J. Algebra 211 (1999) 562–577.

INTERPOLATION
by
INTEGER-VALUED POLYNOMIALS

Sophie Frisch

Abstract. Let R be a Krull ring with quotient field K and $a_1, \ldots, a_n$ in R. If and only if the a_i are pairwise incongruent mod every height 1 prime ideal of infinite index in R does there exist for all values $b_1, \ldots, b_n$ in R an interpolating integer-valued polynomial, i.e., an $f \in K[x]$ with $f(a_i) = b_i$ and $f(R) \subseteq R$. If S is an infinite subring of a discrete valuation ring R_v with quotient field K and $a_1, \ldots, a_n$ in S are pairwise incongruent mod all $M_v^k \cap S$ of infinite index in S, we derive a formula (depending on the distribution of the a_i among residue classes of the ideals $M_v^k \cap S$) for the minimal d, such that for all $b_1, \ldots, b_n \in R_v$ there exists a polynomial $f \in K[x]$ of degree at most d with $f(a_i) = b_i$ and $f(S) \subseteq R_v$.

1. *Introduction.*

Suppose D is an integral domain with quotient field K. Unless D is a field, it is not always possible, given $a_0, \ldots, a_n$ (distinct) and $b_1, \ldots, b_n$ in D, to find a polynomial $f \in D[x]$ with $f(a_i) = b_i$. This is so because the function induced on D by a polynomial with coefficients in D must preserve congruences mod every ideal of D. One might say that the next best thing to interpolation with polynomials in $D[x]$ is interpolation with polynomials in $K[x]$ that map every element of D into D and thus induce a function on D.

We will show that this kind of interpolation is possible for arbitrary arguments and values in D whenever D is a Dedekind ring all of whose residue fields are finite, such as the ring of algebraic integers in a number field. (For $D = \mathbb{Z}$ this is easy to see, and for $D = \mathbb{F}_q[x]$ it has been shown by Carlitz [5].)

More generally, we find that distinct elements $a_0, \ldots, a_n$ of a Krull ring R have the property that for all $b_0, \ldots, b_n$ in R there exists a polynomial $f \in K[x]$ with $f(a_i) = b_i$ and $f(R) \subseteq R$ if and only if the a_i are pairwise incongruent mod every height 1 prime ideal P of R with $[R : P] = \infty$.

We use the customary notation $\mathrm{Int}(E, D) = \{f \in K[x] \mid f(E) \subseteq D\}$ and $\mathrm{Int}(D) = \mathrm{Int}(D, D)$, where D is a domain with quotient field K and E a subset of K. A polynomial $f \in K[x]$ that maps E into D is called "integer-valued" on E,

1991 Math. Subj. Classification: Primary 13B25, 11S05, 13G05; Secondary 11B65, 05A10.

following Pólya [15] and Ostrowski [14], who studied $\mathrm{Int}(D)$ where D is the ring of algebraic integers in a number field. More recently, integer-valued polynomials have been investigated by Cahen [2,3], Chabert [6], McQuillan [12,13], Gilmer, Heinzer and Lantz [9], and others. For a survey of the subject, see the monograph by Cahen and Chabert [4].

To interpolate at arguments $a_0, \ldots, a_n$, we use linear combinations of the polynomials $f_k(x) = \prod_{i=0}^{k-1}(x - a_i)/\prod_{i=0}^{k-1}(a_k - a_i), \quad 0 \le k \le n$. For this purpose we introduce, when R is an infinite subring of a discrete valuation ring R_v, special sequences $(a_k) \subseteq R$ that ensure that the polynomials f_k constructed from them are in $\mathrm{Int}(R, R_v)$ and then show how to embed a finite subset of R in a sequence of this kind.

This approach seems justified by the result that the minimal length of such a sequence containing $\alpha_0, \ldots, \alpha_m \in R$ is equal to the minimal d such that for all $\beta_0, \ldots, \beta_m \in R_v$ there exists an $f \in \mathrm{Int}(R, R_v)$ with $f(\alpha_i) = \beta_i$ and $\deg f \le d$. It also yields a formula for this minimal d, depending on the distribution of the α_i among the residue classes of $R \cap M_v^k$ in R.

2. *Sequences.*

In this section, R may be any commutative ring with identity. We denote the set of non-negative integers $\{0, 1, 2, \ldots\}$ by $\mathbb{N}_0$. The kind of sequences below has already been used in [7]; we need to develop some more of their properties.

2.1 Definition. For a set $\mathcal{I}$ of ideals in a commutative ring with identity R, we define a *partial $\mathcal{I}$-sequence* to be an indexed set $(a_n)_{n \in \mathcal{N}}$, with $\mathcal{N} \subseteq \mathbb{N}_0$, of elements in R, such that for all $I \in \mathcal{I}$ and all $n, m \in \mathcal{N}$

$$a_n \equiv a_m \mod I \qquad \Longleftrightarrow \qquad [R:I] \,\big|\, n - m.$$

(If $[R:I]$ is infinite, we regard it as dividing 0, but no other integer.) A partial $\mathcal{I}$-sequence is called an *$\mathcal{I}$-sequence* if $\mathcal{N}$ is an initial segment of $\mathbb{N}_0$.

2.2 Convention. The *length* of a finite partial sequence $(a_n)_{n \in \mathcal{N}}$ is $\max(\mathcal{N})$.

2.3 Proposition. *For every descending chain $\mathcal{I} = \{I_n \mid n \in \mathbb{N}\}$ of ideals in R*

(a) *every finite partial $\mathcal{I}$-sequence can be completed to an $\mathcal{I}$-sequence,*

(b) *every finite $\mathcal{I}$-sequence can be extended to an infinite $\mathcal{I}$-sequence,*

(c) *every finite set $A \subseteq R$ of elements pairwise incongruent mod I_{n+1}, where $[R:I_n]$ is finite, can be embedded in a finite $\mathcal{I}$-sequence, and one of length less than $[R:I_{n+1}]$, if $[R:I_{n+1}]$ is also finite.*

Proof. Given $(a_n)_{n \in \mathcal{N}}$, and $l \ge \max(\mathcal{N})$, we show how to complete (a_n) to an $\mathcal{I}$-sequence of length l. General principle: For a finite sequence of length l to be an $\mathcal{I}$-sequence ($\mathcal{I}$ being a descending chain of ideals), it suffices that it satisfy the requirements with respect to $I_1, \dots, I_k$, if k satisfies $[R:I_k] > l$ or for all $m \geq k$, $I_m = I_k$.

Case 1: there exists I_k of finite index with $[R:I_k] > l$ or $I_m = I_k$ for $m \geq k$. For $j = 1, \dots, k$ inductively, we assign a different residue class of I_j in R to every residue class mod $[R:I_j]$ in $\mathbb{Z}$ such that 1) for all $n \in \mathcal{N}$, $n + [R:I_j]\mathbb{Z}$ is assigned $a_n + I_j$ (this is consistent because $(a_n)_{n\in\mathcal{N}}$ is a partial $\mathcal{I}$-sequence) and 2) if $r + I_{j-1}$ was assigned to $m + [R:I_{j-1}]\mathbb{Z}$, then the residue classes of I_j in $r + I_{j-1}$ are assigned to the residue classes of $[R:I_j]\mathbb{Z}$ in $m + [R:I_{j-1}]\mathbb{Z}$.

Case 2: there is I_{k-1} with $[R:I_{k-1}] < l$ and $[R:I_k] = \infty$. We proceed as above for $j = 0, \dots, k-1$ and then assign a different residue class of I_k to every $n \leq l$, $n \in \mathbb{N}_0$, such that 1) every $n \in \mathcal{N}$ is assigned $a_n + I_k$ and 2) if $r + I_{k-1}$ was assigned to $m + [R:I_{k-1}]\mathbb{Z}$, every $n \in m + [R:I_{k-1}]\mathbb{Z}$ is assigned a residue class of I_k in $r + I_{k-1}$.

We now define sequence elements for indices $m \notin \mathcal{N}$, $0 \leq m \leq l$, by choosing a_m from the residue class of I_k assigned to $m + [R:I_k]\mathbb{Z}$ (in case 1) or to m (in case 2). The resulting sequence $(a_n)_{n=0}^l$ satisfies the $\mathcal{I}$-sequence requirements with respect to $I_1, \dots I_k$, which is all we need by the general principle stated above. We can extend $(a_n)_{n=0}^l$ to an $\mathcal{I}$-sequence of length $l' > l$, and inductively to an infinite $\mathcal{I}$-sequence by iterating the construction. This shows (a) and (b). It also shows that $\mathcal{I}$-sequences of arbitrary length exist, since we can start with any $a_0 \in R$ and extend it to an infinite $\mathcal{I}$-sequence.

For (c), if $[R:I_{n+1}]$ is finite, we take an $\mathcal{I}$-sequence of length $[R:I_{n+1}] - 1$ and swap every member of A with the unique sequence element congruent to it mod I_{n+1}. Otherwise, we take an $\mathcal{I}$-sequence of length $c \cdot [R:I_n] - 1$, c being the maximal number of elements of A in any residue class of I_n, and swap every $a \in A$ with a sequence element in $a + I_n$, choosing the one in $a + I_{n+1}$, if such exists. $\square$

2.4 Definition. For a set $\mathcal{I}$ of ideals in a commutative ring with identity R, we define a *weak $\mathcal{I}$-sequence* to be a sequence $(a_n)_{n\in\mathcal{N}}$, where $\mathcal{N}$ is an initial segment of $\mathbb{N}_0$, such that for all $I \in \mathcal{I}$ and all $k \geq 0$ the sequence elements a_i with $k[R:I] \leq i < (k+1)[R:I]$ are pairwise incongruent mod I. (For infinite $[R:I]$, we use the convention $0[R:I] = 0$.)

We could also define partial weak $\mathcal{I}$-sequences and show an analogue of Proposition 2.3, but we will not need this. To compare $\mathcal{I}$-sequences and weak $\mathcal{I}$-sequences, we note that

1) An infinite sequence is an $\mathcal{I}$-sequence if and only if for every $I \in \mathcal{I}$ of finite index, every $[R:I]$ consecutive terms of the sequence form a complete system of residues mod I and the terms of the sequence are pairwise incongruent mod every $I \in \mathcal{I}$ of infinite index.
2) An infinite sequence is a *weak* $\mathcal{I}$-sequence if and only if for every $I \in \mathcal{I}$ of finite index, every $[R:I]$ consecutive terms of the sequence *starting at an index divisible by $[R:I]$* form a complete system of residues mod I and the terms of the sequence are pairwise incongruent mod every $I \in \mathcal{I}$ of infinite index.

2.5 Example. In the ring of integers $\mathbb{Z}$, for every fixed $k \in \mathbb{Z}$, the sequence $a_n = k+n$ for $n \geq 0$ is an $\mathcal{I}$-sequence for the set of all ideals of $\mathbb{Z}$.

2.6 Example. If $\mathbb{F}_q$ is the finite field of order q then a weak $\mathcal{I}$-sequence for the set of all ideals of $\mathbb{F}_q[x]$ that runs through $\mathbb{F}_q[x]$ bijectively can be constructed as follows (Wagner [16], see also Amice [1]): Let $\mathbb{F}_q = \{r_0, \ldots, r_{q-1}\}$, where $r_0 = 0$. If $n = \sum_{i=0}^{N} c_i q^i$ with $0 \leq c_i < q$, set $a_n = \sum_{i=0}^{N} r_{c_i} x^i$. This is a weak $\mathcal{I}$-sequence, since $a_0, \ldots, a_{q^m-1}$ are precisely the elements of $\mathbb{F}_q[x]$ of degree less than m and thus form a system of residues mod every ideal generated by an element of degree m, and the q^m sequence elements starting at index kq^m (with $0 \leq k < q$) are just the first q^m elements shifted by $r_k x^m$: $a_{kq^m} = r_k x^m + a_0, \ \ldots, \ a_{(k+1)q^m-1} = r_k x^m + a_{q^m-1}$.

2.7 Example. An infinite $\mathcal{I}$-sequence exists for every descending chain $\mathcal{I}$ of ideals in a ring R. (Apply Proposition 2.3 (b) to $a_0 = 0$.) If R is a countably infinite ring and $\mathcal{I}$ a descending chain of ideals of finite index in R with $\bigcap_{n \in \mathbb{N}} I_n = (0)$ then there exists an $\mathcal{I}$-sequence that runs through R bijectively [8].

3. *Binomial Polynomials.*

Let R_v be a discrete valuation ring (with value group $\mathbb{Z}$ and $v(0) = \infty$), M_v its maximal ideal, K its quotient field and R an infinite subring of R_v. (Throughout this paper, discrete valuation always means discrete rank one valuation.) We will define some useful polynomials in $\mathrm{Int}(R, R_v)$, which are modeled after the polynomials

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

in $\mathrm{Int}(\mathbb{Z})$ and which we therefore call "binomial polynomials". These polynomials were introduced in [7], generalizing a construction of Pólya [15] that has also been employed by Cahen [3], Gunji and McQuillan [10,12] and others. The sequence a_i of elements of R that will replace the sequence of natural numbers in the definition of the binomial polynomials will have to be nicely distributed with respect to the residue classes of $R \cap M_v^n$ in R, in the following sense:

3.1 Definition. A [*partial*] *v-sequence for R* is a [partial] $\mathcal{I}$-sequence with $\mathcal{I} = \{{M_v}^n \cap R \mid n \in \mathbb{N}\}$. In other words, $(a_n)_{n \in \mathcal{N}} \subseteq R$ is a partial v-sequence for R if and only if for all $n \in \mathbb{N}$ and all $i, j \in \mathcal{N}$,

$$v(a_i - a_j) \geq n \quad \iff \quad [R : {M_v}^n \cap R] \mid i - j\,.$$

Similarly, a *weak v-sequence for R* is defined to be a weak $\mathcal{I}$-sequence with $\mathcal{I} = \{{M_v}^n \cap R \mid n \in \mathbb{N}\}$. In other words, $(a_n)_{n \geq 0}$ is a weak v-sequence for R if and only if for all $n \in \mathbb{N}$ and all i, j and $k \in \mathbb{N}_0$,

$$k\,[R : {M_v}^n \cap R] \leq i < j < (k+1)\,[R : {M_v}^n \cap R] \quad \Longrightarrow \quad v(a_i - a_j) < n$$

(If $[R\colon {M_v}^n \cap R]$ is infinite, the elements of a [partial, weak] v-sequence for R must be pairwise incongruent mod ${M_v}^n \cap R$.)

For brevity, we write I_n for ${M_v}^n \cap R$ from this point on.

Note that by the Krull Intersection Theorem, $\bigcap_{k=0}^{\infty} I_k = (0)$. Therefore, there exists for every finite subset A of R an $n \in \mathbb{N}$ such that distinct elements of A are incongruent mod I_n. Since R is infinite, the indices $[R\colon I_k]$ grow arbitrarily large or are infinite from some k on.

3.2 Definition. The *binomial polynomials* constructed from a weak v-sequence (a_n) are

$$f_0 = 1 \qquad \text{and} \qquad f_n(x) = \frac{\prod_{i=0}^{n-1}(x - a_i)}{\prod_{i=0}^{n-1}(a_n - a_i)} \quad \text{for } n > 0.$$

3.3 Proposition. *Let $(a_i)_{i=0}^m$ be a weak v-sequence for R and $(f_i)_{i=0}^m$ the binomial polynomials constructed from it. For $j, k \in \mathbb{N}_0$ let $r_j(k)$ be the remainder of k under integral division by $[R\colon I_j]$, if $[R\colon I_j]$ is finite, and $r_j(k) = k$ otherwise. Then for all $r \in R$ and $0 \le k \le m$*

(a) $v(f_k(r)) = \left|\{j \ge 1 \mid r \equiv a_l \mod I_j \text{ for some } l \text{ with } k - r_j(k) \le l < k\}\right|$,

(b) *in particular,* $f_k \in \mathrm{Int}(R, R_v)$.

Proof. Let $g_k(x) = \prod_{i=0}^{k-1}(x - a_i)$, then $v(f_k(r)) = v(g_k(r)) - v(g_k(a_k))$. For any $s \in R$, $v(g_k(s)) = \sum_{j\ge 1} \left|\{i \mid 0 \le i < k,\ s \equiv a_i \mod I_j\}\right|$. Let $q_j(r) = \left[\frac{k}{[R:I_j]}\right]$, then $k = q_j(k)[R\colon I_j] + r_j(k)$, and the sequence $a_0, \ldots, a_{k-1}$ consists of $q_j(r)$ complete systems of residues mod I_j comprising $a_0, \ldots, a_{k-r_j(k)-1}$ and $r_j(k)$ extra terms a_l for $k - r_j(k) \le l < k$, pairwise incongruent mod I_j.

Now $\left|\{i \mid 0 \le i < k,\ s \equiv a_i \mod I_j\}\right|$ is either $q_j(k)$ or $q_j(k) + 1$, the latter being the case if and only if s is congruent mod I_j to one of the elements a_l with $k - r_j(k) \le l < k$. This extra $+1$ never occurs with $s = a_k$, since a_k is not congruent to any a_l with $k - r_j(k) \le l < k$ by definition of weak v-sequence. □

3.4 Remark. It is easy to see that the binomial polynomials f_k constructed from a weak v-sequence (a_i) for R, where R is an infinite subring of a discrete valuation ring R_v, give a basis of the free R_v-module $\mathrm{Int}(R, R_v)$, cf. [7]. Indeed, $\deg f_k = k$ shows that the f_k are a K-basis of $K[x]$. Since they are in $\mathrm{Int}(R, R_v)$, they form a basis of a free R_v-module $F \subseteq \mathrm{Int}(R, R_v)$. To see $\mathrm{Int}(R, R_v) \subseteq F$, consider $f = \sum d_k f_k$ with $d_k \in K$. A simple induction shows that for $f \in \mathrm{Int}(R, R_v)$ the d_k are actually in R_v: $d_0 = f(a_0)$, and $d_k = f(a_k) - \sum_{i=0}^{k-1} d_i f_i(a_k)$ (by the facts that $f_k(a_k) = 1$ and $f_j(a_k) = 0$ for $j > k$). The last argument also shows that for a polynomial $f \in K[x]$ with $\deg f < m$ to be in $\mathrm{Int}(R, R_v)$ it suffices that $f(a_i) \in R_v$ for $0 \le i < m$.

If a domain S with quotient field K is the intersection of a family of discrete valuation rings in K, $S = \bigcap_{v \in \mathcal{V}} R_v$, then for every subring R of S we have

$\mathrm{Int}(R,S) = \bigcap_{v\in\mathcal{V}} \mathrm{Int}(R,R_v)$. In particular this holds if S is a Krull ring and $\mathcal{V}$ the set of its essential valuations.

3.5 Theorem. *Let R be an infinite subring of a Krull ring S. If $a_0,\dots,a_n \in R$ is a weak v-sequence for R for all essential valuations v of S simultaneously then for all $b_0,\dots,b_n \in S$ there exists $f \in \mathrm{Int}(R,S)$ with $f(a_i) = b_i$ $(0 \le i \le n)$ and $\deg f \le n$.*

Proof. Let $(f_i)_{i=0}^n$ be the binomial polynomials constructed from $(a_i)_{i=0}^n$. For every essential valuation v of S, we know from Proposition 3.3 (b) that the f_i, and therefore R_v-linear combinations of them, are in $\mathrm{Int}(R,R_v)$. Therefore S-linear combinations of the f_i are in $\bigcap_v \mathrm{Int}(R,R_v) = \mathrm{Int}(R,S)$. We define coefficients $d_k \in S$ inductively, such that $f = \sum_{k=0}^n d_k f_k$ maps a_i to b_i for $0 \le i \le n$: let $d_0 = b_0$, and $d_m = b_m - \sum_{k=0}^{m-1} d_k f_k(a_m)$. Since $f_k(a_k) = 1$ and $f_m(a_k) = 0$ for $m > k$, we get $f(a_m) = d_m + \sum_{k=0}^{m-1} d_k f_k(a_m) = b_m$ as required. □

3.6 Corollary. *(Carlitz [5]) Let $\alpha_1,\dots,\alpha_k$ be distinct elements of $\mathbb{F}_q[x]$ and $d = \max_{1\le i\le k} \deg_x \alpha_i$. Then for all $\beta_1,\dots,\beta_k \in \mathbb{F}_q[x]$ there exists $f(t) \in \mathrm{Int}(\mathbb{F}_q[x])$ with $\deg_t f < q^d$ and $f(\alpha_i) = \beta_i$ for $i = 1,\dots,k$.*

Proof. Wagner's sequence (Example 2.6) is a weak $\mathcal{I}$-sequence for the set of all ideals of $\mathbb{F}_q[x]$ and therefore a fortiori a weak v-sequence for all essential valuations of $\mathbb{F}_q[x]$. Its initial segment $a_0,\dots,a_{q^d-1}$ consists of all elements of $\mathbb{F}_q[x]$ of degree at most d, with $\alpha_1,\dots,\alpha_k$ among them. □

Carlitz proved this by showing that a polynomial $f \in \mathbb{F}_q(x)[t]$ with $\deg_t(f) < q^m$ is in $\mathrm{Int}(\mathbb{F}_q[x])$ if and only if it maps all $\alpha \in \mathbb{F}_q[x]$ with $\deg_x(\alpha) < m$ to values in $\mathbb{F}_q[x]$ ([5] Theorem 7.1). Since there are q^m elements of degree less than m in $\mathbb{F}_q[x]$, the Lagrange interpolation polynomial for these arguments will be of degree $q^m - 1$ or less and will therefore be in $\mathrm{Int}(\mathbb{F}_q[x])$ provided the values prescribed for the q^m arguments are in $\mathbb{F}_q[x]$. To relate Carlitz's proof to the one using Wagner's sequence, note that a polynomial $f \in K[x]$ with $\deg f < m$ that takes values $f(a_i) \in R_v$ on a v-sequence $a_0,\dots,a_{m-1}$ for R is (by the argument in 3.4) an R_v-linear combination of the binomial polynomials $f_0,\dots,f_{m-1}$ constructed from the v-sequence and therefore in $\mathrm{Int}(R,R_v)$.

Unfortunately, weak v-sequences for all essential valuations of a Krull ring simultaneously seem to be rare, and we will use a different approach to interpolation with integer-valued polynomials on Krull rings in section 6.

Locally, however, we can use v-sequences to construct interpolating integer-valued polynomials as follows: Let $\alpha_1,\dots,\alpha_k$ be elements of an infinite subring R of a discrete valuation ring R_v that are pairwise incongruent mod all $M_v^n \cap R$ of infinite index in R. By Proposition 2.3, $\alpha_1,\dots,\alpha_k$ can be embedded in a v-sequence $a_0,\dots,a_\ell$. Therefore there exists for arbitrary values $\beta_1,\dots,\beta_k \in R_v$ an $f \in \mathrm{Int}(R,R_v)$ with $\deg f \le \ell$ that maps α_i to β_i, by Theorem 3.5.

In section 5 we will see that the minimal length ℓ of a v-sequence for R containing $\alpha_1,\dots,\alpha_k$ coincides with the minimal d such that for arbitrary values

$\beta_1, \ldots, \beta_k$ in R_v there exists an $f \in \mathrm{Int}(R, R_v)$ with $\deg f \le d$ that maps α_i to β_i; so that, in a sense, interpolation by polynomials in $\mathrm{Int}(R, R_v)$ using v-sequences yields interpolation polynomials of best possible degree.

4. *Embedding sets in v-sequences of minimal length.*

As before, R is an infinite subring of a discrete valuation ring R_v, $I_n = M_v^n \cap R$ and $\mathcal{I} = \{I_n \mid n \ge 0\}$. Recall that the length of a sequence $(a_i)_{i=0}^n$ is n, by convention.

4.1 Definition. Let A be a finite subset of R.

1. We define $d(A)$ to be the minimal $d \in \mathbb{N}_0$ such that for every choice of values $r_a \in R_v$ for $a \in A$ there exists $f \in \mathrm{Int}(R, R_v)$ with $f(a) = r_a$ for all $a \in A$ and $\deg f \le d$, if such a d exists; otherwise $d(A) = \infty$.
2. If A is not embeddable in any v-sequence in R then $\ell(A) = \infty$; otherwise we define $\ell(A)$ to be the minimal ℓ such that there exists a v-sequence $a_0, \ldots, a_\ell$ in R containing A.

4.2 Corollary to Theorem 3.5. *For every finite subset A of R, $d(A) \le \ell(A)$.*

We will show that $d(A) = \ell(A)$ in section 5; but before, we want to derive a formula for $\ell(A)$. In order to do this, we first consider sets that have a simple structure with respect to the chain of ideals $I_n = {M_v}^n \cap R$, $n \ge 0$.

4.3 Definition. We call a non-empty set $L \subseteq R$ an *$\mathcal{I}$-lattice* of dimensions $(d_k)_{k\ge0}$ if, for all $k \ge 0$, L intersects exactly d_k residue classes of I_{k+1} in every residue class of I_k that it intersects. If L is finite, then $d_k = 1$ for all but finitely many k, and we speak of dimensions $d_0, \ldots, d_n$, meaning $d_k = 1$ for $k > n$.

4.4 Definition. To every finite set $A \subseteq R$ whose elements are pairwise incongruent mod I_{n+1}, where $[R : I_n]$ is finite, we associate *dimensions* $(d_k)_{k\ge0}$ and an $\mathcal{I}$-lattice $L_A \subseteq A$, the *spanning lattice* of A, inductively as follows:

- $L_n = A$ and $d_k = 1$ for $k > n$,
- d_k is the maximal number of residue classes of I_{k+1} that L_k intersects in any residue class of I_k, for $0 \le k \le n$;
- L_{k-1} consists of the elements of L_k in those residue classes of I_k that L_k intersects in d_k residue classes of I_{k+1}, for $1 \le k \le n$;

and L_A is L_0, which is easily seen to be an $\mathcal{I}$-lattice of dimensions $d_0, \ldots, d_n$.

The minimal length of a v-sequence into which a finite set can be embedded is most conveniently expressed in the mixed radix number system given by the sequence $[R : I_l]$, $l \ge 0$:

Every $n \in \mathbb{N}_0$ has a unique representation $n = \sum_{l=0}^{\infty} \varepsilon_l(n)[R : I_l]$, where $0 \le \varepsilon_l(n) < [I_l : I_{l+1}]$. Addition of numbers is performed by addition with carry on the vectors of digits, where a carry from position l to position $l+1$ occurs when the l-th digit reaches or exceeds $[I_l : I_{l+1}]$. We will call this the $\mathcal{I}$-ary number system and $\varepsilon_l(n)$ the l-th digit in the $\mathcal{I}$-ary representation of n.

If $[R_v : M_v]$ is finite, then $[I_l : I_{l+1}]$ divides $[{M_n}^l : {M_v}^{l+1}] = [R_v : M_v]$; if $[R_v : M_v]$ is infinite, however, the digits need not be uniformly bounded or even bounded at all. If infinite indices $[R : I_l]$ occur, the system is somewhat degenerate, with $0 \le \varepsilon_N(n) < \infty$ for the maximal $N \in \mathbb{N}_0$ with $[R : I_N]$ finite and $\varepsilon_l(n) = 0$ for all n, if $l > N$. (We use the convention that $0 \cdot [R : I_l] = 0$ even if $[R : I_l] = \infty$.)

Recall that by Proposition 2.3 (a) every partial v-sequence can be completed to a v-sequence of the same length. Therefore, $\ell(A)$ is equal to the minimal ℓ such that A can be arranged as a partial v-sequence of length ℓ.

4.5 Lemma. *Let L be an $\mathcal{I}$-lattice of dimensions $d_0, \ldots, d_m$, with $[R : I_m]$ finite. For every partial v-sequence $(l_n)_{n \in \mathcal{N}}$ of minimal length formed by L, we have $\mathcal{N} = \{n \in \mathbb{N}_0 \mid \varepsilon_i(n) < d_i$ for all $i\}$. Consequently, $\ell(L) = \sum_{k=0}^{m} (d_k - 1)[R : I_k]$.*

Proof. Induction on m. For $m = 0$, L consists of d_0 elements mutually incongruent modulo I_1. Any shortest partial v-sequence is just a listing of the elements of L, in any order, as $l_0, \ldots, l_{d_0 - 1}$, therefore $\mathcal{N} = \{0, \ldots, d_0 - 1\}$ and $\ell(L) = d_0 - 1$.

Now let L be an $\mathcal{I}$-lattice of dimensions $d_0, \ldots, d_m$, $m > 0$. We can arrange L as a partial v-sequence with index set $\mathcal{N} = \{n \in \mathbb{N}_0 \mid \forall i \quad \varepsilon_i(n) < d_i\}$ as follows: Choose a system of representatives $L' \subseteq L$ of the residue classes of I_m that L intersects. L' is an $\mathcal{I}$-lattice of dimensions $d_0, \ldots, d_{m-1}$. Arrange L' as a partial v-sequence $(l_n)_{n \in \mathcal{N}'}$ of minimal length and for each $n \in \mathcal{N}'$ assign indices $n + j[R : I_m]$, $j = 1, \ldots, d_m - 1$ to the elements of $L \setminus L'$ in $l_n + I_m$. Since by induction hypothesis $\mathcal{N}'$ is the set of all $n = \sum_{j=0}^{m-1} k_j [R : I_j]$ with $0 \le k_j < d_j$, $\mathcal{N}$ is the set of all $n = \sum_{j=0}^{m} k_j [R : I_j]$ with $0 \le k_j < d_j$. The length of this partial v-sequence is $\max(\mathcal{N}) = \sum_{k=0}^{m} (d_k - 1)[R : I_k]$.

Now, given any v-sequence of minimal length $(l_n)_{n \in \mathcal{N}}$ formed by L, we show that it must be of this kind: From every residue class of I_m that L intersects, take the element of lowest index. These elements form a lattice L' of dimensions $d_0, \ldots, d_{m-1}$, arranged as a partial v-sequence with index set $\mathcal{N}' \subseteq \mathcal{N}$. The indices of the d_m elements of L in each residue class of I_m are part of an arithmetic progression of period $[R : I_m]$ starting at $n \in \mathcal{N}'$. If, for some $n \in \mathcal{N}'$, the elements of L in $l_n + I_m$ do not have indices $n + j[R : I_m]$, $j = 0, \ldots, d_m - 1$, then some index is at least $n + d_m[R : I_m] \ge d_m[R : I_m] > \sum_{k=0}^{m} (d_k - 1)[R : I_k]$, which is more than the length of the sequence constructed earlier. Therefore, we must have $\mathcal{N} = \{n + j[I : I_m] \mid n \in \mathcal{N}',\ 0 \le j < d_m\}$, the length of the sequence being $\max(\mathcal{N}') + (d_m - 1)[R : I_m]$. This is minimal only if $\max(\mathcal{N}')$ is minimal, i.e., if L' forms a partial v-sequence of minimal length. □

4.6 Theorem. *Let $A \subseteq R$ be a finite set whose elements are pairwise incongruent mod I_{n+1}, where $[R : I_n]$ is finite, and $d_0, \ldots, d_n$ the dimensions of A. Then $\ell(A) = \sum_{j=0}^{n} (d_j - 1)[R : I_j]$.*

Proof. We know $\ell(A) \ge \ell(L_A) = \sum_{j=0}^{n} (d_j - 1)[R : I_j]$. By Proposition 2.3 (a) it suffices to arrange A as a partial v-sequence of length $\sum_{j=0}^{n} (d_j - 1)[R : I_j]$. We define a chain of subsets of A that allows us to do this inductively. Let $A_n = A$ and for $0 < k \le n$ let $A_{k-1} \subseteq A_k$ be a system of representatives of those residue classes of I_k that A_k intersects in the maximal number of elements. It is clear that this maximal number is d_k. A_0 consists of d_0 elements mutually incongruent mod I_1. Listing A_0 as $a_0, \dots, a_{d_0-1}$ in any order makes A_0 into a partial v-sequence of length $d_0 - 1$. Assuming we have arranged A_{k-1} as a partial v-sequence $(a_n)_{n\in\mathcal{N}}$ of length $\sum_{j=0}^{k-1}(d_j - 1)[R : I_j]$, we will extend it to an arrangement of A_k as a partial v-sequence of length $\sum_{j=0}^{k}(d_j - 1)[R : I_j]$.

A_k contains d_k elements in $a_n + I_k$ for each $n \in \mathcal{N}$, plus less than d_k elements each in some further residue classes of I_k. Let $B \subseteq A_k$ be a system of representatives of these further classes. By considering a completion of $(a_n)_{n\in\mathcal{N}}$ to a v-sequence of length $[R : I_k] - 1$ (which exists by Proposition 2.3) and assigning each $b \in B$ the index of the unique sequence element congruent to it mod I_k, we get a partial v-sequence arrangement of $A_{k-1} \cup B$ of length less than $[R : I_k]$. We assign consecutive indices in an arithmetic progression of period $[R : I_k]$, starting at the representative in $A_{k-1} \cup B$, to the elements of A_k in each residue class of I_k. The highest index in this partial v-sequence arrangement of A_k is the highest index in a progression starting at a representative in A_{k-1}, namely $\max(\mathcal{N}) + (d_k - 1)[R : I_k] = \sum_{j=0}^{k}(d_j - 1)[R : I_j]$, since a progression starting at $b \in B$ with index $n < [R : I_k]$ and containing the $l < d_k$ elements of $(b + I_k) \cap A_k$ only reaches index $n + (l - 1)[R : I_k] < l[R : I_k] \le (d_k - 1)[R : I_k]$. □

5. *The degree of the interpolating polynomial.*

If $n = \sum_{l=0}^{\infty} \varepsilon_l(n)[R:I_l]$ with $0 \le \varepsilon_l(n) < [I_l : I_{l+1}]$, we set $r_j(n) = \sum_{l=0}^{j-1} \varepsilon_l(n)[R:I_l]$. This is consistent with our earlier convention that $r_j(n)$ is the remainder of n under integral division by $[R : I_j]$ if $[R : I_j]$ is finite, and $r_j(n) = n$ otherwise.

5.1 Proposition. *Let (a_n) be a v-sequence for R (of length at least k) and f_k the binomial polynomial of degree k constructed from it. Then*

(a) $v(f_k(a_n)) = \left|\{l \ge 1 \mid r_l(k) > r_l(n)\}\right|$,

(b) $v(f_k(a_n)) = 0 \iff \forall\, l \;\; \varepsilon_l(k) \le \varepsilon_l(n)$.

Proof. (a) is true for $k > n$, since then $v(f_k(a_n)) = v(0) = \infty$ and there are infinitely many l with $r_l(k) = k > n = r_l(n)$. (The indices $[R : I_l]$ are unbounded because R is infinite and $\bigcap_{l\ge 0} I_l = (0)$.) Now assume $k \le n$.

$a_n \equiv a_i \bmod I_l$ for at most one i with $k - r_l(k) \le i < k - r_l(k) + [R:I_l]$, by definition of weak v-sequence. Since (a_n) is really a v-sequence and $n \equiv k - r_l(k) + r_l(n) \bmod [R:I_l]$, we know that $a_n \equiv a_{k-r_l(k)+r_l(n)} \bmod I_l$. The condition $a_n \equiv a_i \bmod I_l$ for some i with $k - r_l(k) \le i < k$ is therefore equivalent to $r_l(k) > r_l(n)$, such that (a) follows from Proposition 3.3 (a).

If $r_l(k) > r_l(n)$ then $\exists m \le l$ with $\varepsilon_m(k) > \varepsilon_m(n)$ and if $\varepsilon_m(k) > \varepsilon_m(n)$ then $r_m(k) > r_m(n)$. Therefore, $\forall l \;\; r_l(k) \le r_l(n)$, which is equivalent to $v(f_k(a_n)) = 0$ by (a), is equivalent to $\forall\, l \;\; \varepsilon_l(k) \le \varepsilon_l(n)$. Thus (b) follows from (a). □

From Proposition 5.1 one can easily derive that $v(f_k(a_n))$ equals the number of carries that occur in the addition of k and $n-k$ in the $\mathcal{I}$-ary number system. For $a_n=n$ and $v=v_p$ this is Kummer's result [11] that the exact power of p dividing the binomial coefficient $\binom{n}{k}$ equals the number of carries that occur in the addition of k and $n-k$ in base p arithmetic. Kummer's expression of $v_p(\binom{n}{k})$ in terms of the digits of n, k and $n-k$ in base p also generalizes, provided $[I_n:I_{n+1}]=[R:I_1]$ for all n, cf. [8].

5.2 Lemma. *For $n \geq 0$, let $I_n = M_v^n \cap R$. If $[R:I_n]=\infty$ and a, $b \in R$ are congruent mod I_{n+m}, $m \geq 0$, then $f(b) \equiv f(a) \mod I_{m+1}$ for all $f \in \mathrm{Int}(R,R_v)$.*

Proof. Extend $a=a_0$ to an infinite v-sequence $(a_k)_{k=0}^{\infty}$ for R and construct binomial polynomials $f_k \in \mathrm{Int}(R,R_v)$ from it. Let $f \in \mathrm{Int}(R,R_v)$, then $f=\sum_{k\geq 0} d_k f_k$ with $d_k \in R_v$, since the f_k are an R_v-basis of $\mathrm{Int}(R,R_v)$. Also, $d_0=f(a_0)=f(a)$.

By Proposition 3.3, $v(f_k(b))$ equals the number of $j \geq 1$ such that for some l with $k-r_j(k) \leq l < k$, $b \equiv a_l \mod I_j$. For $k>0$, every j with $n \leq j \leq n+m$ satisfies this condition, because $b \equiv a_0 \mod I_j$ and $r_j(k)=k$. We see that $v(f_k(b)) \geq m+1$ for all $k>0$. Therefore $f(b) \equiv d_0 f_0 = d_0 = f(a) \mod I_{m+1}$. □

5.3 Corollary. *Let $\alpha_1, \dots, \alpha_n \in R$. Only if the α_i are pairwise incongruent mod all $I_n = M_v^n \cap R$ with $[R:I_n]=\infty$ can there exist for all $\beta_1, \dots, \beta_n \in R_v$ an $f \in \mathrm{Int}(R,R_v)$ with $f(\alpha_i)=\beta_i$.*

5.4 Lemma. *Let L be a finite $\mathcal{I}$-lattice embedded in a v-sequence $a_0, \dots, a_l$ of minimal length $l=\ell(L)$, as $L=\{a_n \mid n \in \mathcal{N}\}$, and $(f_k)_{k=0}^{l}$ the binomial polynomials constructed from $a_0, \dots, a_l$. If $n \in \mathcal{N}$ and $k \notin \mathcal{N}$ then $v(f_k(a_n))>0$.*

Proof. If $k \notin \mathcal{N}$ then $\varepsilon_i(k) \geq d_i > \varepsilon_i(n)$ for some i by Lemma 4.5; therefore $v(f_k(a_n))>0$ by Proposition 5.1. □

5.5 Remark. If A is a finite subset of R then $d(A)$ is finite if and only if the elements of A are pairwise incongruent mod all $I_n = M_v^n \cap R$ with $[R:I_n]=\infty$ and $\ell(A)$ is finite under precisely the same conditions: We know from Theorem 3.5 that $d(A) \leq \ell(A)$. Now if a, $b \in A$ are congruent mod I_n with $[R:I_n]=\infty$ then by Lemma 5.2 there does not exist $f \in \mathrm{Int}(R,R_v)$ with $f(a)=0$ and $f(b)=1$, so $d(A)=\infty$. Conversely, if the elements of A are pairwise incongruent mod all I_n of infinite index then $\ell(A)$ is finite by Theorem 4.6.

5.6 Theorem. *For every finite subset A of R, $d(A)=\ell(A)$.*

Proof. $d(A)$ and $\ell(A)$ are each finite if and only if A is a finite set that does not contain two elements congruent mod any $I_n = M_v^n \cap R$ of infinite index. Let A be such a set. In view of Theorem 3.5, we need only show $d(A) \geq \ell(A)$. Let $a_0, \dots, a_l$ be a v-sequence containing A with $l=\ell(A)$. By Lemma 4.5, this is also the minimal length for a v-sequence containing the spanning lattice L of A, therefore $a_0 \in L$ and $a_l \in L$ (otherwise we could chop off the ends of the sequence and re-index starting with 0 to get a shorter v-sequence containing L). Let the sequence $(a_j)_{j=0}^{l}$ be extended to an infinite v-sequence and let f_j be the binomial polynomial of degree j constructed from it.

Suppose $f \in \mathrm{Int}(R, R_v)$ with $f(a_l) = 1$ and $f(a_i) = 0$ for all $a_i \in L$ with $i < l$; we claim that $\deg f \geq l$. The f_j form an R_v-basis of $\mathrm{Int}(R, R_v)$, so $f = \sum_{j \geq 0} d_j f_j$ with $d_j \in R_v$. We show for $k \leq l$ that if $a_k \in L$ then $d_k \equiv \delta_{k,l} \bmod I_1$. Induction on k: if $k = 0$ then $d_0 = f(a_0) = \delta_{0,l}$. For any k with $a_k \in L$, every $j < k$ satisfies (by Lemma 5.4) either $a_j \in L$, in which case $d_j \equiv 0 \bmod I_1$ by induction hypothesis, or $f_j(a_k) \in I_1$. Therefore $f(a_k) = d_k + \sum_{j=0}^{k-1} d_j f_j(a_k)$ shows $d_k \equiv f(a_k) = \delta_{k,l} \bmod I_1$. In particular, we have shown $d_l \neq 0$, which implies $\deg f \geq l$. □

We combine this with the formula for $\ell(A)$ from Theorem 4.6 and the corollary to Lemma 5.2. (The dimensions of a finite subset of R are defined in 4.4.)

5.7 Corollary. *Let R be an infinite subring of a discrete valuation ring R_v, $I_n = M_v^n \cap R$ and $\alpha_1, \ldots, \alpha_k$ (distinct) in R.*

1. *If and only if the α_i are pairwise incongruent mod all I_n of infinite index in R there exists for all $\beta_1, \ldots, \beta_k \in R_v$ an $f \in \mathrm{Int}(R, R_v)$ with $f(\alpha_i) = \beta_i$.*
2. *In that case, the minimal d such that for all $\beta_1, \ldots, \beta_k \in R_v$ there exists an $f \in \mathrm{Int}(R, R_v)$ with $f(\alpha_i) = \beta_i$ and $\deg f \leq d$, is $d = \sum_{j=0}^{n} (d_j - 1)[R : I_j]$, where $d_0, \ldots, d_n$ are the dimensions of the set $\{\alpha_1, \ldots, \alpha_k\}$.*

6. *Interpolation by integer-valued polynomials on Krull rings*

We now turn to Krull rings and characterize those arguments $r_1, \ldots, r_n \in R$ that for every choice of values $s_1, \ldots, s_n \in R$ admit an interpolating polynomial $f \in \mathrm{Int}(R)$. We denote the set of prime ideals of height 1 in R by $\mathrm{Spec}^1(R)$.

6.1 Lemma. *Let v be a discrete valuation on a field K. Suppose $f = \sum_{k=0}^{n} a_k x^k$ in $K[x]$ splits over K as $f(x) = a_n(x - b_1) \ldots (x - b_m)(x - c_1) \ldots (x - c_l)$, where $v(b_i) < 0$ and $v(c_i) \geq 0$. Let $\mu = \min_{0 \leq k \leq n} v(a_k)$ and set $f_+(x) = (x - c_1) \ldots (x - c_l)$ then $v\big(f(r)\big) = \mu + v\big(f_+(r)\big)$ for all $r \in R_v$.*

Proof. If $r \in R_v$, $v(r - b_i) = v(b_i)$ and $v\big(f(r)\big) = v(a_n) + \sum_{i=1}^{m} v(b_i) + v\big(f_+(r)\big)$. We will show that $\sum_{i=1}^{m} v(b_i) = \mu - v(a_n)$. Let $a_n^{-1} f(x) = x^n + a'_{n-1} x^{n-1} + \ldots + a'_0$ then $\mu - v(a_n) = \min_{0 \leq k \leq n} v(a'_k)$ and a'_k is up to sign the elementary symmetric polynomial of degree $n - k$ in the b_i and c_i, so that $\min_{0 \leq k \leq n} v(a'_k) = v(a'_{n-m}) = v\big(e_m(b_1, \ldots, b_m, c_1, \ldots, c_l)\big) = \sum_{i=1}^{m} v(b_i)$. □

6.2 Lemma. *Let R be a domain, $r_1, \ldots, r_{n+1} \in R$ and $a_j = r_j - r_{n+1}$ $(1 \leq j \leq n)$. Then there exists $f \in \mathrm{Int}(R)$ with $f(r_j) = 0$ $(1 \leq j \leq n)$ and $f(r_{n+1}) = 1$ if and only if there exists $g \in \mathrm{Int}(R)$ with $g(a_j) = 0$ $(1 \leq j \leq n)$ and $g(0) = 1$.*

Proof. $(\Rightarrow)$ $g(x) := f(x + r_{n+1})$ $(\Leftarrow)$ $f(x) := g(x - r_{n+1})$ □

6.3 Theorem. *Let R be a Krull ring and let $r_1, \ldots, r_{n+1}$ (distinct) $\in R$ such that $r_i \not\equiv r_{n+1}$ mod P $(1 \le i \le n)$ for all $P \in \operatorname{Spec}^1(R)$ with $[R:P] = \infty$. Then there exists $f \in \operatorname{Int}(R)$ with $f(r_i) = 0$ $(1 \le i \le n)$ and $f(r_{n+1}) = 1$.*

Proof. Let $a_j = r_j - r_{n+1}$ for $1 \le j \le n$. The a_j are distinct non-zero elements of R, none of which are contained in any $P \in \operatorname{Spec}^1(R)$ with $[R:P] = \infty$. By Lemma 6.2, we want an $f \in \operatorname{Int}(R)$ with $f(a_j) = 0$ for $1 \le j \le n$ and $f(0) = 1$. We will first construct a polynomial $g \in K[x]$ with $g(a_j) = 0$ for $1 \le j \le n$, such that for every essential valuation v of R and every $r \in R$, $v\big(g(r)\big) \ge v\big(g(0)\big)$ and then set $f(x) = g(x)/g(0)$.

Let $\mathcal{P} = \{P \in \operatorname{Spec}^1(R) \mid \exists j \;\; a_j \in P\}$ then $\mathcal{P}$ is a finite set of maximal ideals of finite index. Also let, for $P \in \mathcal{P}$, $m_P = \max\{m \in \mathbb{N} \mid \exists j \;\; a_j \in P^m\}$ and define $I = \bigcap_{P\in\mathcal{P}} P^{m_P} = \prod_{P\in\mathcal{P}} P^{m_P}$. Let $N = [R:I]$. Using the Chinese Remainder Theorem mod P^{m_P+1} for $P \in \mathcal{P}$, we can get a system of representatives $(b_i)_{i=1}^N$ of R mod I with the property that for all i and all $P \in \mathcal{P}$, $b_i \notin P^{m_P+1}$. Note that for $P \in \mathcal{P}$ and $k \le m_P$, the number of b_i in any given residue class of P^k is $N/[R:P^k]$, since I is an ideal contained in P^k. In other words,

$$\forall r \in R \;\; \forall P \in \mathcal{P} \;\; \forall k \le m_P \quad \big|\{i \mid v_P(r - b_i) \ge k\}\big| = \frac{N}{[R:P^k]}\,.$$

Let $\mathcal{Q} = \{Q \in \operatorname{Spec}^1(R) \setminus \mathcal{P} \mid \exists i \;\; b_i \in Q\}$ and for $Q \in \mathcal{Q}$ let l_Q be the maximal $l \in \mathbb{N}$ such that $b_i \in Q^l$ for some i. Let $c \in R$ with $v_Q(c) = l_Q + 1$ for all $Q \in \mathcal{Q}$, and $v_P(c) = 0$ for all $P \in \mathcal{P}$. Also, let $\mathcal{Q}' = \{Q \in \operatorname{Spec}^1(R) \mid v_Q(c) > 0\}$, then $\mathcal{Q} \subseteq \mathcal{Q}'$ and $\mathcal{Q}' \cap \mathcal{P} = \emptyset$.

We set $b_i' = c^{-1} b_i$. Then $v_Q(b_i') < 0$ for all $Q \in \mathcal{Q}'$ and $0 \le v_P(b_i') < m_P + 1$ for all $P \in \mathcal{P}$. If $P \in \mathcal{P}$ and $r \in R$, we have $v_P(r - b_i') = v_P\big(c^{-1}(cr - b_i)\big) = v_P(cr - b_i)$. Therefore, for all $r \in R$,

$$\forall P \in \mathcal{P} \;\; \forall k \le m_P \quad \big|\{i \mid v_P(r - b_i') \ge k\}\big| = \big|\{i \mid v_P(cr - b_i) \ge k\}\big| = \frac{N}{[R:P^k]}$$

and in particular $\big|\{i \mid v_P(b_i') \ge k\}\big| = N/[R:P^k]$.

Let m be the maximal number of a_i in any residue class of I in R and set $h(x) = \prod_{i=1}^N (x - b_i')^m$. To get a polynomial g with $g(a_j) = 0$ for $1 \le j \le n$, we now replace certain roots of h with the elements $a_1, \ldots, a_n$. Since the b_i are a complete system of residues mod I in R, there exists for every $j \in \{1, \ldots, n\}$ an i_j with $b_{i_j} \equiv c a_j$ mod I.

Let $g(x) = \prod_{i=1}^{mN} (x - c_i)$ be the polynomial resulting from h by replacing, for each $j \in \{1, \ldots, n\}$, one copy of b_{i_j}' in the multiset of roots of h by a_j. (If $i_j = i_k$ for $k \ne j$ this means $c a_j \equiv c a_k$ mod I and therefore $a_j \equiv a_k$ mod I, and by the definition of m, b_{i_j}' occurs with sufficient multiplicity as a root of h that every $a_k \in a_j + I$ can be exchanged for a different copy of b_{i_j}'.) Note that for $P \in \mathcal{P}$, $0 \le v_P(c_i) < m_P + 1$ for all i.

We claim that for all essential valuations v of R and all $r \in R$, $v(g(r)) \geq v(g(0))$. First, assume $P \in \mathcal{P}$. For all $r \in R$, if $k \leq m_P$ then

$$v_P(r - b'_{i_j}) \geq k \iff v_P(r - a_j) \geq k \tag{$*$}$$

(and consequently $\bigl|\{i \mid v_P(c_i) \geq k\}\bigr| = m\bigl|\{i \mid v_P(b'_i) \geq k\}\bigr|$). This is so because $v_P(r - b'_{i_j}) = v_P\bigl(c^{-1}(cr - b_{i_j})\bigr) = v_P(cr - b_{i_j}) = v_P(cr - ca_j + d)$ with $d \in I$, and then $v_P(d) \geq m_P \geq k$ implies that $v_P(cr - ca_j + d) \geq k$ if and only if $v_P(r - a_j) = v_P(cr - ca_j) \geq k$. We abbreviate $\sum_{i=1}^{m_P} \frac{N}{[R:P^k]}$ by γ_P and get

$$v_P\bigl(g(r)\bigr) = \sum_{i=1}^{mN} v_P(r - c_i) = \sum_{k \geq 1} \bigl|\{i \mid v_P(r - c_i) \geq k\}\bigr| \geq$$

$$\geq \sum_{k=1}^{m_P} \bigl|\{i \mid v_P(r - c_i) \geq k\}\bigr| \overset{(*)}{=} m \sum_{k=1}^{m_P} \bigl|\{i \mid v_P(r - b'_i) \geq k\}\bigr| = m\gamma_P,$$

while $v_P(g(0)) =$

$$= \sum_{k \geq 1} \bigl|\{i \mid v_P(c_i) \geq k\}\bigr| = \sum_{k=1}^{m_P} \bigl|\{i \mid v_P(c_i) \geq k\}\bigr| \overset{(*)}{=} m \sum_{k=1}^{m_P} \bigl|\{i \mid v_P(b'_i) \geq k\}\bigr| = m\gamma_P.$$

Now consider $Q \in \mathcal{Q}'$. For all i, j, $v_Q(b'_i) < 0$ and $v_Q(a_j) = 0$. If $g(x) = \sum_{k=0}^{mN} d_k x^k$ and $\mu = \min_{1 \leq k \leq mN} v_Q(d_k)$ then for all $r \in R$ we have (using Lemma 6.1)

$$v_Q\bigl(g(r)\bigr) = \mu + v_Q\Bigl(\prod_{j=1}^{n}(r - a_j)\Bigr) \geq \ \mu \ = \mu + v_Q\Bigl(\prod_{j=1}^{n} a_j\Bigr) = v_Q\bigl(g(0)\bigr).$$

For the remaining essential valuations v of R, $v(c_i) = 0$ for all i. Therefore, if $r \in R$, $v\bigl(g(r)\bigr) = \sum_{i=1}^{mN} v(r - c_i) \geq 0 = \sum_{i=1}^{mN} v(c_i) = v\bigl(g(0)\bigr)$.

Now let $f(x) = g(x)/g(0)$. For $j = 1, \ldots, n$, $f(a_j) = 0$ because $g(a_j) = 0$, and clearly $f(0) = 1$. Also, $f \in \mathrm{Int}(R)$, because for all $r \in R$ and every essential valuation v of R, $v\bigl(g(r)\bigr) \geq v\bigl(g(0)\bigr)$ and therefore $v\bigl(f(r)\bigr) \geq 0$. $\square$

6.4 Remark. If P is a prime ideal in a domain R with $[R : P] = \infty$ it is well known that $\mathrm{Int}(R, R_P) = R_P[x]$. Every $f \in \mathrm{Int}(R, R_P)$ of degree n is determined by its values at $n+1$ arguments $a_0, \ldots, a_n \in R$ and is therefore equal to the Lagrange interpolation polynomial

$$\varphi(x) = \sum_{i=0}^{n} f(a_i) \frac{\prod_{j \neq i}(x - a_j)}{\prod_{j \neq i}(a_i - a_j)}.$$

If the a_i are chosen pairwise incongruent mod P, then $\varphi(x)$ is clearly in $R_P[x]$.

6.5 Corollary. *Let $r_1, \ldots, r_n$ be distinct elements of a Krull ring R. If and only if the r_i are pairwise incongruent mod all $P \in \mathrm{Spec}^1(R)$ with $[R : P] = \infty$ there exists for all $s_1, \ldots, s_n \in R$ an $f \in \mathrm{Int}(R)$ with $f(r_i) = s_i$ for $1 \leq i \leq n$.*

Proof. The "if" part follows from the Theorem, since R-linear combinations of polynomials in $\mathrm{Int}(R)$ are again in $\mathrm{Int}(R)$. Conversely, if a, $a' \in R$ are congruent mod $P \in \mathrm{Spec}^1(R)$ with $[R:P]=\infty$ then there is no $f \in \mathrm{Int}(R, R_P)$ with $f(a)=0$ and $f(a')=1$, since $f(a) \equiv f(a') \bmod P$ for all $f \in \mathrm{Int}(R, R_P) \supseteq \mathrm{Int}(R)$, by Lemma 5.2 (or by the fact that $\mathrm{Int}(R, R_P) = R_P[x]$, see 6.4). □

References

1. Y. Amice, Interpolation p-adique, *Bull. Soc. Math. France* **92** (1964) 117–180.
2. P.-J. Cahen, Integer-valued polynomials on a subset, *Proc. Amer. Math. Soc.* **117** (1993), 919–929.
3. P.-J. Cahen, Polynômes à valeurs entières, *Canad. J. Math.* **24** (1972), 747–754.
4. P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials* (Mathematical Surveys and Monographs vol. 48), Amer. Math. Soc., Providence RI, 1997.
5. L. Carlitz, Finite sums and interpolation formulas over $\mathrm{GF}[p^n, x]$, *Duke Math. J.* **15** (1948) 1001–1012.
6. J.-L. Chabert, Le groupe de Picard de l'anneau des polynômes à valeurs entières, *J. Algebra* **150** (1992), 213–230.
7. S. Frisch, Integer-valued polynomials on Krull Rings, *Proc. Amer. Math. Soc.* **124**(12) (1996), 3595–3604.
8. S. Frisch, Binomial Coefficients Generalized with respect to a Discrete Valuation, to appear in *Proc. of 7^{th} Int'l Conf. on Fibonacci Numbers and Their Applications in Graz, Austria, 1996*, G. E. Bergum, ed.
9. R. Gilmer, W. Heinzer and D. Lantz, The Noetherian property in rings of integer-valued polynomials, *Trans. Amer. Math. Soc.* **338** (1993), 187–199.
10. H. Gunji and D. L. McQuillan, On a class of ideals in an algebraic number field, *J. Number Theory* **2** (1970), 207–222.
11. E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. reine angew. Math.* **44** (1852), 93–146.
12. D. L. McQuillan, On Prüfer domains of polynomials, *J. reine angew. Math.* **358** (1985), 162–178.
13. D. L. McQuillan, Split primes and integer-valued polynomials, *J. Number Theory* **43** (1993), 216–219.
14. A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 117–124.
15. G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 97–116.
16. C. G. Wagner, Interpolation series for continuous functions on π-adic completions of $\mathrm{GF}(q, x)$, *Acta Arith.* **17** (1971), 389–406.

Institut für Mathematik C
Technische Universität Graz
Steyrergasse 30

A-8010 Graz, Austria
e-mail: `frisch@blah.math.tu-graz.ac.at`