ON P-ORDERINGS, RINGS OF INTEGER-VALUED POLYNOMIALS, AND ULTRAMETRIC ANALYSIS

MANJUL BHARGAVA

CONTENTS

1. INTRODUCTION

In this article, we introduce two new variations of a game called "P-ordering" [4], which we term an *r-removed P-ordering* and a *P-ordering of order h*, respectively. Given any subset S of a Dedekind domain D and a prime ideal P of D, the game involves the construction of a special sequence in S having certain surprising combinatorial properties. In particular, these two notions of P-ordering result in a three-parameter generalization of the usual factorial function $n!$, which we denote $n!_{S,h}^{\{r\}}$; here S, h, and r denote the three parameters, where S is any subset of D, r is a nonnegative integer, and $h \in \mathbb{R} \cup \infty$. The usual factorial function is obtained by setting $S = D = \mathbb{Z}$, $r = 0$, and $h = \infty$.

These generalizations of the factorial function share a number of fundamental properties with the usual factorial function. For example:

Theorem 1. *For any nonnegative integers k and ℓ, we have that $k!_{S,h}^{\{r\}} \ell!_{S,h}^{\{r\}}$ divides $(k + \ell)!_{S,h}^{\{r\}}$.*

Thus the generalized "binomial coefficient" $\binom{k+\ell}{k}_{S,h}^{\{r\}} = (k+\ell)!_{S,h}^{\{r\}}/(k!_{S,h}^{\{r\}}\ell!_{S,h}^{\{r\}})$ is integral for all k and ℓ, analogous to the usual binomial coefficients.

We use these notions of P-ordering and generalized factorials to solve two classical number-theoretic problems in two areas that have traditionally been treated separately in the literature.

The first area concerns the subject of "integer-valued polynomials". The subject goes back to 1915, when Pólya [23] showed that any rational polynomial in one variable mapping the integers to the integers can be uniquely expressed in the form

$$f(x) = \sum_{n=0}^{d} c_n \binom{x}{n},$$

where d is the degree of f and the c_n are integers. In the language of polynomial ring theory, the polynomials $\binom{x}{n}$ are said to form a *regular basis* (i.e., a basis consisting of one polynomial of each degree) for the ring $\mathrm{Int}(\mathbb{Z}, \mathbb{Z})$ of integer-valued polynomials over the rational numbers. This result was extended to polynomials over quadratic number fields (mapping the algebraic integers to themselves) by Pólya [24], and to general number fields by Ostrowski [22].

More generally, given an arbitrary subset S of a Dedekind domain D with quotient field K, the set of polynomials in $K[x]$ that are D-valued ("integer-valued") on S forms a ring, denoted $\mathrm{Int}(S, D)$. Subsequent to Pólya and Ostrowski's work in the case $S = D$, great interest arose in this area not only because of its inherent beauty but also because rings of the form $\mathrm{Int}(S, D)$ "have many remarkable properties, and are a source of examples and counterexamples in commutative algebra" ([21, p. v]). Thus, following Pólya's work, a number of authors examined $\mathrm{Int}(S, D)$ in cases other than $S = D = \mathbb{Z}$ and gave Pólya-style decompositions of $\mathrm{Int}(S, D)$ when $S = D$ or more generally when S is an ideal of D (see, e.g., [22], [16], [17]). A D-module description of $\mathrm{Int}(S, D)$ for general S and D was given in [4] using P-orderings.

A number of different variants of $\mathrm{Int}(S, D)$ have also been considered in the past, and they too have been shown to possess very interesting algebraic properties (see, e.g., [9]). In this article, we consider two such subrings that arise very naturally, and which are of additional interest due to their beautiful connections with p-adic interpolation (described later in this introduction). These two rings are:

(a) the ring $\mathrm{Int}^{\{r\}}(S, D)$ of polynomials $f \in K[x]$ whose first $r+1$ divided differences[1] $\Phi^0 f = f$, $\Phi^1 f$, ..., $\Phi^r f$ are all D-valued on S; and

(b) the ring $\mathrm{Int}_{\mathcal{M}}(S, D)$ of *D-valued polynomials on S of modulus $\mathcal{M}$*, i.e., polynomials $f \in K[x]$ such that $f(mx + a) \in D[x]$ for all $m \in \mathcal{M}$ and $a \in S$; here $\mathcal{M}$ is an ideal of D.

Note that setting $r = 0$ in item (a), or $\mathcal{M} = (0)$ in item (b), recovers the ring $\mathrm{Int}(S, D)$. These two classes of rings have not been considered systematically previously. However, for rings of polynomials with integer-valued differences on S, special cases of these rings (particularly when $r = 1$ and $S = D$) have been studied

---

[1]Recall that the k-th divided difference $\Phi^k f$ of a polynomial $f \in K[x]$ is defined inductively by $\Phi^0 f(x_0) = f(x_0)$ and

$$\Phi^k f(x_0, \ldots, x_k) = \frac{\Phi^{k-1} f(x_0, \ldots, x_{k-1}) - \Phi^{k-1} f(x_0, \ldots, x_{k-2}, x_k)}{x_{k-1} - x_k}.$$

heavily by a number of authors, beginning with the classical works of de Bruijn [13] and Carlitz [12] in the 1950s. Rings of type (b), when $S = D$, were studied in the recent Ph.D. thesis of Yeramian [32]. As we will explain below, both of these types of rings also arise naturally in the context of non-Archimedean analysis.

The question arises as to whether an explicit Pólya-type basis can be given for these more general rings of polynomials. In Section 3, for both types of rings (a) and (b), we give such explicit D-basis decompositions of Pólya type, using the notions of r-removed P-ordering and P-ordering of order h, respectively. The proof, in particular, involves the construction of certain "generalized binomial polynomials", which extend the usual binomial polynomials $\binom{x}{n}$ used by Pólya. Our results thus unify and generalize the results of Pólya and also the results of [4], [8], [13], [16], [17], and [22], and they yield a unified statement (and a more compact proof) of all these results simultaneously in terms of the general P-ordering construct.

The second area we treat concerns the subject of non-Archimedean analysis. Given a subset S of a discrete valuation domain R with quotient field K and maximal ideal P, one is frequently interested in functions from S to K that are continuous in the P-adic topology. A classical and very useful theorem of Mahler [20] states that any continuous function f from the p-adic ring $\mathbb{Z}_p$ to its quotient field $\mathbb{Q}_p$ can be uniquely expressed in the form

$$f(x) = \sum_{n=0}^{\infty} c_n \binom{x}{n},$$

where $c_n \to 0$ p-adically as $n \to \infty$. In the language of "p-adic Banach spaces" (see Section 4), the theorem may be strengthened to state that the binomial polynomials $\binom{x}{n}$ $(n \geq 0)$ form an orthonormal base for the $\mathbb{Q}_p$-Banach space of continuous functions from $\mathbb{Z}_p$ to $\mathbb{Q}_p$, equipped with the supremum norm. Like Pólya's theorem, Mahler's theorem has shown its face in numerous contexts in number theory. Various generalizations of Mahler's theorem have since appeared in the literature, allowing cases where $R \neq \mathbb{Z}_p$ or $S \neq R$ (see, e.g., [1], [27], [28]). An explicit construction of polynomial orthonormal bases for continuous functions from S to K for general compact subsets S of K was given in [7] using P-orderings.

Of course, in P-adic analysis, one frequently requires functions satisfying conditions of smoothness that are stronger than simple continuity. Perhaps the most important examples of such smoothness conditions on P-adic functions are (a) *continuous differentiability*, where functions are not only required to be continuous but also possess continuous derivatives up to a given order, and (b) *local analyticity*, where functions are required to have power series expansions in balls of a given radius. It is known that each space $\mathcal{B}$ of functions from S to K, defined by one of these smoothness conditions, comes naturally equipped with a norm (stronger than the supremum norm) which turns $\mathcal{B}$ into a K-Banach space.

It is thus natural to ask whether Mahler-style expansions exist in these more general settings, i.e., whether analogous constructions of orthonormal bases exist for Banach spaces $\mathcal{B}$ of functions satisfying any of these more stringent conditions of differentiability or analyticity. Such theorems have been achieved in the past for certain very special S, R, and degrees of continuous differentiability or local analyticity (see, e.g., Schikhof [25] or Amice [1]); however, a description in the general case has never previously been given.

In Section 4, for arbitrary compact sets S of K, and for both types of smoothness conditions (a) and (b), we give a unified method for constructing Mahler-style expansions for functions from S to K satisfying such smoothness conditions. Our method thus unifies and generalizes not only Mahler's result but also the constructions in [1], [7], [25], [27], and [28], and it yields a unified statement and also a relatively short proof of these results. The key ingredients in our constructions for each of these two types of smoothness are again the r-removed P-ordering and the P-ordering of order h, respectively. Moreover, we note that our proofs of these Mahler-style basis theorems for such functions are *effective* (unlike many of the previously proved special cases), in that they yield complete information on rates of convergence purely in terms of the combinatorial properties of S.

An important by-product of our results is that, for any $\epsilon > 0$, the functions in any of these K-Banach spaces of functions can be ϵ-approximated by polynomials with respect to their respective Banach norms. (Since the norm in each of these K-Banach spaces is stronger than simply the supremum norm, polynomial approximation in these spaces is a stronger notion than that of "uniform approximation.") In the case of continuous functions with the supremum norm, this is a well-known result of Weierstrass [30] in the Archimedean case and Dieudonné [14] and Kaplansky [18] in the non-Archimedean context. For continuously differentiable functions in the Archimedean setting, the analogous result (with appropriate norm) was proven in the important works of de la Vallée Poussin [26] and Bernstein [3], and various generalizations have since appeared (see, e.g., [19] for a survey). In this article, we obtain significantly stronger versions of these approximation theorems in the non-Archimedean setting by exhibiting explicit polynomial Schauder bases for each of these K-Banach spaces of functions (with effective rates of convergence).

Historically, the construction of orthonormal bases for locally analytic functions of order h was first studied in the classic 1964 work of Amice [1], who examined the special case of certain "well-distributed" sets $S \subset K$. Our work here thus extends Amice's theory to a very general setting and also yields a significantly simpler and shorter treatment.

In the case of r-times continuously differentiable functions on compact sets S, our work here also recovers the special case $r = 0$ and $S = \mathbb{Z}_p$ as in Mahler's theorem, the case $r = 0$ and general S as treated in [7], and the case $r \geq 1$ and $S = \mathbb{Z}_p$ treated in Schikhof [25]. In this paper, we give an effective treatment for arbitrary r and arbitrary S. We note that our work also naturally allows one to construct explicit orthonormal bases for Banach spaces of functions on compact sets S that satisfy desired degrees of *both* continuous differentiability and local analyticity.

One other work that must be mentioned in the context of this subject is that of Barsky [2]. In that work, Barsky had already noticed a close connection between integer-valued polynomials and a certain class of p-adic functions which were termed "k-Lipshitzian". The case $k = 1$ corresponds to (1-times) continuously differentiable functions; for $k > 1$, however, the notion of "k-Lipshitzian" diverges from that of continuous differentiability. We will not consider the class of k-Lipshitzian functions here for the simple reason that the notion of k-Lipshitzian does not appear to generalize well to functions on general compact sets S, which is our primary focus.

This paper is organized as follows. In Section 2, we consider generalizations of a game called "P-ordering" that will play a crucial role in the constructions that

follow. In Section 3 we then construct certain subrings of rings of integer-valued polynomials that naturally relate to the study of smooth *P*-adic functions. We prove versions of Pólya's regular basis theorem for each of these subrings, using the generalized notions of *P*-ordering as introduced in Section 2. In Section 4, we apply these regular basis techniques to the study of K-Banach spaces of continuously differentiable or locally analytic functions on general compact subsets S of a local field K. Finally, in Section 5, we end with a discussion of some generalizations of these results that may be of interest in future work.

2. A game called *P*-orderings

To set up the game, let $S \subset \mathbb{Z}$ be any infinite subset and fix any prime number p. Let v_p denote the p-adic valuation on $\mathbb{Z}$. There may be any number of players in this game, but each player does the following. Each player constructs what is called a *p-ordering of S*, which is a sequence $a_0, a_1, \ldots$ in S formed inductively as follows:

- Choose $a_0 \in S$ arbitrary.
- For $k \geq 1$, choose $a_k \in S$ so as to minimize $v_p((a_k - a_0) \cdots (a_k - a_{k-1}))$.

There may frequently be ties when selecting the value of a_k, and hence one has to make a choice at every such step. Nevertheless, once such a p-ordering of S is constructed, one obtains an associated *p-sequence* $\{\nu_k(S,p)\}_{k=0}^{\infty}$ *of* S, defined by

$$\nu_k(S,p) = p^{v_p((a_k - a_0) \cdots (a_k - a_{k-1}))},$$

consisting of the powers of p minimized at each step.

We declare that a player wins if say after 100 steps, he has the smaller $\nu_{100}(S,p)$. What is the optimal strategy? The surprising and perhaps not-immediately-obvious answer is that the strategy is irrelevant, and the game is always a tie! That is, we have the following theorem:

Theorem 2 ([4]). *The associated p-sequence $\{\nu_k(S,p)\}$ is independent of the choice of p-ordering.*

Thus the p-sequence $\{\nu_k(S,p)\}$ is an invariant of the set S, and we may speak of it without reference to any p-ordering.

In the case $S = \mathbb{Z}$, these invariants are in fact related to a well-known sequence, namely the factorial function. We have the formula

$$k! = \prod_p \nu_k(\mathbb{Z}, p).$$

In [4] and [5], we thus defined a "generalized factorial function" $k!_S$, given by

$$k!_S = \prod_p \nu_k(S, p),$$

associated to any subset S of $\mathbb{Z}$. The sequence $\{k!_S\}_{k=0}^{\infty}$ of generalized factorials encodes and compresses all the invariants $\nu_k(S,p)$ into one sequence; it also occurs and is useful in a number of applications ([4], [5]), including those to be considered in this article.

More generally, let S be any infinite subset of a Dedekind domain D, and let P in D be a prime ideal. Then we may define a P-ordering of S in the analogous

way, obtaining invariants $\nu_k(S, P)$, which are now ideals of D, and a sequence of generalized factorials

$$
(1) \qquad k!_S = \prod_P \nu_k(S, P),
$$

which are also then ideals of D.

If $P = (\pi)$ is principal, we may speak of P-orderings also as "π-orderings" and view the invariants $\nu_k(S, \pi)$ of S as powers of π.

2.1. **On r-removed P-orderings.** We noted that the game of the previous section was always a tie. Let us now change the rules slightly.

Let S again be any infinite subset of a Dedekind domain D, and let $P \subset D$ be a prime. For any integer $r \geq 0$, we define an *r-removed P-ordering of S* to be a sequence $a_0, a_1, \ldots$ in S in which the first $r + 1$ elements $a_0, \ldots, a_r$ are chosen arbitrarily, and then the a_n for $n > r$ are successively chosen to minimize the value of

$$
(2) \qquad \sum_{i \in A_n} v_P(a_n - a_i),
$$

where the sum is over any set A_n of $n - r$ elements in $\{0, \ldots, n-1\}$ that minimizes (2). Thus there is a minimization both over elements $a_n \in S$ and subsets $A_n \subset \{0, \ldots, n-1\}$ of cardinality $n - r$. We write $A_n = \{0, \ldots, n-1\} \setminus \{n_1, \ldots, n_r\}$ for the chosen value of A_n yielding this desired minimum, where $n_1, \ldots, n_r$ denote the indices that have been "removed".

Again, there are choices to be made, for both a_n and A_n, at each step of the r-removed p-ordering process. However, once an r-removed P-ordering is constructed in this way, we then obtain what we call the associated *r-removed P-sequence* $\{\nu_k^{\{r\}}(S, P)\}$ of S, defined by

$$
(3) \qquad \nu_k^{\{r\}}(S, P) = P^{\sum_{i \in A_k} v_P(a_k - a_i)}.
$$

Note that a 0-removed P-ordering (resp. P-sequence) coincides with the usual notion of P-ordering (resp. P-sequence).

What now is the strategy in choosing the sequence $a_0, a_1, \ldots$ to minimize the valuation of $\nu_k^{\{r\}}(S, P)$ as k becomes large? It turns out as before that the strategy does not matter; we have again the following independence theorem:

Theorem 3. *The associated r-removed P-sequence of S is independent of the choice of r-removed P-ordering.*

Thus for each value of r, the r-removed P-sequence of S yields yet another sequence of invariants of the set S. We may encode these invariants into a single sequence $\{k!_S^{\{r\}}\}$, called the *r-removed factorial function*, defined by

$$
k!_S^{\{r\}} = \prod_P \nu_k^{\{r\}}(S, P).
$$

The usual factorial sequence of S is of course the special case $r = 0$. We postpone the proof of Theorem 3 to Section 3.1.1.

2.2. **On P-orderings of order h.** Let us now change the rules of the game in yet another way. As before, let S be any infinite subset of a Dedekind domain D, and let P be a prime of D. Fix any integer $h \geq 0$. This time, we ask each player to construct a *P-ordering of S of order h*, which is a sequence $a_0, a_1, \ldots$ in S in which a_0 is chosen arbitrarily, and then the a_n are successively chosen to minimize the value of the sum

$$(4) \qquad \sum_{i=0}^{n-1} \min(h, v_P(a_n - a_i)).$$

(That is, we essentially "cap off" all valuations of differences of elements $a_n - a_i$ at h, thus helping the players to keep the values of the sum (4) small.)

Given such a P-ordering of order h, one obtains an associated *P-sequence of order h*, denoted $\{\nu_k(S, P, h)\}$ and defined by

$$(5) \qquad \nu_k(S, P, h) = P^{\sum_{i=0}^{k-1} \min(h, v_P(a_k - a_i))}.$$

Note that a P-ordering (resp. P-sequence) of order ∞ coincides with the usual notion of P-ordering (resp. P-sequence).

Given h, what is the strategy for the players in choosing the sequence $a_0, a_1, \ldots$ to keep the P-adic valuations of $\nu_k(S, P, h)$ to a minimum as k becomes large? It turns out again that the game is always a tie. We have the following independence theorem:

Theorem 4. *The associated P-sequence of S of order h is independent of the choice of P-ordering of order h.*

Thus for every h, the P-sequence of S of order h gives yet another sequence of invariants of the set S. Note that the ordinary P-sequence $\{\nu_k(S, P)\}$ of S is simply $\{\nu_k(S, P, \infty)\}$. We postpone the proof of Theorem 4 to Section 3.2.2.

Now suppose that $\mathcal{M}$ is any ideal of D, with prime factorization $\mathcal{M} = P_1^{h_1} \cdots P_r^{h_r}$. We define the *$k$th factorial ideal of S of modulus $\mathcal{M}$* by

$$(6) \qquad \nu_k(S; \mathcal{M}) = \prod_{i=1}^{r} \nu_k(S, P_i, h_i);$$

the usual factorial $k!_S$, defined by (1), may be considered as the special case $\mathcal{M} = (0)$. Factorials of modulus $\mathcal{M}$ will play an important role in Sections 3.2 and 4.2.

Remark 5. Theorems 3 and 4 in fact admit a common generalization; see Theorem 30.

The generalized factorial functions we have described in this section will turn out to be critical in the study of integer-valued polynomials on S, and in the study of P-adically smooth functions on S. We turn first to the subject of integer-valued polynomials.

3. Rings of integer-valued polynomials

In this section, we introduce and study two new rings of integer-valued polynomials, namely 1) the ring $\mathrm{Int}^{\{r\}}(S, D)$ of integer-valued polynomials on S whose divided differences of order up to r are also integer-valued on S, and 2) the ring $\mathrm{Int}_{\mathcal{M}}(S, D)$ of integer-valued polynomials on S of modulus $\mathcal{M}$. These rings of polynomials arise in a very natural way and also play a central role in the study of smooth p-adic functions (see Section 4).

3.1. **Polynomials with integer-valued divided differences.** As we have already seen in Pólya's theorem (and its generalizations), a rational polynomial that takes integer values on the integers (or on any infinite subset S of $\mathbb{Z}$) need not be an integral polynomial itself. One key property that an integer polynomial f possesses, which an integer-valued polynomial does not necessarily share, is that of *congruence preservation*, i.e., $f(x) \equiv f(y) \pmod{m}$ whenever $x \equiv y \pmod{m}$. In other words, the *first divided difference*

$$(7) \qquad \Phi f(x, y) = \frac{f(x) - f(y)}{x - y}$$

of f is also an integral polynomial (now in two variables); in particular, it too takes only integer values. This gives a criterion on the *values* taken by a polynomial that can be used to distinguish integral polynomials from integer-valued polynomials.

This still does not distinguish the two types of polynomials entirely, of course. However, more generally, if f is an integral polynomial, then so is its *n-th divided difference* $\Phi^n f(x_0, \ldots, x_n)$, defined inductively by the equation

$$(8) \qquad \Phi^n f(x_0, \ldots, x_n) = \frac{\Phi^{n-1} f(x_0, \ldots, x_{n-1}) - \Phi^{n-1} f(x_0, \ldots, x_{n-2}, x_n)}{x_{n-1} - x_n}.$$

It is easy to see that a polynomial is integral if and only if it *and* all its n-th divided differences take integer values on S, where S is any infinite subset of $\mathbb{Z}$. This follows, e.g., from the Newton interpolation formula

$$
\begin{aligned}
f(x) \;=\; & f(a_0) + \Phi f(a_0, a_1)(x - a_0) + \Phi^2 f(a_0, a_1, a_2)(x - a_0)(x - a_1) + \cdots \\
& + \Phi^{d-1} f(a_0, \ldots, a_{d-1})(x - a_0) \cdots (x - a_{d-2}) \\
& + \Phi^d f(a_0, \ldots, a_{d-1}, x)(x - a_0) \cdots (x - a_{d-1}),
\end{aligned}
$$

where $a_0, \ldots, a_{d-1} \in S$ are any integers, and d denotes the degree of f. (By convention, the 0-th divided difference $\Phi^0 f$ of f is f itself; it is known that $\Phi^n f$ is a function symmetric in its $n + 1$ arguments.)

Thus a rational polynomial that is integer-valued on S can be distinguished from an integral polynomial by computing its k-th divided differences for sufficiently many values of k. Given any integer $r \geq 0$, the set of integer-valued polynomials on S whose k-th divided differences are also integer-valued for all $k \leq r$ forms a ring, which we denote by $\mathrm{Int}^{\{r\}}(S, \mathbb{Z})$. That $\mathrm{Int}^{\{r\}}(S, \mathbb{Z})$ is indeed a ring follows from the product identity

$$\Phi^k (fg)(x_0, \ldots, x_k) = \sum_{i=0}^{k} \Phi^i f(x_0, \ldots, x_i) \Phi^{k-i} g(x_i, \ldots, x_k).$$

In particular, the case $r = 0$ recovers the usual ring $\mathrm{Int}(S, \mathbb{Z})$ of integer-valued polynomials on S. Also, we have seen already that $\bigcap_{r=0}^{\infty} \mathrm{Int}^{\{r\}}(S, \mathbb{Z}) = \mathbb{Z}[x]$.

The ring $\mathrm{Int}^{\{r\}}(S, \mathbb{Z})$ consists precisely of those polynomials that cannot be distinguished from integral polynomials even after the computation of all divided differences on S up to the r-th divided differences. More generally, we have the following:

Definition 6. Let S be any subset of a Dedekind domain D having quotient field K. Then the set of all polynomials in $K[x]$ whose k-th divided differences for $k = 0, \ldots, r$ are all D-valued on S forms a ring, which we denote by $\mathrm{Int}^{\{r\}}(S, D)$.

In Sections 3.1.1–3.1.2, we derive a regular basis theorem for these special rings $\mathrm{Int}^{\{r\}}(S, \mathbb{Z})$ of integer-valued polynomials. More generally, for a Dedekind domain D, we give necessary and sufficient conditions on S, D, and r for $\mathrm{Int}^{\{r\}}(S, D)$ to have a regular basis, and we give a construction of such a basis whenever it exists. (The significantly simpler special case $r = 0$ was treated in [4].)

3.1.1. *Local basis for* $\mathrm{Int}^{\{r\}}(S, D)$. We begin by constructing an explicit regular basis for $\mathrm{Int}^{\{r\}}(S, D)$ in the case where $D = R$ is local. Thus let K denote a local field with discrete valuation, let R be its valuation ring, and let π be a uniformizer. Let $v(x)$ denote the π-valuation of x, normalized so that $v(\pi) = 1$.

Given any compact subset S of K and an r-removed π-ordering $\Lambda = \{a_i\}$ of S, define the *r-removed factorial function* $n!_\Lambda^{\{r\}}$ of S by

$$n!_\Lambda^{\{r\}} = \prod_{i \in A_n} (a_n - a_i)$$

(i.e., $n!_\Lambda^{\{r\}}$ generates the ideal $\nu_k^{\{r\}}(S, \pi)$) and define the *n-th r-removed generalized binomial polynomial* by

(9)
$$\binom{x}{n}_\Lambda^{\{r\}} = \frac{(x - a_0)(x - a_1) \cdots (x - a_{n-1})}{n!_\Lambda^{\{r\}}}.$$

We claim that these r-removed binomial polynomials lie in $\mathrm{Int}^{\{r\}}(S, R)$, and moreover, they form a regular basis for the ring $\mathrm{Int}^{\{r\}}(S, R)$. We state this in the following theorem.

Theorem 7. *Let $r \geq 0$ be any integer, and let $\Lambda = \{a_i\}_{i=0}^\infty$ be an r-removed π-ordering of S. Then the r-removed binomial polynomials $\{\binom{x}{n}_\Lambda^{\{r\}}\}_{n \geq 0}$ form an R-basis for the ring $\mathrm{Int}^{\{r\}}(S, R)$.*

Proof. First, let us check that the r-removed binomial polynomials actually lie in $\mathrm{Int}^{\{r\}}(S, R)$. To achieve this, we prove the following key formula for the divided differences of $\binom{x}{n}_\Lambda^{\{r\}}$; this formula will also be of use in the sequel.

Lemma 8. *Fix any elements $a_0, \ldots, a_{n-1}$ and $b_0, \ldots, b_q$ in R. For each vector $\boldsymbol{i} = (i_1, \ldots, i_q)$ satsfying $0 \leq i_1 < \cdots < i_q < n$, we define the sequence $m_{\boldsymbol{i}}(0)$, $m_{\boldsymbol{i}}(1), \ldots, m_{\boldsymbol{i}}(n - 1)$ inductively by choosing $m_{\boldsymbol{i}}(k)$ to be the smallest index in $\{0, \ldots, q\} \setminus \{m_{\boldsymbol{i}}(i_j) : i_j < k\}$ that maximizes $v(b_{m_{\boldsymbol{i}}(k)} - a_k)$. Then for $f(x) = (x - a_0) \cdots (x - a_{n-1})$, we have the formula*

(10)
$$\Phi^q f(b_0, \ldots, b_q) = \sum_{\substack{\boldsymbol{i} = (i_1, \ldots, i_q) \\ 0 \leq i_1 < \cdots < i_q < n}} \prod_{k \in \{0, \ldots, n-1\} \setminus \{i_1, \ldots, i_q\}} (b_{m_{\boldsymbol{i}}(k)} - a_k).$$

Proof. We proceed via induction on $q + n = q + \deg(f)$. In the case of $q + n = 0$ (indeed for $q = 0$ and any n), the formula simply states that $f = f$, since the only vector $\boldsymbol{i}$ in the sum in this case is the empty vector. Now set $f_0(x) = f(x)/(x - a_0)$; then we have the following identity (itself easily proven by induction on q):

(11) $\Phi^q f(b_0, \ldots, b_q) = (b_{m_{\boldsymbol{i}}(0)} - a_0)\Phi^q f_0(b_0, \ldots, b_q) + \Phi^{q-1} f(b_0, \ldots, \widehat{b_{m_{\boldsymbol{i}}(0)}}, \ldots, b_q),$

where $\widehat{b_{m_{\boldsymbol{i}}(0)}}$ denotes an omitted term. Now the induction hypothesis gives the first term of (11) as the $i_1 \neq 0$ part of the sum in (10), while the second term of (11) gives the $i_1 = 0$ part of the sum in (10). The lemma follows.   □

To prove that $\binom{x}{n}_\Lambda^{\{r\}} \in \mathrm{Int}^{\{r\}}(S, R)$, we apply the lemma with $a_0, a_1, \ldots, a_{n-1}$ as in the r-removed π-ordering Λ, and $b_0, \ldots, b_q$ arbitrary elements of S, where $q \le r$. With $f(x)$ as in the lemma, we have formula (10) for $\Phi^q f(b_0, \ldots, b_q)$. For a vector $\boldsymbol{i} = (i_1, \ldots, i_q)$, let $m_{\boldsymbol{i}}(0), \ldots, m_{\boldsymbol{i}}(n-1)$ be the sequence as constructed in the lemma, and furthermore let $m_{\boldsymbol{i}}(n)$ be the unique element of $\{0, \ldots, q\} \setminus \{i_1, \ldots, i_q\}$. Then, by the construction of $m_{\boldsymbol{i}}(k)$, we know that $v(b_{m_{\boldsymbol{i}}(k)} - a_k) \ge v(b_{m_{\boldsymbol{i}}(n)} - a_k)$. Thus for any given $i = (i_1, \ldots, i_q)$, we have

(12)

$$
\begin{aligned}
v\Big(\prod_{k \in \{0, \ldots, n-1\} \setminus \{i_1, \ldots, i_q\}} (b_{m_{\boldsymbol{i}}(k)} - a_k) \Big) \;&\ge\; v\Big(\prod_{k \in \{0, \ldots, n-1\} \setminus \{i_1, \ldots, i_q\}} (b_{m_{\boldsymbol{i}}(n)} - a_k) \Big) \\[2mm]
&\ge\; v\Big(\prod_{k \in \{0, \ldots, n-1\} \setminus \{n_1, \ldots, n_r\}} (a_n - a_k) \Big) \\[2mm]
&=\; v(n!_\Lambda^{\{r\}}),
\end{aligned}
$$

since $\Lambda = \{a_i\}$ is an r-removed π-ordering. Thus for any $q \le r$ and $b_0, \ldots, b_q \in S$, formula (10) gives an expression for $\Phi^q(b_0, \ldots, b_q)$ as a sum of terms, where each term is an R-multiple of $n!_\Lambda^{\{r\}}$. Thus $\binom{x}{n}_\Lambda^{\{r\}} \in \mathrm{Int}^{\{r\}}(S, R)$, as desired.

To see that these polynomials actually form an R-basis for $\mathrm{Int}^{\{r\}}(S, R)$, let $f \in \mathrm{Int}^{\{r\}}(S, R)$ denote any element of degree d, and write

$$
f(x) = \sum_{j=0}^{d} c_j \binom{x}{j}_\Lambda^{\{r\}}
$$

for some elements $c_j \in K$. We wish to show that the c_j actually lie in R. Suppose not, and let n be the minimal index such that $c_n \notin R$. We consider the value of $\Phi^r f(a_{n_1}, \ldots, a_{n_r}, a_n)$, where $n_1, \ldots, n_r$ denote as usual the r indices removed at the n-th step of the r-removed π-ordering process. Then it is easy to see that $\Phi^r[c_j \binom{x}{j}_\Lambda^{\{r\}}](a_{n_1}, \ldots, a_{n_r}, a_n)$ vanishes for $j > n$, while for $j < n$ it is in R by the minimality of n and the fact that the binomial polynomials are in $\mathrm{Int}^{\{r\}}(S, R)$. We conclude that $\Phi^r[c_n \binom{x}{n}_\Lambda^{\{r\}}](a_{n_1}, \ldots, a_{n_r}, a_n) = c_n$ must also be in R, a contradiction. It follows that all c_n must lie in R, and thus the polynomials $\binom{x}{n}_\Lambda^{\{r\}}$ indeed form an R-basis for $\mathrm{Int}^{\{r\}}(S, R)$, as was desired. $\qquad\square$

Remark 9. The arguments above in fact show that the generalized factorials $\{k!_S^{\{r\}}\}$ must occur as the denominators of the leading coefficients of any regular basis of $\mathrm{Int}^{\{r\}}(S, R)$. Moreover, for any sequence $\{a_i\}$ in S, the polynomials

$$
\frac{(x - a_0)(x - a_1) \cdots (x - a_{k-1})}{k!_\Lambda^{\{r\}}}, \quad k = 0, 1, 2, \ldots,
$$

give a regular basis of $\mathrm{Int}_{\pi^h}^{\{r\}}(S, R)$ *if and only if* $\{a_i\}$ is an r-removed π-ordering of S.

As a consequence we note that Theorem 7 implies, in particular, that the fractional ideal consisting of 0 and all the leading coefficients of degree k polynomials in $\mathrm{Int}^{\{r\}}(S, R)$ is simply $(k!_S^{\{r\}})^{-1}$. Since the definition of the ring $\mathrm{Int}^{\{r\}}(S, R)$ does not depend on any choice of π-ordering, Theorem 3 follows.

3.1.2. *Global basis for* $\text{Int}^{\{r\}}(S, D)$. Now suppose that D is any Dedekind domain having quotient field K. Standard localization arguments (see, e.g., [23], [22], and [4]) then show that the fractional ideal of all leading coefficients of degree k polynomials in $\text{Int}^{\{r\}}(S, D)$ is $(k!_S^{\{r\}})^{-1}$.

If the ideal $(k!_S^{\{r\}})^{-1}$ is not principal, then the ring $\text{Int}^{\{r\}}(S, D)$ clearly cannot have a regular basis. Otherwise, one may construct a regular basis using r-removed P-orderings, as follows. For each prime ideal P of D, let $\{a_i^{(P)}\}$ be an r-removed P-ordering of S. For each $n \geq 0$, construct (using the Chinese Remainder Theorem) a sequence $\{a_{i,n}\}_{i=0}^{n-1}$ in D such that for every prime P dividing $n!_S^{\{r\}}$, we have $a_{i,n} \equiv a_i^{(P)} \pmod{P^{e+1}}$, where $P^e \,\|\, n!_S^{\{r\}}$. Then we have the following analogue of Pólya and Ostrowski's regular basis theorems in the context of $\text{Int}^{\{r\}}(S, D)$:

Theorem 10. *The ring* $\text{Int}^{\{r\}}(S, D)$ *has a regular basis if and only if* $k!_S^{\{r\}}$ *is a nonzero principal ideal for all* $k \geq 0$. *In that case, a regular basis for* $\text{Int}^{\{r\}}(S, D)$ *is given by*

$$B_k(x) = \frac{(x - a_{0,k})(x - a_{1,k}) \cdots (x - a_{k-1,k})}{\beta_k}, \quad k = 0, 1, 2, \ldots ,$$

where β_k *denotes an element of* D *such that* $(\beta_k) = k!_S^{\{r\}}$.

Proof. We need only check that the values of $B_k(x)$ and of its first r divided differences on S all lie in D. For this, it suffices to check that all these values lie in the localization D_P for each prime P. But this is implied by Theorem 7 and the fact that the $a_{i,n}$ were chosen sufficiently close P-adically to an r-removed P-ordering $\{a_i^{(P)}\}$ of S. The result follows. □

3.2. **Integer-valued polynomials having a given modulus.**

3.2.1. *The modulus of an integer-valued polynomial.* Let $f(x)$ be an integer-valued polynomial on $\mathbb{Z}$, i.e., a polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(a) \in \mathbb{Z}$ for all $a \in \mathbb{Z}$. Then, as we demonstrate below, there exist infinitely many $m \geq 0$ such that $f(mx + a) \in \mathbb{Z}[x]$ for all $a \in \mathbb{Z}$ (equivalently, for all $a \in \{0, 1, \ldots, m-1\}$). That is, although f itself might not be an integral polynomial, there exist infinitely many m such that f is integral when considered as a polynomial on each of the residue classes modulo m. For any such value of m, we say that f is (integer-valued) *of modulus* m.

If an integer-valued polynomial is of modulus m, then it is clearly also of modulus km for any $k \geq 0$; in particular, any integer-valued polynomial is of modulus 0. To see that any integer-valued polynomial is of modulus m for some $m > 0$, we may apply Pólya's regular basis theorem, which states that any integer-valued polynomial on $\mathbb{Z}$ can be expressed as a $\mathbb{Z}$-linear combination of the polynomials $\binom{x}{n}$, $n = 0, 1, \ldots$. As it is easy to see that $\binom{x}{n}$ is of modulus $m = \text{lcm}(1, 2, \ldots, n)$ but is not of modulus m for any smaller positive m, it follows that any degree n polynomial taking integer values on $\mathbb{Z}$ is necessarily of modulus $\text{lcm}(1, 2, \ldots, n)$, but might not be of any smaller positive modulus.

The set of all integer-valued polynomials on $\mathbb{Z}$ forms a ring, which is generally denoted by $\text{Int}(\mathbb{Z})$. The set of all integer-valued polynomials of a given fixed modulus m is seen to form a subring of $\text{Int}(\mathbb{Z})$, which we denote by $\text{Int}_m(\mathbb{Z})$. In particular, $\text{Int}_0(\mathbb{Z}) = \text{Int}(\mathbb{Z})$.

In the following two subsections, we derive a regular basis theorem for $\mathrm{Int}_m(\mathbb{Z})$ analogous to Pólya's regular basis theorem for $\mathrm{Int}(\mathbb{Z})$. In fact, we consider the following more general situation. Let D be a Dedekind domain and let $S \subseteq D$ be any subset. As is customary, denote by $\mathrm{Int}(S, D)$ the ring of D-valued polynomials on S.

Definition 11. For any ideal $\mathcal{M}$ of D, we say that a polynomial f is *D-valued on S of modulus $\mathcal{M}$* if for all $m \in \mathcal{M}$ and $a \in S$, $f(mx + a) \in D[x]$. We denote the ring of all D-valued polynomials on S of modulus $\mathcal{M}$ by $\mathrm{Int}_{\mathcal{M}}(S, D)$.

Again, $\mathrm{Int}_{(0)}(S, D) = \mathrm{Int}(S, D)$. In Section 3.2.3, we give necessary and sufficient conditions on S, D, and $\mathcal{M}$ for $\mathrm{Int}_{\mathcal{M}}(S, D)$ to have a regular basis (i.e., a D-basis consisting of one element of each degree), and we give a construction of such a basis whenever it exists. The (much simpler) special case $\mathcal{M} = (0)$ was treated in [4].

3.2.2. *Local basis for* $\mathrm{Int}_{\mathcal{M}}(S, D)$. We first turn to the problem of constructing a regular basis for $\mathrm{Int}_{\mathcal{M}}(S, D)$ when $D = R$ is local, i.e., when it is a discrete valuation domain. Thus, in this subsection, let K denote a local field with discrete valuation, let R be its valuation ring, and let π be a uniformizer. Denote by $v(x)$ the π-valuation of $x \in K$, normalized so that $v(\pi) = 1$.

Given any compact subset S of K and a π-ordering $\Lambda = \{a_i\}$ of S of order h, define the factorial function $n!_{S,h}$ by

$$n!_{S,h} = \pi^{\sum_{i=0}^{n-1} \min(h, v(a_n - a_i))}$$

(i.e., $n!_{S,h}$ generates $\nu_k(S, \pi, h)$) and define the *n-th generalized binomial polynomial of order h* by

$$(13) \qquad \binom{x}{n}_{\Lambda,h} = \frac{(x - a_0)(x - a_1) \cdots (x - a_{n-1})}{n!_{S,h}}.$$

Then $\binom{x}{n}_{\Lambda,h} \in \mathrm{Int}_{\pi^h}(S, R)$, as the π-valuation of $\binom{\pi^h X + a}{n}_{\Lambda,h}$ is

$$\sum_{i=0}^{n-1} \min(h, v(a - a_i)) - \sum_{i=0}^{n-1} \min(h, v(a_n - a_i)),$$

which is nonnegative for $a \in S$ since $\{a_i\}$ is a π-ordering of S of order h.

It turns out that these generalized binomial polynomials of order h actually form an R-basis for the space $\mathrm{Int}_{\pi^h}(S, R)$ (see [32], [1] for a nice discussion of the special case $S = R$):

Theorem 12. *Let $\{a_i\}_{i=0}^{\infty}$ be a π-ordering of S of order h. Then the polynomials $\{\binom{x}{n}_{\Lambda,h}\}_{n \geq 0}$ form a regular basis for the ring $\mathrm{Int}_{\pi^h}(S, R)$.*

It is most convenient to prove Theorem 12 first for a special class of π-orderings. We say that a π-ordering $\Lambda = \{a_i\}$ of order h is *restricted* if for any m and n, $a_m \equiv a_n \pmod{\pi^h}$ implies $a_m = a_n$. We note that any π-ordering of order h can be transformed into a restricted π-ordering of order h by replacing each a_n $(n \geq 0)$ by a_m, where $m \geq 0$ is the smallest integer such that $a_m \equiv a_n \pmod{\pi^h}$; thus restricted π-orderings of order h exist.

Proof of Theorem 12 for restricted Λ. We have already seen that the polynomials $\binom{x}{n}_{\Lambda,h}$ lie in $\mathrm{Int}_{\pi^h}(S, R)$ for all $k \geq 0$. Conversely, any polynomial $f \in \mathrm{Int}_{\pi^h}(S, R)$

having degree d may be expressed in the form

$$\text{(14)} \qquad f(x) = \sum_{n=0}^{d} c_n \binom{x}{n}_{\Lambda,h},$$

where the coefficients c_n lie in K; we claim that the c_n must lie in R. For if not, let m be the minimal index such that $c_m \notin R$ and let k equal the number of times a_m occurs in the multiset $\{a_0, a_1, \ldots, a_{m-1}\}$.

We now set $x = \pi^h X + a_m$ in (14) to obtain

$$\text{(15)} \qquad f(\pi^h X + a_m) = \sum_{n=0}^{d} c_n P_{m,n}(X),$$

where

$$\text{(16)} \qquad P_{m,n}(X) = \binom{\pi^h X + a_m}{n}_{\Lambda,h},$$

and we examine the coefficient of X^k in (15). Since $f \in \mathrm{Int}_{\pi^h}(S, R)$, the coefficient of X^k in (15) must be integral. Now the coefficient of X^k in $P_{m,n}(X)$ is zero for $n > m$, since $P_{m,n}(X)$ is actually a multiple of X^{k+1} by the definition of k. Furthermore, the coefficient of X^k in $c_n P_{m,n}(X)$ for $n < m$ must be integral by the minimality of m and the fact that $\binom{x}{n}_{\Lambda,h} \in \mathrm{Int}_{\pi^h}(S, R)$. It follows that the coefficient of X^k in $c_m P_{m,m}(X)$ must also be integral. However, we may write

$$\text{(17)} \qquad P_{m,m}(X) = \prod_{i=0}^{m-1} \left(\frac{\pi^h X + a_m - a_i}{\pi^{\min(h, v(a_m - a_i))}} \right),$$

where each of the factors on the right-hand side is clearly integral and of π-valuation zero. It follows from this factorization and the definition of k that the π-valuation of the coefficient of X^k in $P_{m,m}(X)$ is zero, and hence we must have $c_m \in R$, a contradiction. $\qquad\square$

We may now prove Theorem 12 for general π-orderings Λ of order h using a simple change-of-basis argument.

Proof of Theorem 12 *for general* Λ. Denote by Λ_0 any restricted π-ordering of order h. Then we have already shown that $\{\binom{x}{n}_{\Lambda_0,h}\}_{n \geq 0}$ forms an R-basis for $\mathrm{Int}_{\pi^h}(S, R)$. Since the polynomials $\binom{x}{n}_{\Lambda,h}$ also lie in $\mathrm{Int}_{\pi^h}(S, R)$, there exists a transformation $T = (t_{mn})$ defined over R such that

$$\binom{x}{m}_{\Lambda,h} = \sum_{n=0}^{m} t_{mn} \binom{x}{n}_{\Lambda_0,h}$$

for all $m, n \geq 0$. We wish to show that t_{mn} is invertible over R. However, T is lower triangular, and $t_{nn} = 1$ for all n since the leading coefficients of $\binom{x}{n}_{\Lambda,h}$ and $\binom{x}{n}_{\Lambda_0,h}$ are identical. The invertibility of T follows. $\qquad\square$

Remark 13. The arguments in fact show that the generalized factorials $\{k!_{S,h}\}$ must occur as the denominators of the leading coefficients of any regular basis of $\mathrm{Int}_{\pi^h}(S, R)$; moreover, for any sequence $\{a_i\}$ in S, the polynomials

$$\frac{(x - a_0)(x - a_1) \cdots (x - a_{k-1})}{k!_{S,h}}, \quad k = 0, 1, 2, \ldots,$$

give a regular basis of $\mathrm{Int}_{\pi^h}(S,R)$ *if and only if* $\{a_i\}$ *is a* π-*ordering of* S *of order* h.

As a consequence, we note that Theorem 12 implies that the fractional ideal consisting of 0 and all the leading coefficients of degree k polynomials in $\mathrm{Int}_{\pi^h}(S,R)$ is simply $\nu_k(S,\pi,h)^{-1}$. Since the definition of the ring $\mathrm{Int}_{\pi^h}(S,R)$ does not depend on any choice of π-ordering, Theorem 4 also follows.

3.2.3. *Global basis for* $\mathrm{Int}_{\mathcal{M}}(S,D)$. Next, suppose D is a general Dedekind domain with quotient field K. The identical arguments via localization show that the fractional ideal of leading coefficients of degree k polynomials in $\mathrm{Int}_{\mathcal{M}}(S,D)$ must be $\nu_k(S;\mathcal{M})^{-1}$.

If the ideal $\nu_k(S;\mathcal{M})^{-1}$ is not principal, then evidently the ring $\mathrm{Int}_{\mathcal{M}}(S,D)$ will not have a regular basis. Otherwise, a construction analogous to that in Section 3.1.2 yields a regular basis also in this case. Namely, let $\{a_i\}$ be any sequence in D that, for every nonzero prime power P^h appearing in the prime factorization of $\mathcal{M}$, is termwise congruent modulo P^h to some P-ordering of S of order h. Such a sequence may be constructed using the Chinese Remainder Theorem. Then we have the following analogue of Pólya and Ostrowski's regular basis theorems in the context of $\mathrm{Int}_{\mathcal{M}}(S,D)$:

Theorem 14. *The ring* $\mathrm{Int}_{\mathcal{M}}(S,D)$ *has a regular basis if and only if* $\nu_k(S;\mathcal{M})$ *is a nonzero principal ideal for all* $k \geq 0$. *In that case, a regular basis of* $\mathrm{Int}_{\mathcal{M}}(S,D)$ *is given by*

$$B_k(x) = \frac{(x-a_0)(x-a_1)\cdots(x-a_{k-1})}{\beta_k}, \quad k = 0,1,2,\dots ,$$

where β_k *denotes an element of* D *such that* $(\beta_k) = \nu_k(S;\mathcal{M})$.

The proof of Theorem 14 is analogous to that of Theorem 10.

4. Smooth functions on compact subsets of local fields

In this section, we investigate two fundamental notions of smoothness for functions on compact subsets of local fields, namely, continuous differentiability and local analyticity.

Let K be a local field, i.e., the quotient field of a complete discrete valuation ring R whose residue ring $R/\pi R$ is finite. As usual, one equips K with the non-Archimedean absolute value $|x| = |R/\pi R|^{-v(x)}$, where $v(x)$ denotes the valuation of x normalized so that $v(\pi) = 1$. This absolute value satisfies the ultrametric triangle inequality $|x+y| \leq \max(|x|,|y|)$, and induces a metric topology (the "π-adic" topology) on K.

A *K-Banach space* is a complete normed K-linear space $\mathcal{B}$ whose norm $\|\cdot\|$ also satisfies the ultrametric triangle inequality $\|v+w\| \leq \max(\|v\|,\|w\|)$. For example, let S be any compact subset of K. Then the space $C(S,K)$ of continuous functions from S to K, equipped with the supremum norm $\|f\|_\infty = \sup_{x \in S}\{|f(x)|\}$, is a K-Banach space. There are many linear subspaces of $C(S,K)$ which are of interest as K-Banach spaces in their own right—for instance, spaces of functions satisfying various conditions of analyticity. We consider some of these spaces in Sections 4.1 and 4.2.

As shown in [25], much of the theory of K-Banach spaces parallels that of Hilbert spaces. For example, there is the notion of *orthogonality* of two elements x,y in a

K-Banach space $\mathcal{B}$: we write $x \perp y$ if $\|x\| \leq \|x - \lambda y\|$ for all $\lambda \in K$. It is easy to see that the orthogonality relation $\perp$ is in fact symmetric. More generally, we say that a set $\{x_1, x_2, \ldots\} \subset \mathcal{B}$ is *orthogonal* if each element x_i is orthogonal to every element in the K-linear span of the other x_j's ($j \neq i$). In addition, if each x_i satisfies $\|x_i\| = 1$, then we say that $\{x_1, x_2, \ldots\}$ is an *orthonormal* set.

As with separable Hilbert spaces, for separable K-Banach spaces (i.e., those having countable dense subsets) there is the notion of an *orthonormal base*. A set $\{e_0, e_1, \ldots\}$ is an orthonormal base of a K-Banach space $\mathcal{B}$ if it is an orthonormal set in $\mathcal{B}$ and every element $x \in \mathcal{B}$ can be expressed as a convergent sum $x = \sum c_n e_n$ for some sequence of elements $c_n \in K$. It is not hard to see that the latter definition of orthonormal base is equivalent to the following (for further information, see [25] or [15]):

Definition 15. A sequence of elements $e_0, e_1, \ldots$ in a K-Banach space $\mathcal{B}$ is said to be an *orthonormal base* of $\mathcal{B}$ if
(i) any $v \in \mathcal{B}$ has a unique representation as a convergent sum $v = \sum_{n=0}^{\infty} c_n e_n$, where $c_n \in K$ and $c_n \to 0$;
(ii) $\|v\| = \sup_{n \geq 0}\{|c_n|\}$.

For example, Mahler's theorem [20] implies that the sequence of polynomials $\binom{x}{n}$ forms an orthonormal base of the $\mathbb{Q}_p$-Banach space $C(\mathbb{Z}_p, \mathbb{Q}_p)$. Indeed, Mahler's theorem immediately gives property (i) of Definition 15, while property (ii) can in fact be deduced from Pólya's theorem as follows. Because of property (i), it suffices to check (ii) on finite linear combinations $v = f(x) = \sum_{n=0}^{N} c_n \binom{x}{n}$. In that case, (ii) amounts to the statement that the *fixed divisor* $d(f)$ of f, i.e., the greatest common divisor of the values taken by $f(x)$ on $\mathbb{Z}_p$, is equal to $\gcd_{n \geq 0}\{c_n\}$ (viewed as a power of p). Clearly $d(f)$ is a multiple of $\gcd\{c_n\}$, since each polynomial $\binom{x}{n}$ is $\mathbb{Z}_p$-valued on $\mathbb{Z}_p$. Now suppose $d(f)$ is not equal to $\gcd\{c_n\}$. Then $f(x)/d(f)$ is a $\mathbb{Z}_p$-valued polynomial on $\mathbb{Z}_p$, but in its expansion as

$$\frac{f(x)}{d(f)} = \sum_{n=0}^{N} \frac{c_n}{d(f)} \binom{x}{n}$$

we see that not all the coefficients $\frac{c_n}{d(f)}$ are integers in $\mathbb{Z}_p$, contradicting Pólya's regular basis theorem for $\mathbb{Z}_p$, i.e., that the polynomials $\binom{x}{n}$ form a $\mathbb{Z}_p$-basis for the $\mathbb{Z}_p$-valued polynomials on $\mathbb{Z}_p$. We conclude that $d(f) = \gcd_{n \geq 0}\{c_n\}$, yielding property (ii).

It is thus property (ii) that relates orthonormal bases of K-Banach spaces with integer-valued polynomials. In this section, we wish to further study and make use of this relationship.

Analogous polynomial orthonormal bases also exist for the $\mathbb{Q}_p$-Banach spaces $C(S, K)$, where S is any compact subset of a local field K; these bases were constructed in [4] and [7] using P-orderings and by examining the corresponding rings $\text{Int}(S, \mathbb{Z}_p)$ of integer-valued polynomials.

In Section 4.1.1, we completely resolve the case of r-*times continuously differentiable functions* on an arbitrary compact subset S of a local field K. In particular, we construct explicit polynomial orthonormal bases for the K-Banach space $C^r(S, K)$ of such functions, using the notion of r-removed P-orderings. This is accomplished by exploiting connections with the ring $\text{Int}^{\{r\}}(S, R)$ of polynomials having integer-valued k-th divided differences for all $0 \leq k \leq r$. In Section 4.1.2, we show that any

regular polynomial orthonormal base of $C^r(S, K)$ must in fact come from a regular basis for the ring $\text{Int}^{\{r\}}(S, R)$.

We then turn to the case of "locally analytic functions". In [1], Amice constructed polynomial orthornormal bases for the K-Banach space $LA_h(S, K)$ of *locally analytic functions of order h on S* (to be defined in the next section) in the case where S is "well-distributed" in K in a certain sense. Using P-orderings of order h, we show in Section 4.2.1 that natural polynomial orthonormal bases for locally analytic functions of order h on S can in fact be constructed for *any* compact subset S of K. The connection with integer-valued polynomials of modulus π^h, as studied in Section 3.2, is again one of the main keys to the construction and its proof. In Section 4.2.2, we show in fact that *any* regular polynomial orthonormal base of $LA_h(S, K)$ must be a regular basis for the ring $\text{Int}_{\pi^h}(S, R)$.

4.1. The Banach space of r-times continuously differentiable functions.
In this subsection, we consider continuously differentiable functions on arbitrary compact subsets of local fields. The formulation of a notion of continuous differentiability in the non-Archimedean setting turns out to be a bit more subtle than in the Archimedean case if it is to have "desirable" properties. For example, if we define a C^1 (continuously differentiable) function simply as one having a continuous derivative then, contrary to the Archimedean case, local invertibility of the function does not necessarily hold even at a point having a nonzero derivative. In fact, there exist differentiable functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$ such that $f'(x) = 1$ for all $x \in \mathbb{Z}_p$ even though f is not injective in any neighborhood of 0 (see [25, Example 26.6])!

To regain some of these desirable properties—such as local invertibility—for continuously differentiable functions, it becomes necessary to strengthen the definition of such functions. The most common method for accomplishing this is through the notion of divided differences.

Let $S \subset K$ again be a compact set without isolated points. We say that a function $f : S \to K$ is *continuously differentiable*[2] if its divided difference function $\Phi f : S \times S \setminus \Delta \to K$ (as defined by (7)) is extendable to a continuous function on all of $S \times S$, where $\Delta \subset S \times S$ denotes the diagonal $\{(x, x) : x \in S\}$. Of course, for such a function f we then have $f'(a) = \Phi f(a, a)$ for any $a \in S$. Moreover, a version of local invertibility then holds for such functions f (see, e.g., [25, Theorem 27.5]).

We note that, in the Archimedean case of functions $f : I \to \mathbb{R}$ (where I is a compact subset of $\mathbb{R}$ without isolated points), this definition of continuous differentiability in fact agrees with the usual definition, since the existence of a continuous derivative at $a \in I$ implies the existence of a continuous extension of $\Phi f(x, y)$ to $(x, y) = (a, a)$. As such an extension is *not* automatic in the non-Archimedean case, it must be stated to exist explicitly.

More generally, we may define C^r (or r-times continuously differentiable) functions in terms of r-th divided differences:

Definition 16. Let S be a compact subset of a local field K, having no isolated points. A function $f : S \to K$ is said to be a C^r (or *r-times continuously differentiable*) function if its r-th divided difference function $\Phi^r f : S^{r+1} \setminus \Delta \to K$ (as defined by (8)) is extendable to a continuous function on all of S^{r+1}; here Δ denotes the "fat diagonal" of S^{r+1}, i.e., the set $\{(x_0, \ldots, x_r) \in S^{r+1} : x_i =$

---

[2]In the literature, some authors refer to this condition instead as "uniformly differentiable" or "strictly differentiable".

x_j for some $i \neq j$}. The norm of such a function f is given by $\|f\| = \|f\|_{C^r(S,K)} :=$ $\max\{|f|, |\Phi f|, \ldots, |\Phi^r f|\}$, where $|\Phi^q f|$ denotes the supremum of the values of $\Phi^q f$ on its domain S^{q+1} of definition.

The set $C^r(S, K)$ of all C^r-functions on S, under the norm as given in Definition 16, forms a K-Banach space. Since it is known to possess countable dense subsets, the question arises as to whether one can explicitly describe an orthonormal base for $C^r(S, K)$. Using the ideas of Sections 2 and 3, we show in Section 4.2.1 that natural polynomial orthonormal bases for C^r-functions on S may be given for any compact subset S of K.

The constructions given involve only certain combinatorial properties of the set S, which are encoded in what we have termed "r-removed P-orderings" and "r-removed generalized factorials".

4.1.1. *Interpolation series for the spaces $C^r(S, K)$.* Let S again be a compact subset of a local field K having no isolated points. Let R be the valuation ring of K and let π be a uniformizer. Let $\Lambda = \{a_i\}$ be an r-removed π-ordering of S and define the r-removed generalized binomial polynomials $\binom{x}{n}_\Lambda^{\{r\}}$ as in Section 3.1.1, (9). Then the main result of this section is:

Theorem 17. *The r-removed generalized binomial polynomials*

$$(18) \qquad \binom{x}{n}_\Lambda^{\{r\}} = \frac{(x - a_0)(x - a_1) \cdots (x - a_{n-1})}{n!_\Lambda^{\{r\}}},$$

for $n = 0, 1, 2, \ldots$, form an orthonormal base for $C^r(S, K)$.

We begin by proving Theorem 17 first for a special class of r-removed π-orderings. Given an r-removed π-ordering $\Lambda = \{a_i\}$ and a nonnegative integer n, we say that a_n is *old* (mod π^m) if $a_n \equiv a_j$ (mod π^m) for some $j \in A_n$; otherwise, we say that a_n is *new* (mod π^m). (Recall $A_n = \{1, \ldots, n\} \setminus \{n_1, \ldots, n_r\}$, where $n_1, \ldots, n_r$ denote the r indices removed at the n-th step of the r-removed π-ordering process.) We say that an r-removed π-ordering $\Lambda = \{a_i\}$ is *proper* if: 1) $a_0 = a_1 = \cdots = a_r$; and 2) for all m and all $n > r$, a_n is chosen to be a new element (mod π^m) only when it is not possible to choose a_n to be old. (Thus, for example, the sequence 0, 0, 1, 1, p, p, $p^3 + 1$, $2p$ forms the initial segment of a proper 1-removed p-ordering, whereas the sequence 0, 0, 1, 1, p, p, $2p$, $p^3 + 1$ does not.)

We note that, by construction, each element of S occurs $r + 1$ times in any proper r-removed π-ordering of S (if it occurs at all). In particular, the first $r + 1$ elements of a proper π-ordering are all equal.

In the case that Λ is proper, we have the following weak analogue of Lucas's theorem for the generalized binomials $\binom{x}{n}_\Lambda^{\{r\}}$ and their first r divided differences.

Lemma 18. *Suppose $\Lambda = \{a_i\}$ is a proper r-removed π-ordering and that a_n is new (mod π^m). Let $f(x) = \binom{x}{n}_\Lambda^{\{r\}}$. Then, for any $0 \leq q \leq r$, we have*

$$\Phi^q f(b_0, \ldots, b_q) \equiv \Phi^q f(b_0', \ldots, b_q') \pmod{\pi}$$

whenever $b_j, b_j' \in S$ and $b_j \equiv b_j'$ (mod π^m) for all $j \in \{0, \ldots, q\}$.

Proof. By (10), we have

$$(19) \qquad \Phi^q f(b_0, \ldots, b_q) = \sum_{\substack{i = (i_1, \ldots, i_q) \\ 0 \leq i_1 < \cdots < i_q < n}} \frac{1}{n!_\Lambda^{\{r\}}} \prod_{k \in \{0, \ldots, n-1\} \setminus \{i_1, \ldots, i_q\}} (b_{m_i(k)} - a_k)$$

and similarly,

$$(20) \qquad \Phi^q f(b'_0, \ldots, b'_q) = \sum_{\substack{\boldsymbol{i}=(i_1,\ldots,i_q) \\ 0 \le i_1 < \cdots < i_q < n}} \frac{1}{n!_\Lambda^{\{r\}}} \prod_{k \in \{0,\ldots,n-1\} \setminus \{i_1,\ldots,i_q\}} (b'_{m'_{\boldsymbol{i}}(k)} - a_k),$$

where the $m'_{\boldsymbol{i}}(k)$ are constructed in the analogous way using the b'_j rather than the b_j.

By (12), we see that each term in the sum on the right-hand side of (19) (or of (20)) has a nonnegative valuation and is thus in R. Now such a term on the right-hand side of (19) has a nonzero value modulo π if and only if the inequalities in (12) are actually equalities. Suppose this is the case for a particular term $T_{\boldsymbol{i}}$ in (19) corresponding to the q-tuple $\boldsymbol{i} = (i_1,\ldots,i_q)$. Then if the inequalities in (12) are equalities, we must have: (a) $v(b_{m_{\boldsymbol{i}}(k)} - a_k) = v(b_{m_{\boldsymbol{i}}(n)} - a_k)$ for each $k \in \{0,\ldots,n-1\} \setminus \{i_1,\ldots,i_q\}$; and (b) the sequence $a_0,\ldots,a_{n-1}, b_{m_{\boldsymbol{i}}(n)}$ forms the first $n+1$ terms of an r-removed π-ordering Λ^* of S. (Here, $m_{\boldsymbol{i}}(n)$ again denotes the unique element of $\{0,\ldots,q\} \setminus \{i_1,\ldots,i_q\}$.) Note that condition (b) implies that the q-tuple $\boldsymbol{i} = (i_1,\ldots,i_q)$ can be extended to an r-tuple $(i_1,\ldots,i_r)$ with $v(b_{m_{\boldsymbol{i}}(n)} - a_{i_k}) = 0$ for $q < k \le r$.

The fact that Λ^* is also an r-removed π-ordering implies that $b_{m_{\boldsymbol{i}}(n)}$ must be new (mod π^m) in Λ^*; i.e., $b_{m_{\boldsymbol{i}}(n)} \not\equiv a_k \pmod{\pi^m}$ for all $k \in \{0,\ldots,n-1\} \setminus \{i_1,\ldots,i_q\}$, since otherwise Λ would not be proper either. Therefore, if each occurrence of $b_{m_{\boldsymbol{i}}(n)}$ were to be replaced by $b'_{m_{\boldsymbol{i}}(n)}$ in the term $T_{\boldsymbol{i}}$ in (19), then, since $b_{m_{\boldsymbol{i}}(n)} - a_k$ and $b'_{m_{\boldsymbol{i}}(n)} - a_k$ have the same last nonzero π-adic digit for all $k \in \{0,\ldots,n-1\} \setminus \{i_1,\ldots,i_q\}$, the value of $T_{\boldsymbol{i}}$ modulo π would remain unchanged.

Furthermore, suppose each occurrence of the variable $b_{m_{\boldsymbol{i}}(k)}$ were to be replaced by $b'_{m_{\boldsymbol{i}}(k)}$ in the term $T_{\boldsymbol{i}}$ in (19) for some set of $k \in \{0,\ldots,n-1\} \setminus \{i_1,\ldots,i_q\}$. Then by condition (a) and the properness of Λ^*, we have $v(b_{m_{\boldsymbol{i}}(k)} - a_k) = v(b_{m_{\boldsymbol{i}}(n)} - a_k) < m$, and hence $b_{m_{\boldsymbol{i}}(k)} - a_k$ and $b'_{m_{\boldsymbol{i}}(k)} - a_k$ again have the same last nonzero π-adic digit. Thus the value of $T_{\boldsymbol{i}}$ modulo π would again remain unchanged.

Finally, suppose a variable b_j were changed to b'_j in $T_{\boldsymbol{i}}$, where j is not of the form $m_{\boldsymbol{i}}(k)$ for any $k \in \{0,\ldots,n-1\} \setminus \{i_1,\ldots,i_q\}$. Then since the variable b_j does not even appear in the expression for $T_{\boldsymbol{i}}$ in that case, the value of $T_{\boldsymbol{i}}$ again would not change.

The above arguments show, in particular, that for such a term $T_{\boldsymbol{i}}$ in (19) that is nonzero modulo π, the corresponding term $T'_{\boldsymbol{i}}$ in (20) involves the same indices (i.e., $m_{\boldsymbol{i}}(k) = m'_{\boldsymbol{i}}(k)$ for all k). Furthermore, we have $T_{\boldsymbol{i}} \equiv T'_{\boldsymbol{i}} \pmod{\pi}$ for all such $\boldsymbol{i}$. By interchanging b_j and b'_j in the above arguments we also see that, for each term $T'_{\boldsymbol{i}}$ in (20) that is nonzero modulo π, the corresponding term $T_{\boldsymbol{i}}$ in (19) is also nonzero (mod π) and has the same value (mod π). We conclude that the terms in (19) and (20) that are nonzero modulo π correspond to the same indices $\boldsymbol{i}$, and they also share the same values (mod π). Meanwhile, the remaining terms in both (19) and (20) must all be zero (mod π). The lemma follows. $\square$

We are now ready to show that any f in $C^r(S,K)$ with $\|f\|_{C^r(S,K)} \le 1$ can be expressed (mod π) as an R-linear combination of r-removed generalized binomial polynomials. Moreover, this can be done in such a way so that the first r-divided differences also agree (mod π):

Lemma 19. *Suppose that $f \in C^r(S, K)$ is a function with $\|f\|_{C^r(S,K)} \le 1$ such that, for any $0 \le q \le r$, we have*

$$\Phi^q f(b_0, \ldots, b_q) \equiv \Phi^q f(b'_0, \ldots, b'_q) \pmod{\pi}$$

whenever $b_j, b'_j \in S$ satisfy $b_j \equiv b'_j \pmod{\pi^m}$ for all $j \in \{0, \ldots, q\}$. Let $\Lambda = \{a_i\}$ be a proper r-removed π-ordering of S, and let T be the set of n such that a_n is new $\pmod{\pi^m}$. Then there exists a function $h : T \to R$ such that if we set

$$g(x) = \sum_{n \in T} h(n) \binom{x}{n}_{\Lambda}^{\{r\}},$$

then

$$\Phi^q f(b_0, \ldots, b_q) \equiv \Phi^q g(b_0, \ldots, b_q) \pmod{\pi}$$

for all $0 \le q \le r$ and all $b_0, \ldots, b_q \in S$. Moreover, the values of $h(n)$ are uniquely determined modulo π.

Proof. Let f be as in the lemma. By the assumption on f and the definition of T, it is clear that the values of $\Phi^q f \pmod{\pi}$ on S^{q+1}, for all $0 \le q \le r$, are completely determined by the values of $\Phi^q f \pmod{\pi}$ on elements of the form $(a_{m_0}, \ldots, a_{m_q})$ where $m_0, \ldots, m_q \in T$.

We claim that the values of $\Phi^q f \pmod{\pi}$ on such elements (and thus also on S^{q+1}) for all $0 \le q \le r$ are in fact completely determined by just the values of

$$(21) \qquad f(a_0), \ \Phi f(a_1, a_0), \ \ldots \ , \ \Phi^{r-1} f(a_{r-1}, \ldots, a_0) \pmod{\pi}$$

and of

$$(22) \qquad\qquad \Phi^r f(a_n, a_{n_1}, \ldots, a_{n_r}) \pmod{\pi}$$

for $n \in T - \{0, \ldots, r-1\}$. Moreover, for any chosen values of these $|T|$ divided differences in (21) and (22), there exists a function $f \in C^r(S, K)$ having this set of $|T|$ divided differences $\pmod{\pi}$.

To prove the claim, consider a specific divided difference $\Phi^q f(a_{m_0}, \ldots, a_{m_q})$, where $m_i \in T$ for all i. Since each element $a \in S$ occurs $r + 1$ times in a proper r-removed π-ordering (if it occurs at all), we may assume without loss of generality that $m_0, m_1, \ldots, m_q$ are distinct integers in T. We wish to express $\Phi^q f(a_{m_0}, \ldots, a_{m_q}) \pmod{\pi}$ in terms of the $|T|$ divided differences modulo π listed in (21) and (22).

For convenience, we may renumber the a_{m_i} if necessary so that m_0 is equal to $n = \max_i\{m_i\}$. If $n = m_0 < r$, then $\Phi^q f(a_{m_0}, \ldots, a_{m_q})$ already appears in the list (21) and we are done. Hence we may assume $n \ge r$. In that case, we may then renumber $m_1, \ldots, m_q$ and $n_1, \ldots, n_r$ so that $a_{m_0} = a_n$, $a_{m_1} = a_{n_1}$, $\ldots$, $a_{m_k} = a_{n_k}$, but $\{m_{k+1}, \ldots, m_q\} \cap \{n_{k+1}, \ldots, n_r\} = \emptyset$ and $v(a_n - a_{m_i}) \le v(a_n - a_{n_i})$ for $k + 1 \le i \le q$. The latter condition is possible to arrange because the sequence $\{a_i\}$ is an r-removed π-ordering of S, so the valuations $v(a_n - a_{n_1}), \ldots, v(a_n - a_{n_r})$ are the r highest among all valuations of the form $v(a_n - a_j)$ where $j < n$.

With these new numberings, we now prove that we can express $\Phi^q f(a_{m_0}, \ldots, a_{m_q}) \pmod{\pi}$ in terms of the $|T|$ divided differences $\pmod{\pi}$ in (21) and (22) by induction

on $m_0 = n$. First, setting also $n_0 = n$, we have the following algebraic identity:

$$\Phi^q f(a_n, a_{m_1}, \ldots, a_{m_q})$$

(23)
$$= \sum_{i=0}^{q} \frac{a_{n_i} - a_{m_i}}{a_n - a_{m_i}} \prod_{j=i+1}^{q} \frac{a_n - a_{n_j}}{a_n - a_{m_j}} \Phi^q f(a_{m_1}, \ldots, a_{m_i}, a_{n_i}, \ldots, a_{n_q}).$$

This identity, once discovered, is elementary to prove by induction on q. Indeed, the identity for $q = 0$ simply states that $\Phi^0 f(a_n) = \Phi^0 f(a_n)$, while the identity for general $q > 0$ can be deduced from the identity for $q - 1$ through the observation that $\Phi^q f(a_n, a_{m_1}, \ldots, a_{m_q}) = \Phi^{q-1} g(a_n, a_{m_2}, \ldots, a_{m_q})$, where $g(x) = \Phi^1 f(a_{m_1}, x)$.

We now note that the terms in the sum on the right-hand side of (23), from $i = 1$ to $i = k$, are each equal to zero, while the remaining nonzero terms in the sum each must have nonnegative valuation. Indeed, $v(a_n - a_{m_j}) \leq v(a_n - a_{n_j})$ by assumption, and similarly we have $v(a_n - a_{m_i}) = \min\{v(a_n - a_{m_i}), v(a_n - a_{n_i})\} \leq v(a_{n_i} - a_{m_i})$ by the ultrametric triangle inequality. By the induction hypothesis, $\Phi^q f(a_{m_1}, \ldots, a_{m_i}, a_{n_i}, \ldots, a_{n_q})$ is determined modulo π by the $|T|$ divided differences (mod π) in (21) and (22), since $m_1, \ldots, m_q$ and $n_1, \ldots, n_r$ are all less than $m_0 = n$. We conclude that the sum in (23) is well defined (mod π) once the values in (21) and (22) are fixed, and hence $\Phi^q f(a_n, a_{m_1}, \ldots, a_{m_q})$ is also now determined, proving the claim.

To see that this claim proves the lemma, we note that h uniquely determines the set of divided differences in (21) and (22) by Lemma 18. Conversely, given an f satisfying the conditions of the lemma, the values of h (modulo π) can be uniquely recovered from f using the recursive formula

(24)
$$h(n) \equiv \Phi^r f(a_n, a_{n_1}, \ldots, a_{n_r}) - \sum_{\substack{i \in T \\ i < n}} h(i) \Phi^r \binom{x}{i}_{\Lambda}^{\{r\}} (a_n, a_{n_1}, \ldots, a_{n_r}) \pmod{\pi};$$

this recursive formula holds because we have:

$$\Phi^r \binom{x}{j}_{\Lambda}^{\{r\}} (a_n, a_{n_1}, \ldots, a_{n_r}) = \begin{cases} 1 & \text{if } j = n, \\ 0 & \text{if } j > n. \end{cases}$$

Thus every f is represented by exactly one h (mod π), and the proof is complete. $\square$

We may now give a proof of Theorem 17 in the case when Λ is proper.

Proof of Theorem 17 *for proper* Λ. Let $f \in C^r(S, K)$ be a function. We first wish to show that f has a unique expansion as

$$f(x) = \sum_{n=0}^{\infty} c_n \binom{x}{n}_{\Lambda}^{\{r\}},$$

where c_n tends to zero as n tends to infinity. Since S is compact, we may rescale S and f if necessary and assume that $S \subset R$ and $\|f\| \leq 1$, i.e., the values of all the q-th divided differences of f on S lie in R for $0 \leq q \leq r$.

As at the end of the proof of Lemma 19, uniqueness of the c_n follows by noting that the c_n can be computed recursively from the values of f at the a_i via the formula

(25)
$$c_n = \Phi^r f(a_n, a_{n_1}, \ldots, a_{n_r}) - \sum_{i=0}^{n-1} c_i \Phi^r \binom{x}{i}_{\Lambda}^{\{r\}} (a_n, a_{n_1}, \ldots, a_{n_r}).$$

To prove existence, it suffices to show that there exists a sequence c_n with finitely many nonzero terms such that if we set

$$g(x) = \sum c_n \binom{x}{n}_\Lambda^{\{r\}},$$

then

$$\Phi^q f(b_0, \dots, b_q) \equiv \Phi^q g(b_0, \dots, b_q) \pmod{\pi}$$

for all $0 \le q \le r$ and all $(b_0, \dots, b_q) \in S^{q+1}$, since we can then apply the same reasoning to $[f(x) - \sum c_n \binom{x}{n}_\Lambda^{\{r\}}]/\pi$, and so on. By the assumption $f \in C^r(S, K)$, we know that the functions f, Φf, $\dots$, $\Phi^r f$ are π-adically continuous on S, S^2, $\dots$, S^{r+1}, respectively, and so f must satisfy the conditions of Lemma 19 for some m. In this case, setting $c_n = h(n)$ for $n \in T$ and $c_n = 0$ otherwise furnishes the desired sequence.

To complete the proof of Theorem 17 for proper π-orderings Λ, we need only verify property (ii) of Definition 15. Because of property (i), it again suffices to check (ii) on finite linear combinations $v = f(x) = \sum_{n=0}^{N} c_n \binom{x}{n}_{\Lambda,h}$. Since $\left\| \binom{x}{n}_\Lambda^{\{r\}} \right\| = 1$ for all n by construction, we clearly have $\|f\| \le \sup_{n \ge 0}\{|c_n|\}$. To show equality, suppose $\|f\| < |c_n|$ for some n, and let k be the integer such that $\|f\| = |\pi^k|$. Then f/π^k must be in $\mathrm{Int}^{\{r\}}(S, R)$; however, in its expansion as

$$\frac{f(x)}{\pi^k} = \sum_{n=0}^{N} \frac{c_n}{\pi^k} \binom{x}{n}_\Lambda^{\{r\}},$$

we see that not every coefficient $\frac{c_n}{\pi^k}$ is in R, contradicting Theorem 7. We conclude $\|f\| = \sup_{n \ge 0}\{|c_n|\}$, and the proof is complete. $\qquad\square$

We may now also deduce Theorem 17 for arbitrary π-orderings, which we turn to next.

4.1.2. *Correspondence between $C^r(S, K)$ and $\mathrm{Int}^{\{r\}}(S, R)$.* Having constructed a regular polynomial orthonormal base for $C^r(S, K)$, we may now describe *all* such bases for $C^r(S, K)$. The key is to note the precise relationship between $C^r(S, K)$ and the ring $\mathrm{Int}^{\{r\}}(S, R)$.

We begin with the following general proposition describing orthonormal bases of K-Banach spaces and the associated R-modules spanned by them:

Proposition 20. *Let $\mathcal{B}$ be any K-Banach space, and suppose $\mathcal{B}$ has an orthonormal base given by $f_0, f_1, \dots$. Let $\mathcal{I} \subset \mathcal{B}$ denote the R-module spanned by the f_i, and let V be the K-vector space $\mathcal{I} \otimes K$. Then every other orthonormal base of $\mathcal{B}$ spanning V as a K-vector space is of the form $g_0, g_1, \dots$, where the g_i form an R-basis of the R-module $\mathcal{I}$. Moreover, we have*

$$(26) \qquad\qquad \mathcal{I} = \{f \in V : \|f\| \le 1\}.$$

Proof. Let $f_0, f_1, \dots$ and $\mathcal{I}$ be as defined in the proposition, and suppose $g_0, g_1, \dots$ is any other R-basis of $\mathcal{I}$. By assumption, for any $h \in \mathcal{B}$ there exists a unique sequence $b_m \to 0$ such that

$$(27) \qquad\qquad h = \sum_{m=0}^{\infty} b_m f_m.$$

To show property (i) of Definition 15, we wish to show that there exists a sequence $c_n \to 0$ such that

$$(28) \qquad\qquad\qquad h = \sum_{n=0}^{\infty} c_n g_n.$$

Since both the f_i and g_i form R-bases of $\mathcal{I}$, there exist transformations $T = (t_{mn})$ and $U = (u_{nm})$ over R such that

$$f_m = \sum_{n=0}^{\infty} t_{mn} g_n \quad \text{and} \quad g_n = \sum_{m=0}^{\infty} u_{nm} f_m.$$

In particular, these summations each contain only finitely many nonzero terms; i.e., there exist integers $N(m)$ and $M(n)$ such that $t_{mn} = 0$ for all $n \geq N(m)$ and $u_{nm} = 0$ for all $m \geq M(n)$. Define c_n by the formula

$$c_n = \sum_{m=0}^{\infty} b_m t_{mn};$$

the series converges for every n since $t_{mn} \in R$ and $b_m \to 0$. Moreover, for any nonnegative integer i, there exists M such that π^i divides b_m for $m \geq M$, and there exists N such that $t_{1n} = \cdots = t_{Mn} = 0$ for $n \geq N$. Hence π^i divides c_n for $n \geq N$, and so $c_n \to 0$.

To demonstrate (28), it suffices to verify that the two sides of the equality agree modulo π^i for all nonnegative integers i. With notation as in the preceding paragraph, we have

$$f = \sum_{m=0}^{\infty} b_m f_m \equiv \sum_{m=0}^{M} b_m \sum_{n=0}^{\infty} t_{mn} g_n = \sum_{m=0}^{M} \sum_{n=0}^{N} b_m t_{mn} g_n \quad (\mathrm{mod}\ \pi^i).$$

On the other hand,

$$\sum_{n=0}^{\infty} c_n g_n \equiv \sum_{n=0}^{N} g_n \sum_{m=0}^{\infty} b_m t_{mn} \equiv \sum_{n=0}^{N} \sum_{m=0}^{M} b_m t_{mn} g_n \quad (\mathrm{mod}\ \pi^i),$$

and (28) follows.

To prove property (ii) of Definition 15, we first prove the equality (26). Let $\mathcal{I}' = \{f \in V : \|f\| \leq 1\}$. Since $f_0, f_1, \dots$ form an orthonormal base for $\mathcal{B}$, we have $\|f_i\| = 1$ for all i and hence $\mathcal{I} \subset \mathcal{I}'$. To see $\mathcal{I} = \mathcal{I}'$, let $f \in \mathcal{I}'$ be any element. Then since $f \in V$, there exists a sequence d_m in K such that $f = \sum_{m=0}^{M} d_m f_m$. Now since the f_i form an orthonormal base of $\mathcal{B}$, we have $\max\{|d_m|\} = \|f\| \leq 1$, and hence $d_m \in R$ for all m. It follows that $f \in \mathcal{I}$, and thus $\mathcal{I} = \mathcal{I}'$, as desired.

Finally, we show that the elements g_n satisfy property (ii) of Definition 15. Because of property (i), it suffices to check property (ii) on finite linear combinations $h(x) = \sum_{n=0}^{N} c_n g_n(x)$. We wish to show that $c = \max\{|c_n|\}$ is equal to $\|h\|$. Since the g_n are in $\mathcal{I} = \mathcal{I}'$, clearly $\|h\| \leq c$. Now suppose $\|h\| < c$, so that $\|h\| < |c_n|$ for some n, and let k be the integer such that $\|h\| = |\pi^k|$. Then the function $h(x)/\pi^k$ is in $\mathcal{I}$, due to (26); however, in the expansion of $h(x)/\pi^k$ as

$$\frac{h(x)}{\pi^k} = \sum_{n=0}^{N} \frac{c_n}{\pi^k} g_n$$

we see that not every coefficient $\frac{c_n}{\pi^k}$ is in R, contradicting the fact that the g_i form an R-basis of $\mathcal{I}$. It follows that $\|h\| = c$, yielding property (ii) for the g_i. Thus the g_i form an orthonormal base for $\mathcal{B}$, and this is the desired conclusion. $\qquad\square$

In the case of Theorem 17, we have $V = K[x]$, $\mathcal{B} = C^r(S, K)$, and $\mathcal{I} = \operatorname{Int}^{\{r\}}(S, R)$. Proposition 20 now immediately gives:

Theorem 21. *Let S be a compact subset of K without isolated points, and let $f_0, f_1, \dots$ be a sequence of polynomials in $K[x]$ such that $\deg(f_i) = i$. Then the sequence $f_0, f_1, \dots$ forms an orthonormal base for the K-Banach space $C^r(S, K)$ if and only if it forms an R-basis for the ring $\operatorname{Int}^{\{r\}}(S, R)$.*

Although the theorem above describes all regular polynomial orthonormal bases of $C^r(S, K)$ in terms of $\operatorname{Int}^{\{r\}}(S, R)$, the bases $\{\binom{x}{n}_\Lambda^{\{r\}}\}$ constructed in the previous section are very special; namely, they are useful for interpolation of functions due to the recursive formula (25). As a consequence, for these bases, if a sum of the type $\sum_{n=0}^\infty c_n \{\binom{x}{n}_\Lambda^{\{r\}}\}$ converges pointwise to an element of $C^r(S, K)$, then it actually converges to that element (i.e., with respect to the much stronger $C^r(S, K)$ norm)! This follows directly from the proof of Theorem 17. We note that this special property does not necessarily hold true for general bases of $C^r(S, K)$ (see, e.g., the construction in [7] for examples of this phenomenon). This property is enjoyed by these special bases due to the structure of r-removed π-orderings. We end by combining Remark 9 with Theorem 21 to obtain:

Theorem 22. *Let S be a compact subset of K without isolated points, let $\{a_i\}$ be a sequence of elements in S, and let $\{\beta_i\}$ be a nonzero sequence in K. Then the polynomials*

$$\frac{(x - a_0)(x - a_1) \cdots (x - a_{n-1})}{\beta_n}, \quad n = 0, 1, 2, \dots,$$

form an orthonormal base of $C^r(S, K)$ if and only if $\{a_i\}$ is an r-removed π-ordering of S and $(\beta_n) = (n!_\Lambda^{\{r\}})$ as ideals in R.

4.2. **The Banach space of locally analytic functions of order h.** Rather than considering conditions of continuous differentiability as in Section 4.1, we may instead consider the other important notion of smoothness that plays a central role in Archimedean analysis, namely that of (local) analyticity. In non-Archimedean analysis too, the context of the particular problem often dictates which notion—differentiability or analyticity—is the more useful.

Let K again denote a local field with valuation ring R and uniformizer π. Let $a \in K$, let $\rho = |\pi|^h$ for some integer h, and let $B(a, \rho)$ denote the closed ball with center a and radius ρ.

Definition 23. A function $f \in C(B(a, \rho), K)$ is *analytic* on $B(a, \rho)$ if f can be expanded as a power series

$$f(x) = \sum_{n=0}^\infty c_n \left(\frac{x - a}{\pi^h} \right)^n$$

which converges for all $x \in B(a, \rho)$ (equivalently, $\lim_{n \to \infty} c_n = 0$). The norm of such a function f is given by $\|f\|_{B(a,\rho)} := \sup_{n \geq 0}\{|c_n|\}$.

It can be shown that the expansion property, the radius of convergence, and the norm of f in Definition 23 do not depend on the choice of a in the ball $B(a, \rho)$ (see [25, Theorem 25.5]). It follows that the notion of "analytic continuation" as in Archimedean analysis does not quite make sense in the non-Archimedean scenario. This motivates the definition of a *locally analytic* function on a compact subset S of K, which means a function $f : S \to K$ such that for every $a \in S$, there is a neighborhood U of a such that f extends to an analytic function on U.

Since S is compact, there is a uniform h that will work for all $a \in S$. Such a function is then called *locally analytic of order h*. Let us assume from here onward that S is compact and has no isolated points. Then we have:

Definition 24. A function $f : S \to K$ is *locally analytic of order h* if for every $a \in S$, $f|_{B(a,|\pi|^h) \cap S}$ is extendable to an analytic function on all of $B(a, |\pi|^h)$. The norm of such a function f is given by $\|f\| = \|f\|_{LA_h(S,K)} := \sup_{a \in S}\{\|f\|_{B(a,|\pi^h|)}\}$.

If S has no isolated points (as we have assumed), then any extension of $f : S \to K$ into a ball $B(a, \rho)$ for $a \in S$ must be unique if it exists (see [25]). Hence, in particular, the norm of a locally analytic function $f : S \to K$ of order h is well defined. The space $LA_h(S, K)$ of locally analytic functions of order h from S to K under this norm is easily seen to be a K-Banach space. One can also easily see that this K-Banach space has a countable dense subset, implying the existence of an orthonormal base. The goal of the next section is the construction of an explicit (polynomial) orthonormal base for $LA_h(S, K)$.

4.2.1. *Interpolation series for the space $LA_h(S, K)$.* Let S again be a compact subset of a local field K having no isolated points. Let R be the valuation ring of K and let π be a uniformizer. Let $\Lambda = \{a_i\}$ be a π-ordering of S of order h and define the generalized binomial polynomials $\binom{x}{n}_{\Lambda,h}$ of order h as in Section 3.2.2, (13). In this section, we prove the following theorem:

Theorem 25. *The generalized binomial polynomials*

$$(29) \qquad \binom{x}{n}_{\Lambda,h} = \frac{(x - a_0)(x - a_1)\cdots(x - a_{n-1})}{n!_{S,h}},$$

$n = 0, 1, 2, \ldots$, *form an orthonormal base for* $LA_h(S, K)$.

To prove Theorem 25, we begin by observing that the space $LA_h(S, K)$ has an obvious orthonormal base as follows. Let T_0 denote the set of all n such that the residue class of a_n modulo π^h does not occur in $\{a_0, a_1, \ldots, a_{n-1}\}$. Define the functions $\{\Xi_{k,i}\}_{k\geq 0, i \in T_0}$ by

$$\Xi_{k,i} = \begin{cases} \left(\frac{x - a_i}{\pi^h}\right)^k & \text{if } x \in B(a_i, |\pi|^h); \\ 0 & \text{if } x \notin B(a_i, |\pi|^h). \end{cases}$$

Then clearly the $\Xi_{k,i}$ form an orthonormal base for $LA_h(S, K)$. We prove Theorem 25 by molding this rather ludicrous basis into our generalized binomial polynomial basis (13).

We first prove Theorem 25 for a special class of π-orderings. For a π-ordering $\{a_i\}$ of S of order h, the *repetition value* of a_n modulo π^h is the number of times the residue class of $a_n \pmod{\pi^h}$ occurs in the set $\{a_0, a_1, \ldots, a_{n-1}\}$. A π-ordering $\Lambda = \{a_i\}$ of order h is *proper* if for each n, the element a_n is chosen to have the highest possible repetition value modulo π^h. For example, $0, 1, p, p^3 + 1, 2p$ forms the initial segment of a proper p-ordering of order 2, whereas a p-ordering of order 2 having initial segment $0, 1, p, 2p, p^3 + 1$ is not proper.

Generalizing T_0, let T_k denote the set of all n such that the repetition value of a_n modulo π^h is k. The following lemma illustrates why the notion of proper is so useful.

Lemma 26. *Assume* $\Lambda = \{a_i\}$ *is proper, and let* $m, n \in T_k$. *Then modulo* π,

$$(30) \qquad P_{m,n}(X) = \binom{\pi^h X + a_m}{n}_{\Lambda, h}$$

is identically zero if $m < n$, *is a monic polynomial in* X *of degree* k *if* $m = n$, *and is either identically zero or a monic polynomial in* X *of degree at most* k *if* $m > n$.

Proof. The π-valuation of $P_{m,n}$ is equal to

$$(31) \qquad \sum_{i=0}^{n-1} \min(h, v(a_m - a_i)) - \sum_{i=0}^{n-1} \min(h, v(a_n - a_i)),$$

which is always nonnegative by the very construction of the π-ordering $\{a_i\}$ of order h. If $m < n$, then the fact that the element a_n (of repetition value k) was chosen at the n-th step rather than a_m (which would have had repetition value $\geq k + 1$) indicates that $\sum_{i=0}^{n-1} \min(h, v(a_m - a_i)) > \sum_{i=0}^{n-1} \min(h, v(a_n - a_i))$. Hence if $m < n$, then the π-valuation of $P_{m,n}$ is positive and so $P_{m,n}$ vanishes modulo π.

If $m = n$, then expression (31) shows that the π-valuation of $P_{m,n}$ is zero. We may write

$$(32) \qquad P_{m,n}(X) = \prod_{i=0}^{n-1} \left(\frac{\pi^h X + a_m - a_i}{\pi^{\min(h, v(a_m - a_i))}} \right),$$

where each of the factors on the right side is integral and of π-valuation zero. It is clear from this factorization that, modulo π, the polynomial $P_{m,n}$ is monic and its degree is simply the number of factors for which $h = \min(h, v(a_m - a_i))$. This is the repetition value of a_m modulo π^h, namely, k.

Finally, if $m > n$, then the π-valuation (31) of $P_{m,n}$ is either zero or positive. If it is positive, then $P_{m,n}$ vanishes modulo π; if it is zero, then (32) again gives an expression for $P_{m,n}$ and so the identical argument to the case $m = n$ then shows that, modulo π, $P_{m,n}$ is a monic polynomial of degree at most k. This is the desired conclusion. $\qquad\square$

Let $\mathcal{E}_m$ denote the R-submodule of $LA_h(S, K)$ spanned by $\{\Xi_{k,i}\}_{0 \leq k \leq m, \, i \in T_0}$, and denote by $\bar{\mathcal{E}}_m$ the $R/\pi R$-vector space of functions in $\mathcal{E}_m$ reduced modulo π.

Then Lemmas 26 implies the following:

Corollary 27. *Assume the π-ordering Λ is proper. If $\phi : S \to R/\pi R$ is a function in $\bar{\mathcal{E}}_k$, then there is a unique function $\tau : \bigcup_{i=0}^{k} T_i \to R/\pi R$ such that*

$$(33) \qquad \phi(x) = \sum_{i=0}^{k} \sum_{n \in T_i} \tau(n) \binom{x}{n}_{\Lambda,h}.$$

Proof. Every τ gives rise to a unique ϕ. On the other hand, we claim that every ϕ is represented by a unique τ. Indeed, since $\phi \in \bar{\mathcal{E}}_k$, for any $m \geq 0$ we may write

$$(34) \qquad \phi(\pi^h X + a_m) = \sum_{j=0}^{k} c_{m,j} X^j$$

for some set of constants $c_{m,j}$ in $R/\pi R$. Let us further write

$$(35) \qquad P_{m,n}(X) = \binom{\pi^h X + a_m}{n}_{\Lambda,h} = \sum_{j=0}^{n} b_{m,n,j} X^j$$

where $b_{m,n,j} \in R$. If $m, n \in T_i$, then Lemma 26 implies that $b_{m,n,i}$ is 0 (mod π) for $n > m$ and is a unit in R for $n = m$. Furthermore, if $m \in T_i$ and $n \in T_j$ where $j < i$, then Lemma 26 again implies that $b_{m,n,i} = 0$, since $P_{m,n}(X)$ is of degree strictly smaller than i in that case. Hence, by equating the coefficients of X^i in (33), using the expansions (34) and (35), we find that the value of $\tau(m) \in R/\pi R$ for $m \in T_i$ is uniquely determined from ϕ by the recursive formula

$$(36) \qquad \tau(m) = c_{m,i} - \sum_{\substack{n \in T_i \\ n < m}} \tau(n) \, b_{m,n,i} - \sum_{\substack{n \in T_j \\ j > i}} \tau(n) \, b_{m,n,i};$$

i.e., $\tau(m)$ is determined from the values of $\tau(n)$ for $n < m$ ($n \in T_i$) and for $n \in T_j$ ($j > i$). Thus every ϕ is represented by exactly one τ. $\qquad \square$

Proof of Theorem 25 *for proper Λ.* First, we wish to show that any $f \in LA_h(S, K)$ can be expressed uniquely in the form $\sum_{n=0}^{\infty} c_n \binom{x}{n}_{\Lambda,h}$, where $c_n \to 0$ as $n \to \infty$. To see this, it suffices to assume $\|f\| \leq 1$ (by scaling f by an element of R if necessary) and to show that there exists a unique sequence c_n (mod π) with finitely many nonzero terms such that, as polynomials in X, we have

$$f(\pi^h X + a_m) \equiv \sum_{n=0}^{\infty} c_n \binom{\pi^h X + a_m}{n}_{\Lambda,h} \pmod{\pi}$$

for all $m \in T_0$, since we can then apply the same reasoning to $[f(x) - \sum c_n \binom{x}{n}_{\Lambda,h}]/\pi$, and so on. Now since $f \in LA_h(S, K)$, the reduction $\bar{f}$ of f modulo π is contained in $\bar{\mathcal{E}}_k$ for sufficiently large k, and so the previous lemma implies the existence of such a sequence c_n modulo π.

The uniqueness of the sequence $\{c_n\}$ follows from the observation that the c_m can be computed recursively from f, as follows. Since $f \in LA_h(S, K)$, we may write

$$(37) \qquad f(\pi^h X + a_m) = \sum_{n=0}^{\infty} c_n P_{m,n}(X) = \sum_{i=0}^{\infty} c_{m,i} X^i$$

for some constants $c_{m,i} \in R$ determined by f. Suppose, furthermore, that

$$P_{m,n}(X) = \sum_{j=0}^{n} b_{m,n,j} X^j,$$

where $b_{m,n,j} \in K$. If $m \in T_k$, then, as observed in the proof of Theorem 12, $b_{m,n,k} = 0$ for $n > m$ and is a unit in R for $n = m$. Hence, equating the coefficients of X^k in (37) above, we obtain

$$\sum_{n=0}^{m} c_n b_{m,n,k} = c_{m,k} \quad \Rightarrow \quad c_m = \frac{c_{m,k} - \sum_{n=0}^{m-1} c_n b_{m,n,k}}{b_{m,m,k}},$$

and thus the c_m are indeed uniquely determined by the function $f \in LA_h(S,K)$.

To complete the proof of Theorem 25 for proper π-orderings Λ, we need only verify that the generalized binomial polynomials $\binom{x}{n}_{\Lambda,h}$ satisfy property (ii) of Definition 15. Because of property (i), it suffices to check (ii) on finite linear combinations $v = f(x) = \sum_{n=0}^{N} c_n \binom{x}{n}_{\Lambda,h}$. Since $\|\binom{x}{n}_{\Lambda,h}\| = 1$ for all n by construction, we clearly have $\|f\| \leq \sup_{n \geq 0}\{|c_n|\}$. To show equality, suppose $\|f\| < |c_n|$ for some n, and let k be the integer such that $\|f\| = |\pi|^k$. Then f/π^k is in $\text{Int}_{\pi^h}(S,R)$, but in its expansion as

$$\frac{f(x)}{\pi^k} = \sum_{n=0}^{N} \frac{c_n}{\pi^k} \binom{x}{n},$$

we see that $\frac{c_n}{\pi^k} \notin R$ for some n, contradicting Theorem 12. We conclude that $\|f\| = \sup_{n \geq 0}\{|c_n|\}$, and the proof is complete. $\square$

We show how Theorem 25 follows for general π-orderings of order h in the next subsection.

As a final remark, we note that all the theorems in this section remain true when $h = \infty$ and "locally analytic of order h" is replaced by "continuous"; these results were treated earlier in [4] and [7]. Thus, in a sense, "continuous" may naturally be considered equivalent to the phrase "locally analytic of order ∞".

4.2.2. *Correspondence between $LA_h(S,K)$ and $\text{Int}_{\pi^h}(S,R)$.* Applying Proposition 20 again, we obtain the following theorem relating bases of the space $LA_h(S,K)$ with those of the ring $\text{Int}_{\pi^h}(S,R)$:

Theorem 28. *Let S be a nonempty compact subset of K without isolated points, and let $f_0, f_1, \ldots$ be a sequence of polynomials spanning the polynomial ring $K[x]$ as a K-vector space. Then the sequence $f_0, f_1, \ldots$ forms an orthonormal base for the K-Banach space $LA_h(S,K)$ if and only if it is an R-basis for the ring $\text{Int}_{\pi^h}(S,R)$ of R-valued polynomials of modulus π^h.*

In particular, Theorem 28 now implies Theorem 25 for any π-ordering of order h.

Theorem 28 makes precise the relationship between $LA_h(S,K)$ and $\text{Int}_{\pi^h}(S,R)$ and describes all possible regular polynomial orthonormal bases of $LA_h(S,K)$ in terms of this relationship. Nevertheless, there is again something very special about the bases $\{\binom{x}{n}_{\Lambda,h}\}$ constructed in Section 4.2.1. Namely, these bases are useful for the interpolation of functions, due to the recursive formula (36). As a consequence, for these special bases, if a sum of the type $\sum_{n=0}^{\infty} c_n \{\binom{x}{n}_{\Lambda,h}\}$ converges pointwise to an element of $LA_h(S,K)$, then it actually converges to that element (i.e., with

respect to the much stronger $LA_h(S, K)$ norm)! This follows directly from the proof of Theorem 25. We note that this special property does not necessarily hold true for general bases of $LA_h(S, K)$ (see [7] for a method for constructing examples of this phenomenon). This remarkable property is enjoyed by these special bases due to the combinatorial properties of proper π-orderings of order h. We end by combining Remark 13 with Theorem 28 to obtain:

Theorem 29. *Let S be any compact subset of K, let $\{a_i\}$ be any sequence of elements in S, and let $\{\beta_i\}$ be any nonzero sequence in K. Then the polynomials*

$$\frac{(x - a_0)(x - a_1) \cdots (x - a_{n-1})}{\beta_n}, \ \ n = 0, 1, 2, \ldots,$$

form an orthonormal base of $LA_h(S, K)$ if and only if $\{a_i\}$ is a π-ordering of S of order h and $(\beta_n) = (n!_{S,h})$ as ideals in R.

5. Conclusions and further results

Let K again denote a local field having valuation ring R, and let S be any compact subset of K without isolated points. Suppose $\mathcal{B}$ is a K-Banach space of continuous functions $f : S \to K$ whose norm function is bounded below by the usual supremum norm on $C(S, K)$, and suppose that $\mathcal{B}$ has an orthonormal base $f_0, f_1, \ldots$ of polynomials in $K[x]$, where f_d has degree d. Then the polynomials f_i span an R-module $\mathcal{I}$, which must necessarily be an R-submodule of the ring $\mathrm{Int}(S, R)$ of R-valued polynomials on S. The argument of the proof of Proposition 20 implies that if $g_0, g_1, \ldots$ is any other orthonormal polynomial base for $\mathcal{B}$, then $g_0, g_1, \ldots$ must span this same R-module $\mathcal{I}$. Conversely, if $g_0, g_1, \ldots$ is any regular R-basis for $\mathcal{I}$, then the g_i form an orthonormal base for $\mathcal{B}$. Thus there is a correspondence between bases for $\mathcal{I}$ and bases for $\mathcal{B}$.

If, moreover, the K-Banach space $\mathcal{B}$ is also a K-Banach algebra, then the R-module $\mathcal{I}$ becomes a ring of "integer-valued" (i.e., R-valued) polynomial mappings on S. This was precisely the case with the K-Banach spaces $\mathcal{B}$ considered in this article. For $\mathcal{B} = LA_h(S, K)$, we found $\mathcal{I} = \mathrm{Int}_{\pi^h}(S, R)$; and for $\mathcal{B} = C^r(S, K)$, we showed that $\mathcal{I} = \mathrm{Int}^{\{r\}}(S, R)$.

It is an interesting question as to how this correspondence might manifest itself for other natural spaces of functions defined on subsets of local fields. It is also an interesting problem to investigate how the function-theoretic aspects of the K-Banach spaces $\mathcal{B}$ are related to the ring-theoretic properties of the corresponding rings $\mathcal{I}$ of integer-valued polynomials. For example, one thing that one immediately observes is that stronger conditions of analyticity yield "smaller" rings of integer-valued polynomials. For example, we have recently shown in joint work (see [6]) that the ring $\mathrm{Int}_{\pi^h}(S, R)$ is finitely generated as an algebra over R, while the ring $\mathrm{Int}^{\{r\}}(S, R)$ is not. This reflects the fact that conditions of analyticity are indeed quite a bit stronger than those of continuous differentiability (as is true also in the Archimedean case).

Given the ideas of Sections 2–4, one further example of such a correspondence that we may consider, between K-Banach spaces and rings of integer-valued polynomials, is the following.

Let D be a Dedekind domain, $S \subset D$ a subset, and P any prime ideal of D. We have considered two distinct types of P-orderings in Section 2, namely: a) P-orderings of order h, and b) r-removed P-orderings. There is no reason not to

combine the two notions, namely to consider "*r*-removed *P*-orderings of order *h*". More precisely, an *r-removed P-ordering of S of order h* is a sequence $a_0, a_1, \ldots$ of elements in S constructed inductively to minimize the value of

$$(38) \qquad \sum_{i \in A_n} \min(h, v_P(a_n - a_i)),$$

where the sum is over any set A_n of $n - r$ elements in $\{0, \ldots, n-1\}$ minimizing (38).

We thereby obtain what we term the associated *r-removed p-sequence of order h* of S, denoted $\{\nu_k^{\{r\}}(S, P, h)\}$:

$$(39) \qquad \nu_k^{\{r\}}(S, P, h) = P^{\sum_{i \in A_n} \min(h, v_P(a_k - a_i))}.$$

Note that the case $r = 0$ coincides with *P*-orderings (resp. *P*-sequences) of order h, while the case $h = \infty$ coincides with *r*-removed *P*-orderings (resp. *P*-sequences). The associated *P*-sequence $\{\nu_k^{\{r\}}(S, P, h)\}$ gives invariants of the set S for each choice of (h, r). We have:

Theorem 30. *The associated r-removed P-sequence $\{\nu_k^{\{r\}}(S, P, h)\}$ of S of order h is independent of the choice of r-removed P-ordering of order h.*

Now suppose $D = R$ is a discrete valuation domain with uniformizer π and quotient field K and let $S \subset R$ be any subset without isolated points. An *r*-removed π-ordering Λ of S of order h yields *r-removed generalized polynomials* $\binom{x}{n}_{\Lambda,h}^{\{r\}}$ *of order* h, defined by

$$\binom{x}{n}_{\Lambda,h}^{\{r\}} = \frac{\prod_{i=0}^{n-1}(x - a_i)}{n!_{S,h}^{\{r\}}},$$

where

$$n!_{S,h}^{\{r\}} = \pi^{\sum_{i \in A_n} \min(h, v(a_n - a_i))}.$$

Finally, let $\mathrm{Int}_{\pi^h}^{\{r\}}(S, R)$ denote the ring of all polynomials $f \in K[x]$ whose q-th divided differences for $q = 0, 1, \ldots, r$ are R-valued polynomials on S^{q+1} with modulus π^h. Also, let $C_h^r(S, K)$ denote the K-Banach space consisting of those continuous functions $f : S \to K$ whose q-th divided differences for $q = 0, 1, \ldots, r$ extend to locally analytic functions of order h on S^{q+1}.

We may now combine all the main theorems of this paper into the following, giving one final generalization of the Pólya-Mahler theorems:

Theorem 31. *Let Λ be an r-removed π-ordering of S of order h. Then the corresponding generalized binomial polynomials $\binom{x}{n}_{\Lambda,h}^{\{r\}}$ form a regular basis for the ring $\mathrm{Int}_{\pi^h}^{\{r\}}(S, R)$ of integer-valued polynomials, and (when S is compact) also form an orthonormal base for the K-Banach space $C_h^r(S, K)$ of smooth functions on S.*

Again, one shows in the analogous manner that if $f_0, f_1, \ldots$ is a sequence of polynomials in $K[x]$ with $\deg(f_d) = d$, then it forms an orthonormal basis for $C_h^r(S, K)$ if and only if it simultaneously forms a regular basis for $\mathrm{Int}_{\pi^h}^{\{r\}}(S, R)$. One finds, as in [6], that the latter ring is also finitely generated whenever h is finite.

All these results are proven by directly combining the techniques used, throughout Sections 3 and 4, for the subscripts h and superscripts $\{r\}$. The global version

of the regular basis theorem for $\mathrm{Int}_{\mathcal{M}}^{\{r\}}(S, D)$ may be proven just as in Section 3.1.2. We decided not to prove the results of this paper directly in this generality because it would not have significantly shortened the treatment, and because in the primary applications in the literature the basic notions of local analyticity and continuous differentiability tend to appear separately and in different contexts; it is thus desirable to see the techniques required in each case separately. However, we thought we should at least state the result in a combined way here, not only because of its inherent interest, but in case someone may find the combined result of use in applications in the future.

Theorem 31 also now implies Theorem 1: the product of two polynomials f, g in the ring $\mathrm{Int}_{\pi^h}^{\{r\}}(S, R)$, having degrees k and ℓ, respectively, will yield a degree $k + \ell$ polynomial $fg \in \mathrm{Int}_{\pi^h}^{\{r\}}(S, R)$. Choosing f and g to have denominators $k!_{S,h}^{\{r\}}$ and $\ell!_{S,h}^{\{r\}}$, respectively, then yields Theorem 1.

Lastly, we note that all results in this paper proven for a discrete valuation ring R (Theorems 1–4, 7, 12, 17, 20–22, 25, 28, 30, and 31) hold equally well in any rank-one valuation domain R so long as S is assumed to be compact (or that its closure is compact, in the case of Theorems 1–4, 7, 12, and 30). This is because the r-removed π-ordering of order h construction is still well defined and valid in this generality. For ordinary π-orderings, this has been explained by Cahen and Chabert in [10] and [11]; the same reasoning applies in general. One must simply replace all occurrences of π^α in the proofs by π_α, where $\pi_\alpha \in R$ denotes an element with valuation α (since now not all valuations can be achieved by taking powers of a fixed uniformizer π). Otherwise, all proofs are essentially identical.

References

[1] Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964), 117-180. MR0188199 (32:5638)

[2] D. Barsky, Fonctions k-lipschitziennes sur un anneau local et polynômes à valeurs entières, *Bull. Soc. Math. France* **101** (1973), 397–411. MR0371863 (51:8080)

[3] S. Bernstein, *Leçons sur les propriétés extrémales de la meilleure approximation des fonctions analytiques d'une variable réelle*, Paris, 1926.

[4] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. reine. angew. Math.* **490** (1997), 101-127. MR1468927 (98j:13016)

[5] M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly* **107** (2000), 783–799. MR1792411 (2002d:05002)

[6] M. Bhargava, P.-J. Cahen, and J. Yeramian, Finite generation properties for rings of integer-valued polynomials, *J. Algebra*, to appear.

[7] M. Bhargava and K. S. Kedlaya, Continuous functions on compact subsets of local fields, *Acta Arith.* **91** (1999) 191-198. MR1735672 (2001d:11117)

[8] P.-J. Cahen, Polynômes à valeurs entières, *Canad. J. Math.* **24** (1972), 747-754. MR0309923 (46:9027)

[9] P.-J. Cahen and J.-L. Chabert, *Integer-valued polynomials*, Mathematical Surveys and Monographs, 48, American Mathematical Society, Providence, RI, 1997. MR1421321 (98a:13002)

[10] P.-J. Cahen, J.-L. Chabert, and K. A. Loper, High dimension Prüfer domains of integer-valued polynomials, *Journal Korean Math. Soc.* **38** (2001), 915–935. MR1849332 (2002f:13039)

[11] P.-J. Cahen and J.-L. Chabert, On the ultrametric Stone-Weierstrass theorem and Mahler's expansion, *Journal de Théorie des Nombres de Bordeaux* **14** (2002), 1–15. MR1925989 (2003g:46086)

[12] L. Carlitz, A note on integral-valued polynomials. *Indag. Math.* **21** (1959), 294–299. MR0108462 (21:7178)

[13] N. G. de Bruijn, Some classes of integer-valued functions, *Indag. Math.* **17** (1955), 363–367. MR0071450 (17:128a)

[14] J. Dieudonné, Sur les fonctions continues *p*-adiques, *Bull. Sci. Math.* 2ème série **68** (1944), 79–95. MR0013142 (7:111c)

[15] J. Fresnel and M. van der Put, *Rigid Analytic Geometry and its Applications*, Birkhäuser, 2004. MR2014891 (2004i:14023)

[16] G. Gerboud, Polynômes à valeurs entières sur l'anneau des entiers de Gauss, *Comptes Rendus Acad. Sci. Paris* **307** (1988) 375-378. MR965801 (89m:11097)

[17] H. Gunji and D. L. McQuillan, Polynomials with integral values, *Proc. Roy. Irish Acad.* **A78** (1978) 1-7. MR0472801 (57:12491)

[18] I. Kaplansky, The Weierstrass theorem in fields with valuations, *Proc. Amer. Math. Soc.* **1** (1950), 356–357. MR0035760 (12:6e)

[19] J. G. Llavona, *Approximation of continuously differentiable functions*, North-Holland Mathematics Studies, vol. 130, North-Holland, Amsterdam, 1986. MR870155 (88f:41001)

[20] K. Mahler, An interpolation series for a continuous function of a *p*-adic variable, *J. reine angew. Math.* **199** (1958), 23-34. MR0095821 (20:2321)

[21] W. Narkiewicz, *Polynomial Mappings*, Springer-Verlag, Berlin, 1995. MR1367962 (97e:11037)

[22] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919) 117-124.

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

[24] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919) 97-116.

[25] W. Schikhof, *Ultrametric Calculus: An Introduction to p-adic Analysis*, Cambridge Stud. Adv. Math., Vol. 4, Cambridge Univ. Press, Cambridge, UK, 1984. MR791759 (86j:11104)

[26] C. de la Vallée-Poussin, Sur l'approximation des fonctions d'une variable réelle et de leurs dérivées par des polynômes et des suites finies de Fourier, *Bull. Acad. Sci. Belgique* (1908), 193–254.

[27] A. Verdoodt, Orthonormal bases for non-Archimedean Banach spaces of continuous functions, *p-adic functional analysis* (Poznań, 1998), 323–331, Lecture Notes in Pure and Appl. Math., 207, Dekker, New York, 1999. MR1703503 (2000h:46095)

[28] C. G. Wagner, Interpolation series for continuous functions on π-adic completions of GF(q, x), *Acta Arith.* **17** (1970/1971), 389–406. MR0282973 (44:207)

[29] C. G. Wagner, Polynomials over GF(q,x) with integral-valued differences, *Arch. Math. (Basel)* **27** (1976), no. 5, 495–501. MR0417137 (54:5197)

[30] K. Weierstrass, Über die analytische Darstellbarkeit sogenannter willkürlicher Functionen einer reellen Veränderlichen, *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin*, 1885 (II).

[31] Z. Yang, Locally analytic functions over completions of $F_r[U]$, *J. Number Theory* **73** (1998), no. 2, 451–458. MR1657996 (99h:11062)

[32] J. Yeramian, *Anneaux de Bhargava*, Ph.D. Thesis, Université Aix-Marseille, 2004.

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08544
E-mail address: bhargava@math.princeton.edu