated by the classes of the ideals $\Pi_q(\mathcal{O}_K)$ where q is a power of a ramified prime.*

Happily, there are finitely many ramified primes. For quadratic fields, the Pólya group is also the group of ambiguous classes of Hilbert [**16**, Proposition II.4.4]. The quadratic Pólya fields were characterized by Zantema [**57**]. They are all the quadratic fields with only one ramified prime and also, in the real case, the fields with 2 ramified primes under another condition.

Proposition 33. *The quadratic Pólya fields are:*
- in the imaginary case: $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, and $\mathbb{Q}(\sqrt{-p})$ with p prime $\equiv 3 \pmod 4$,
- in the real case: $\mathbb{Q}(\sqrt{p})$ with p prime, and if the norm of the fundamental unit is 1, also $\mathbb{Q}(\sqrt{pq})$ with p and q prime.

Example 34. $K = \mathbb{Q}(\sqrt{-23})$ is a Pólya field. Indeed, 23 is the only ramified prime and $\Pi_{23}(\mathcal{O}_K)$ is the principal ideal $\sqrt{-23}\,\mathcal{O}_K$. Yet K has class number 4 [**37**, Tables].

In the same paper, Zantema proved also that all *cyclotomic fields* (that is, fields generated by roots of unity) are Pólya fields. More recently, a systematic study of the Galoisian Pólya fields of degree ≤ 6 was undertaken by Leriche [**39**].

The classical embedding problem asks if every number field is contained in a number field whose ring of integers is a principal ideal domain. The answer is negative. A similar but weaker question asks to embed every number field in a Pólya field. A positive answer was recently obtained: every number field K is contained in its Hilbert class field L (that is, its maximal nonramified Abelian extension) and L was shown to be a Pólya field [**40**, Thm. 3.3].

A twin of $\mathbb{Z}$ in characteristic p. The strongest similarities with $\mathbb{Z}$ are to be found in the ring $\mathbb{F}_q[T]$ of polynomials with coefficients in a finite field, rather than in the ring of integers of a number field, although $\mathbb{F}_q[T]$ has a positive characteristic p. Indeed it admits a (strong) Newton sequence, often referred to as the *Car sequence* [**17**].

Similarly to what we did in (13) to build a v-ordering, let $a_0 = 0, a_1, \ldots, a_{q-1}$ be the elements of $\mathbb{F}_q$ and $n = n_0 + n_1 q + \cdots + n_r q^r$ be the base q extension of n. Then set

$$a_n = a_{n_0} + a_{n_1} T + \cdots + a_{n_r} T^r.$$

It is not difficult to see that for each degree n polynomial $f \in \mathbb{F}_q[T]$, the first q^n terms of this sequence form a set of representatives modulo f. In fact, the same is true of q^n consecutive terms. This is a strong answer to the Schinzel problem, as in [Remark 7], and one can derive that $\{a_n\}_{n\geq 0}$ is a strong Newton sequence. The generalized binomials $\binom{X}{a_n} = \prod_{k=0}^{n-1} \frac{X-a_k}{a_n-a_k}$ thus form a regular basis of $\mathrm{Int}(\mathbb{F}_q[T])$ and a

degree n polynomial is integer-valued on $\mathbb{F}_q[T]$ if and only if it is so on $n+1$ consecutive terms of this sequence!

Having a Newton sequence, the factorial $n!_{\mathbb{F}_q[T]}$ is the product $\prod_{k=0}^{n-1}(a_n - a_k)$ and this turns out to be (up to an invertible element) the factorial introduced by Carlitz back in 1940! [**18**].

As for number fields (finite extensions of $\mathbb{Q}$), one may ask if a finite extension K of $\mathbb{F}_q(T)$, that is, a *function field*, can be such that its ring of integers, denoted by $\mathcal{O}_K$, admits a Newton sequence. Unlike number fields, that can obviously be the case: if $K = \mathbb{F}_q(\sqrt{T})$, then $\mathcal{O}_K = \mathbb{F}_q[\sqrt{T}]$ is clearly isomorphic to $\mathbb{F}_q[T]$; the same can be said for $K = \mathbb{F}_{q^2}(T)$, with $\mathcal{O}_K = \mathbb{F}_{q^2}[T]$. Yet it is conjectured that for a separable finite extension, $\mathcal{O}_K$ never admits a Newton sequence, unless it is isomorphic to some $\mathbb{F}_{q^n}[T]$. This was proved by Adam for a totally imaginary extension [**2**, Theorem 18].

Finally let us mention that Adam [**1**] also obtained an analogue of Pólya's 1915 theorem [Theorem 8] for entire functions in the case of $\mathbb{F}_q(T)$.

7. MORE AND MORE RINGS. We focused our review on the classical ring $\mathrm{Int}(\mathbb{Z})$ of integer-valued polynomials over $\mathbb{Z}$, then over subsets of $\mathbb{Z}$, and then over the ring of integers of a number field (or more generally a Dedekind domain with finite residue fields). But of course, there is more.

Subsets. As encountered occasionally above, one can consider the ring $\mathrm{Int}(E, D)$ of integer-valued polynomials over a subset E of a domain D, other than $\mathbb{Z}$. For instance, if D is a Dedekind domain with finite residue fields, $\mathrm{Int}(E, D)$ is a Prüfer domain, being an overring of $\mathrm{Int}(D)$, and has thus many interesting properties.

Derivatives. $f = \binom{X}{2}$ is integer-valued, $f' = X - \frac{1}{2}$ is not. The study of integer-valued polynomials whose derivatives are integer-valued dates back to the 1950s [**53**]. More generally one can investigate the rings $\mathrm{Int}^{(k)}(D)$ of polynomials which are integer-valued on a domain D, together with their derivatives up to order k, allowing k to be infinite. For instance $f = \frac{X^2(X-1)^2}{2}$ belongs to $\mathrm{Int}^{(\infty)}(\mathbb{Z})$ as $f' \in \mathbb{Z}[X]$. And of course one can generalize again to subsets!

Finite differences. Given a polynomial $f \in \mathbb{Z}[X]$, one can define, for each $h \in \mathbb{Z}$, the finite difference $\Delta_h f = \frac{f(X+h)-f(X)}{h}$. And then finite differences of order 2 by $\Delta_l \Delta_h f$, and so on. The study of the ring $\mathrm{Int}^{[k]}(\mathbb{Z})$ of polynomials which are integer-valued together with their finite differences up to order k, allowing k to be infinite, is also quite ancient. A regular basis of $\mathrm{Int}^{[k]}(\mathbb{Z})$ was determined by Carlitz in 1959 [**19**], of the form $c_n^{[k]}\binom{X}{n}$, with coefficients $c_n^{[k]}$ in $\mathbb{Z}$. For instance

$$c_n^{[1]} = \mathrm{lcm}\{j \mid 1 \le j \le n\} \text{ and } c_n^{[\infty]} = \prod_{p \in \mathbb{P}} p^{[\frac{n}{p}]}.$$

Of course one can more generally consider $\mathrm{Int}^{[k]}(D)$, for any domain D. But finite differences do not really agree with subsets (even in the case of a subset E of $\mathbb{Z}$: $a, h \in E$ does not imply $a + h \in E$).

Divided differences. The *divided difference* of a polynomial $f \in K[X]$ (given some field K) is a polynomial in two indeterminates: $\Phi(f)(X, Y) = \frac{f(X)-f(Y)}{X-Y}$. One can iterate this procedure. In fact, divided differences (with $K = \mathbb{R}$) date back to Cauchy (who attributes them to Ampere) [**20**]. If f is a polynomial of degree n, its divided difference of order k is a symmetric polynomial of degree $n - k$ in $k + 1$ indeterminates:

$$\Phi^k f(X_0, \ldots, X_k) = \sum_{0 \le i \le k} \frac{f(X_i)}{\prod_{j \neq i}(X_i - X_j)}.$$

There is also the following analogue of Taylor's formula:

$$f(X) = f(a) + (X - a)\,\Phi^1 f(a, a) + \cdots + (X - a)^n\,\Phi^n f(a, a, \ldots, a). \qquad (16)$$

One can study the ring $\mathrm{Int}^{\{k\}}(D)$ of polynomials that are integer-valued on a domain D together with their divided differences up to order k. No need here to allow k to be infinite, as $\mathrm{Int}^{\{\infty\}}(D) = D[X]$ by (16). But one can perfectly well consider subsets!

As for finite differences, there are regular bases of $\mathrm{Int}^{\{k\}}(\mathbb{Z})$ of the form $c_n\binom{X}{n}$. Bhargava obtained such bases in 2009 [**9**], using another notion of p-orderings called *k-removed p-orderings*. He also generalized Mahler's approximation theorem: these bases are orthonormal bases of the Banach space $\mathcal{C}^k(\mathbb{Z}_p, \mathbb{Q}_p)$ of functions whose derivatives up to the order k are "uniformly continuously differentiable" [**9**]. In fact, even for a subset E of $\mathbb{Z}$ such that the completion $\widehat{E}$ of E is compact, every basis of $\mathrm{Int}^{\{k\}}(E, \mathbb{Z})$ is an orthonormal basis of $\mathcal{C}^k(\widehat{E}, \mathbb{Q}_p)$. Explicit formulas were recently given [**26**] for such bases in case $\widehat{E}$ is a regular subset [Example 23.2].

Interplay. In general, one has the containments

$$\mathrm{Int}^{\{k\}}(D) \subseteq \mathrm{Int}^{[k]}(D) \subseteq \mathrm{Int}^{(k)}(D).$$

Moreover, $\mathrm{Int}^{\{1\}}(D) = \mathrm{Int}^{[1]}(D)$. For k finite, these containments are usually strict. For instance, the set of prime ideals above some prime number p is uncountable in the case of $\mathrm{Int}^{(k)}(\mathbb{Z})$ but finite for $\mathrm{Int}^{[k]}(\mathbb{Z})$. Moreover, there is no regular bases of the form $c_n\binom{X}{n}$ for $\mathrm{Int}^{(k)}(\mathbb{Z})$ (see [**14**] for the description of a basis of $\mathrm{Int}^{(1)}(\mathbb{Z})$). Yet

$$\mathrm{Int}^{(\infty)}(\mathbb{Z}) = \mathrm{Int}^{[\infty]}(\mathbb{Z}) \ \ [\mathbf{53}].$$

One can ask when $\mathrm{Int}^{(\infty)}(D) = \mathrm{Int}^{[\infty]}(D)$ (not true for the ring of Gaussian integers!). A full answer is given in the case of Dedekind domains in [**21**, 15].

More, more, and more! There are many other generalizations: for instance, integer-valued polynomials on matrices! Let us just give one recent example [**29**]: if $T_n(\mathbb{Z})$ denotes the ring of $n \times n$ triangular integer matrices, the ring of integer-valued polynomials on $T_n(\mathbb{Z})$, that is, $\mathrm{Int}(T_n(\mathbb{Z})) = \{f \in \mathbb{Q}[X] \mid f(T_n(\mathbb{Z})) \subseteq T_n(\mathbb{Z})\}$ is nothing else than $\mathrm{Int}^{\{n-1\}}(\mathbb{Z})$. But one must draw the line somewhere!

REFERENCES

1. D. Adam, Car–Pólya and Gel'fond's theorems for $\mathbb{F}_q[T]$, *Acta Arith.* **115** (2004) 287–303.
2. ———, Pólya and Newtonian function fields, *Manuscripta Math.* **126** (2008) 231–246.
3. D. Adam, P.-J. Cahen, Newtonian and Schinzel quadratic fields, *J. Pure Appl. Algebra* **215** (2011) 1902–1918.
4. D. Adam, J.-L. Chabert, Y. Fares, Subsets of $\mathbb{Z}$ with simultaneous orderings, *Integers* **10** (2010) 435–451.
5. Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964) 117–180.
6. M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.* **490** (1997) 101–127.
7. ———, Generalized factorials and fixed divisors over subsets of a Dedekind domain, *J. Number Theory* **72** (1998) 67–75.
8. ———, The factorial function and generalizations, *Amer. Math. Monthly* **107** (2000) 783–799.

9. ———, On P-orderings, rings of integer-valued polynomials, and ultrametric analysis, *J. Amer. Math. Soc.* **22** (2009) 963–993.
10. M. Bhargava, P.-J. Cahen, J. Yeramian, Finite generation properties for rings of integer-valued polynomials, *J. Algebra* **322** (2009) 1129–1150.
11. M. Bhargava, K. S. Kedlaya, Continuous functions on compact subsets of local fields, *Acta Arith.* **91** (1999) 191–198.
12. J. Boulanger, J.-L. Chabert, Asymptotic behavior of characteristic sequences of integer-valued polynomials, *J. Number Theory* **80** (2000) 238–259.
13. D. Brizolis, Ideals in rings of integer-valued polynomials, *J. Reine Angew. Math.* **285** (1976) 28–52.
14. D. Brizolis, E. G. Straus, A basis for the ring of doubly integer-valued polynomials, *J. Reine Angew. Math.* **286/287** (1976) 187–195.
15. P.-J. Cahen, J.-L. Chabert, Elasticity for integral-valued polynomials, *J. Pure Appl. Algebra* **103** (1995) 303–311.
16. ———, *Integer-Valued Polynomials*. Amer. Math. Soc. Surveys and Monographs, Vol. 48, Providence, 1997, http://dx.doi.org/10.1090/surv/048.
17. M. Car, Répartition modulo 1 dans un corps de série formelle sur un corps fini, *Acta Arith.* **69** (1995) 229–242.
18. L. Carlitz, A set of polynomials, *Duke Math. J.* **6** (1940) 486–504.
19. ———, A note on integral-valued polynomials, *Indag. Math. (N.S.)* **62** (1959) 294–299.
20. A.-L. Cauchy, Sur les fonctions interpolaires, *C.R. Acad. Sci. Paris* **11** (1840) 775–789.
21. J.-L. Chabert, Dérivées et différences divisées à valeurs entières, *Acta Arith.* **63** (1993) 143–156.
22. ———, Une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers, *Canad. Math. Bull.* **39** (1996) 402–407.
23. ———, Integer-valued polynomials on prime numbers and logarithm power expansion, *European J. Combin.* **28** (2007) 754–761.
24. J.-L. Chabert, P.-J. Cahen, Old problems and new questions around integer-valued polynomials and factorial sequences, in *Multiplicative Ideal Theory in Commutative Algebra*. Ed. J. W. Brewer, S. Glaz, W. Heinzer, B. Olberding. Springer, New York, 2006. 89–108, http://dx.doi.org/10.1007/978-0-387-36717-0.
25. J.-L. Chabert, S. Chapman, W. Smith, A basis for the ring of polynomials integer-valued on prime numbers, in *Factorization in Integral Domains*. Ed. D. D. Anderson. Lecture Notes in Pure and Appl. Math., Vol. 189, Dekker, New York, 1997. 271–284.
26. J.-L. Chabert, S. Evrard, Y. Fares, Regular subsets of valued fields and Bhargava's v-orderings, *Math. Z.* **274** (2013) 263–290.
27. J. Dieudonné, Sur les fonctions continues p-adiques, *Bull. Sci. Math.* **68** (1944) 79–95.
28. S. Evrard, Y. Fares, p-adic subsets whose factorials satisfy a generalized Legendre formula, *Bull. London Math. Soc.* **40** (2008) 37–50.
29. S. Evrard, Y. Fares, K. Johnson, Integer-valued polynomials on lower triangular integer matrices, *Monatsh. Math.* **170** (2013) 147–160.
30. S. Frisch, Interpolation by integer-valued polynomials, *J. Algebra* **211** (1999) 562–577.
31. ———, Integer-valued polynomials on algebras, *J. Algebra* **373** (2013) 414–425.
32. R. Gilmer, Sets that determine integer-valued polynomials, *J. Number Theory* **33** (1989) 95–100.
33. R. Gilmer, W. Smith, Finitely generated ideals of the ring of integer-valued polynomials, *J. Algebra* **81** (1983) 150–164.
34. K. Johnson, The invariant subalgebra and anti-invariant submodule of $K_*K_{(p)}$, *J. K-Theory* **2** (2008) 123–145.
35. I. Kaplansky, *Commutative Rings*. Univ. Chicago Press, Chicago, 1974.
36. A. J. Kempner, Polynomials and their residue systems, *Trans. Amer. Math. Soc.* **22** (1921) 240–288.
37. H. Koch, *Algebraic Number Theory*. Springer, New York, 1997, http://dx.doi.org/10.1007/978-3-642-58095-6.
38. A. M. Legendre, *Essai sur la Théorie des Nombres*. Second edition. Courcier, Paris, 1808, http://gallica.bnf.fr/ark:/12148/bpt6k62826k.
39. A. Leriche, Cubic, quartic and sextic Pólya fields, *J. Number Theory* **133** (2013) 59–71.
40. A. Leriche, About the embedding of a number field in a Pólya field, *J. Number Theory* **145** (2014) 210–229.
41. K. Mahler, An interpolation series for continuous functions of a p-adic variable, *J. Reine Angew. Math.* **199** (1958) 23–34 and **208** (1961) 70–72.
42. A. Mingarelli, Abstract factorials of arbitrary sets of integers (2007), http://arxiv.org/abs/0705.4299.
43. H. Minkowski, Zur theorie der quadratischen Formen, *J. Reine Angew. Math.* **101** (1897) 196–202.
44. M. Nagata, *Local Rings*. Interscience, New York, 1962.
45. W. Narkiewicz, Some unsolved problems, *Mem. Soc. Math. France* **25** (1971) 159–164.

46. ———, *Polynomial Mappings*. Lecture notes, Vol. 400, Springer, New York, 1995, http://dx.doi.org/10.1007/BFb0076894.
47. A. Ostrowski, Über ganzwertige polynome in algebraischen Zahlkörpern, *J. Reine Angew. Math.* **149** (1919) 117–124.
48. G. Pólya, Ueber ganzwertige ganze funktionen, *Rend. Circ. Matem. Palermo* **40** (1915) 1–16.
49. ———, Über ganzwertige polynome in algebraischen Zahlkörpern, *J. Reine Angew. Math.* **149** (1919) 97–116.
50. W.H. Schikhof, *Ultrametric Calculus, An Introduction to p-adic Analysis*. Cambridge Univ. Press, Cambridge, 1984, http://dx.doi.org/10.1017/CBO9780511623844.
51. I. Schur, Über eine Klasse von endlichen Gruppen linearer substitutionen, *Sitzungsber. Preuss. Akad. Wiss.* (1905) 77–91.
52. Th. Skolem, Ein Satz über ganzwertige polynome, *Det Kongelige Norske Videnskabers Selskab* **9** (1936) 111–113.
53. E. G. Straus, On the polynomials whose derivatives have integral values at integers, *Proc. Amer. Math. Soc.* **2** (1951) 24–27.
54. R. J. Valenza, Elasticity of factorizations in number fields, *J. Number Theory* **36** (1990) 212–218.
55. M. Wood, P-orderings: A metric viewpoint and the non-existence of simultaneous orderings, *J. Number Theory* **99** (2003) 36–56.
56. J. Yeramian, Anneaux de Bhargava, *Comm. Algebra* **32** (2004) 3043–3069.
57. H. Zantema, Integer valued polynomials over a number field, *Manuscripta Math.* **40** (1982) 155–203.

PAUL-JEAN CAHEN received his Ph.D. in 1973 at the University Paris XI-Orsay with Pierre Samuel as adviser. He is currently retired.
12 Traverse du lavoir de grand mère, 13100 Aix-en-Provence, France.
pauljean.cahen@gmail.com

JEAN-LUC CHABERT received his Ph.D. in 1973 at the University Paris XI-Orsay with Pierre Samuel as adviser. He is currently professor emeritus of the University of Picardie.
LAMFA, UMR-CNRS 7352, University of Picardie, 80039 Amiens, France.
jean-luc.chabert@u-picardie.fr