Proc. Amer. Math. Soc.
124 (1996) 3595–3604.

INTEGER-VALUED POLYNOMIALS ON KRULL RINGS

Sophie Frisch

Abstract. If R is a subring of a Krull ring S such that R_Q is a valuation ring for every finite index $Q = P \cap R$, P in $\mathrm{Spec}^1(S)$, we construct polynomials that map R into the maximal possible (for a monic polynomial of fixed degree) power of PS_P, for all P in $\mathrm{Spec}^1(S)$ simultaneously. This gives a direct sum decomposition of $\mathrm{Int}(R, S)$, the S-module of polynomials with coefficients in the quotient field of S that map R into S, and a criterion when $\mathrm{Int}(R, S)$ has a regular basis (one consisting of 1 polynomial of each non-negative degree).

Introduction

If A is an infinite subset of a domain S, we write $\mathrm{Int}(A, S)$ for the S-module of polynomials with coefficients in the quotient field of S that – when acting as a function by substitution of the variable – map A into S. For $\mathrm{Int}(S, S)$, the ring of integer-valued polynomials on S, we write $\mathrm{Int}(S)$. Beyond the fact (known of old) that the binomial polynomials $\binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!}$ form a basis of the free $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$, the study of $\mathrm{Int}(S)$ originated with Pólya [16] and Ostrowski [15], who let S be the ring of integers in a number field (their results have been generalized to Dedekind rings by Cahen [4]). $\mathrm{Int}(R, S)$ for $R \neq S$ has only begun to attract attention more recently [2, 3, 6, 8, 11, 13].

We will treat Pólya's and Ostrowski's questions in the case where $R \neq S$ and S is a Krull ring; in particular the question when $\mathrm{Int}(R, S)$ is a free S-module that admits a regular basis, and the related one of determining the highest power of PS_P, where P is a height 1 prime ideal of S, that a monic polynomial of fixed degree can map R into. Following Pólya, we call a sequence of polynomials $(g_n)_{n\in\mathbb{N}_0}$ *regular*, if $\deg g_n = n$ for all n. One basic connection between a module of polynomials and the modules of leading coefficients should be kept in mind:

0.1 Lemma. *Let R be a unitary subring of a field K, M an R-submodule of $K[x]$, and $I_n = \{$ leading coefficients of n-th degree polynomials in $M\} \cup \{0\}$.*

(i) If $(g_n)_{n\in\mathbb{N}_0}$ is a regular sequence of monic polynomials in $K[x]$ such that $I_n g_n \subseteq M$ for all n, then $M = \sum_{n=0}^{\infty} I_n g_n$ (direct sum).

(ii) A regular set of polynomials in M is an R-basis if and only if the leading coefficient of the n-th degree polynomial generates I_n as an R-module.

(iii) M has a regular R-basis if and only if each I_n is non-zero and cyclic.

Proof. (i) If $(g_n)_{n\in\mathbb{N}_0}$ is as stated, then $\sum_{n=0}^{\infty} I_n g_n \subseteq M$ and the sum is direct, since $\deg(g_n) = n$ makes the g_n linearly independent over K. An induction on $N = \deg f$

1991 *Mathematics Subject Classification.* Primary 13B25, 13F05; Secondary 13F20, 11C08.

shows that $f \in M$ implies $f \in \sum_{n=0}^{N} I_n g_n$. Indeed, for $N=0$, $f \in I_0 = g_0 I_0$, and if $N > 0$ and a_N is f's leading coefficient, then $a_N \in I_N$, so $h = f - a_N g_N \in M$ and $h \in \sum_{n=0}^{N-1} I_n g_n$ by induction hypothesis. (ii) and (iii) are easy. □

1. Polynomials mapping a Set into a Discrete Valuation Ring

Throughout section one, v is a discrete valuation on a field K with value-group $\Gamma_v = \mathbb{Z}$ and $v(0) = \infty$, and R_v its valuation ring with maximal ideal M_v. In a kind of generic local regular basis theorem, we will establish the connection (well-known in special cases) between $\mathrm{Int}(A, R_v)$ and the maximal power of M_v that a monic polynomial of degree n can map A into, for all $A \subseteq K$ for which this maximum exists for every n. A subset A of the quotient field of a domain R is called R-fractional if there exists a $d \in R \setminus \{0\}$ such that $dA \subseteq R$.

1.0 Lemma. *If R is an integrally closed domain with quotient field L, $A \subseteq L$ and f non-constant $\in L[x]$ then $f(A)$ is R-fractional if and only if A is.*

Proof. Let $f \in L[x]$, $\deg f = n > 0$. If $f(A)$ is R-fractional there is a non-zero $d \in R$, with $df(a) \in R$ for every $a \in A$. Let $c \in R \setminus \{0\}$, such that $cf \in R[x]$, and set $g = cdf = c_n x^n + \ldots + c_0$. For every $a \in A$, $g(a) \in R$ implies that $c_n a$ is integral over R, therefore $c_n a \in R$ and $c_n A \subseteq R$. The converse is clear. □

Since a set $B \subseteq K$ is R_v-fractional if and only if $\min_{b \in B} v(b)$ exists, Lemma 1.0 shows that A being R_v-fractional is necessary and sufficient for $\min_{a \in A} v(f(a))$ to exist for any non-constant $f \in K[x]$. To exclude polynomials identically zero on A, for which $\min_{a \in A} v(f(a)) = \infty$, we need $\deg f < |A|$, so that the conditions on A in Lemma 1.1 below are necessary.

1.1 Lemma. *Let $n \in \mathbb{N}_0$. If A is an R_v-fractional subset of K with $|A| > n$, then* $\max\{\min_{a \in A} v(f(a)) \mid f \text{ monic } \in K[x],\ \deg f = n\}$ *exists.*

Proof. The case $n=0$ is trivial; so let $n > 0$ and $m \in \mathbb{N}$ such that A is not contained in any union of n cosets of M_v^m in K. Such an m exists, since $n < |A|$ and by the Krull Intersection Theorem $\bigcap_{m \in \mathbb{N}} M_v^m = (0)$. We show that for every monic $f \in K[x]$ of degree n there exists an $a_0 \in A$ with $v(f(a_0)) < nm$ (and consequently $\max\{\min_{a \in A} v(f(a)) \mid f \text{ monic } \in K[x],\ \deg f = n\} < nm$).

Let v' be an extension of v to the splitting field of f over K, $R_{v'}$ its valuation-ring with maximal ideal $M_{v'}$, and $e = [\Gamma_{v'} : \Gamma_v]$. A is not contained in any union of n cosets of ${M_{v'}}^{me}$ in K'. Pick an $a_0 \in A$ that is not in $u + {M_{v'}}^{me}$ for any root u of f in K', then $v(f(a_0)) = v'(f(a_0)) = \sum_{i=1}^{n} v'(a_0 - u_i) < nm$. □

1.2 Theorem. *Let A be an infinite, R_v-fractional subset of K. For $n \in \mathbb{N}_0$ set* $\gamma_{v,A}(n) = \max\{\min_{a \in A} v(f(a)) \mid f \text{ monic } \in K[x],\ \deg f = n\}$.

(i) ${M_v}^{-\gamma_{v,A}(n)} = \{$*leading coefficients of degree n polynomials in* $\mathrm{Int}(A, R_v)\} \cup \{0\}$

(ii) *A regular basis of* $\mathrm{Int}(A, R_v)$ *is given by* $(c_n g_n)_{n \in \mathbb{N}_0}$, *with* $g_n \in K[x]$ *monic,* $\deg g_n = n$, *and* $c_n \in K$, *such that* $\min_{a \in A} v(g_n(a)) = \gamma_{v,A}(n)$ *and* $v(c_n) = -\gamma_{v,A}(n)$.

Proof. Let $I_{n,v} = \{$leading coefficients of degree n polynomials in $\mathrm{Int}(A, R_v)\} \cup \{0\}$. The leading coefficient c_n of any n-th degree polynomial in $\mathrm{Int}(A, R_v)$ must satisfy $v(c_n) \geq -\gamma_{v,A}(n)$, so $I_{n,v} \subseteq {M_v}^{-\gamma_{v,A}(n)}$. Now, for $n \in \mathbb{N}_0$, let g_n be monic of degree n

in $K[x]$ with $\min_{a\in A} v(g_n(a)) = \gamma_{v,A}(n)$ (such things exist by dint of Lemma 1.1) then ${M_v}^{-\gamma_{v,A}(n)} g_n \subseteq \mathrm{Int}(A, R_v)$, so ${M_v}^{-\gamma_{v,A}(n)} \subseteq I_{n,v}$. This shows (i) and also that $I_{n,v} g_n \subseteq \mathrm{Int}(A, R_v)$ for all $n \in \mathbb{N}_0$. (ii) follows by Lemma 0.1 and the fact that ${M_v}^{-\gamma_{v,A}(n)} = c_n R_v$ for every $c_n \in K$ with $v(c_n) = -\gamma_{v,A}(n)$. □

Before deriving a formula for $\max\{\min_{a\in A} v(f(a)) \mid f \text{ monic} \in K[x],\ \deg f = n\}$, when A is a subring of R_v, we check that the other plausible way of normalizing the polynomials would yield the same value. We also see that polynomials mapping $A \subseteq R_v$ into the maximal possible power of M_v can be chosen to split with their roots in any set that M_v-adically approximates A (for instance in A itself, or, if R_v is the localization of a ring R at a prime ideal of finite index, in R). We need a lemma from [7] (but include the proof).

1.3 Lemma. *Let $f \in R_v[x]$, not all of whose coefficients lie in M_v, split over K, as $f(x) = d(x - b_1)\cdot \ldots \cdot (x - b_m)\cdot (x - c_1)\cdot \ldots \cdot (x - c_l)$ with $v(b_i) < 0$, $v(c_i) \geq 0$, and put $f_+(x) = (x - c_1)\cdot \ldots \cdot (x - c_l)$. Then for all $r \in R_v$ $\quad v(f(r)) = v(f_+(r))$.*

Proof. For $r \in R_v$ $v(r - b_i) = v(b_i)$ and so $v(f(r)) = v(d) + \sum_{i=1}^{m} v(b_i) + v(f_+(r))$; we show $v(d) = -\sum_{j=1}^{m} v(b_i)$. Consider $d^{-1}f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Since $f \in R_v[x] \setminus M_v[x]$, $v(d) = -\min_{0\leq k\leq n} v(a_k)$. But a_k is the elementary symmetric polynomial of degree $n - k$ in the b_i and c_i, so the minimal valuation is attained by $v(a_{n-m}) = \sum_{i=1}^{m} v(b_i)$. □

1.4 Proposition. *Let $A \subseteq R_v$ and $0 \leq n < |A|$, then α and γ below are equal:*

$$\alpha \;=\; \max\{\min_{a\in A} v(f(a)) \mid f \in R_v[x] \setminus M_v[x],\ \deg f = n\},$$

$$\gamma \;=\; \max\{\min_{a\in A} v(f(a)) \mid f \text{ monic } \in K[x],\ \deg f = n\}.$$

If, furthermore, $B \subseteq R_v$, such that B intersects every coset of ${M_v}^l$ that A intersects, for all $l \in \mathbb{N}$, then δ below is equal to α and γ; and so is β, if B is also a ring:

$$\beta \;=\; \max\{\min_{a\in A} v(f(a)) \mid f \in B[x] \setminus (M_v \cap B)[x],\ \deg f = n\},$$

$$\delta \;=\; \max\{\min_{a\in A} v(f(a)) \mid f(x) = \textstyle\prod_{i=1}^{n}(x - d_i),\ d_i \in B\}.$$

Proof. Let B be a fixed subset of R_v that intersects every coset of every power of M_v that A intersects (e.g. $B = R_v$, when only interested in α and γ). For $n = 0$ all four expressions are equal to 0; now consider a fixed $n > 0$. Clearly $\delta \leq \gamma$ and, if B is a ring, $\delta \leq \beta \leq \alpha$. Also $\gamma \leq \alpha$, because, given f monic in $K[x]$, there exists a $d \in R_v$ such that $df = g \in R_v[x] \setminus M_v[x]$ and for all $a \in A$ $v(g(a)) = v(d) + v(f(a)) \geq v(f(a))$, and so $\min_{a\in A} v(g(a)) \geq \min_{a\in A} v(f(a))$.

To show $\alpha \leq \delta$, we fix $f \in R_v[x] \setminus M_v[x]$ of degree n and construct a monic g that splits with roots in B such that $v(g(a)) \geq \min_{a\in A} v(f(a))$ for all $a \in A$. Let v' be an extension of v to the splitting field of f over K. For all $a \in A$, $v'(f(a)) = v'(f_+(a))$ with $f_+(x) = \prod_{i=1}^{l}(x - c_i)$, where the c_i are the roots of f in $R_{v'}$, by Lemma 1.3. Put $s = \min_{a\in A} v'(f_+(a))$. We replace each c_i by a $d_i \in B$ chosen such that $\prod_{i=1}^{l}(x - d_i) = h(x)$ satisfies: for all $a \in A$ $v'(h(a)) \geq s$. If $(c_i + M_{v'}^k) \cap A \neq \emptyset$ for all $k \in \mathbb{N}$, we pick d_i out of $(c_i + M_{v'}^s) \cap B$; otherwise out of $(c_i + M_{v'}^k) \cap B$ with k maximal such that $(c_i + M_{v'}^k) \cap A \neq \emptyset$. Since the intersection of a residue class of $M_{v'}^k$ in $R_{v'}$ with R_v is either empty or an entire residue class of a power of M_v in R_v, and B intersects all of these that A intersects, it is possible to find such d_i in B. Now for every $a \in A$ either $v'(a-d_i) \geq v'(a-c_i)$ for all i and so $v'(h(a)) \geq v'(f_+(a)) \geq s$, or $v'(a-d_i) \geq s$ for some i and hence $v'(h(a)) \geq s$. To get a polynomial of degree n, set $g(x) = (x-d_0)^{n-l}h(x)$, $d_0 \in B$. □

2. Polynomials mapping into a maximal Power of M_v

If R is an infinite subring of a discrete valuation ring R_v, we will construct polynomials $g_n(x) = (x-a_1)\dots(x-a_n)$ that map R into the maximal possible (for a monic polynomial of degree n) power of M_v, by finding sequences (a_i) in R that show a nice distribution among the cosets of $M_v^n \cap R$, to serve as roots.

This generalizes a procedure of Pólya [16] (also used by Gunji and McQuillan [12, 14], Cahen [4] and others) for the special case where $R_v = R_Q$, Q being a prime ideal of index q in R such that R_Q is a discrete valuation ring: Pick $\pi \in Q \setminus Q^2$ and a complete set of residues $r_0, ..., r_{q-1}$ of Q in R and define $a_n = \sum_{i\geq 0} r_{c_i}\pi^i$, if $n = \sum_{i\geq 0} c_i q^i$ is the q-adic expansion of n. The resulting polynomials map R into the highest possible power of Q and can be used to give a regular basis of $\mathrm{Int}(R_v)$ (most clearly stated in [14]). Gilmer [10] has remarked that the construction even works for $\mathrm{Int}(D)$, D a quasi-local ring with principal maximal ideal.

The $\mathcal{I}$-sequences below are defined for any commutative ring R. All sequences are indexed by an initial segment of $\mathbb{N}$ or $\mathbb{N}_0$. Quantifiers over indices of such a sequence are assumed to range over precisely the index-set.

2.0 Definition. For a set $\mathcal{I}$ of ideals in a commutative ring R we define an *$\mathcal{I}$-sequence* in R to be a sequence (a_n) of elements in R with the property

$$\forall I \in \mathcal{I} \quad \forall n, m \qquad a_n \equiv a_m \mod I \quad \Longleftrightarrow \quad [R:I] \mid n-m.$$

We define a *homogeneous* $\mathcal{I}$-sequence to be one with the additional property

$$\forall I \in \mathcal{I} \quad \forall n \geq 1 \qquad a_n \in I \iff [R:I] \mid n.$$

(Any infinite $[R:I]$ we regard as dividing 0, but no other integer.) Note that $a_1, a_2, ..$ is a homogeneous $\mathcal{I}$-sequence if and only if $0{=}a_0, a_1, a_2, ..$ is an $\mathcal{I}$-sequence.

2.1 Proposition. *Let $\mathcal{I} = \{I_n \mid n \in \mathbb{N}\}$ be a descending chain of ideals in a commutative ring R, then there exists an infinite homogeneous $\mathcal{I}$-sequence in R.*

Proof. Put $I_0 = R$. For $k \geq 0$, if $[I_k : I_{k+1}]$ is finite, let $\{a_j^{(k)} \mid 0 \leq j < [I_k : I_{k+1}]\}$ be a system of representatives of $I_k : I_{k+1}$ with $a_0^{(k)} = 0$, otherwise let $(a_j^{(k)})_{j\in\mathbb{N}_0}$ be a sequence in I_k of elements pairwise incongruent mod I_{k+1}, with $a_0^{(k)} = 0$. If $I_N \in \mathcal{I}$ with $[R:I_N]$ finite, then every $n < [R:I_N]$ has a unique representation $n = \sum_{k=0}^{N-1} j_k[R:I_k]$ with $0 \leq j_k < [I_k:I_{k+1}]$, and we set $a_n = \sum_{k=0}^{N-1} a_{j_k}^{(k)}$. If the indices of ideals in $\mathcal{I}$ get arbitrarily large while remaining finite, this defines our $\mathcal{I}$-sequence inductively. Otherwise there exists $I_N \in \mathcal{I}$ of maximal finite index such that either $[I_N : I_{N+1}]$ is infinite or $I_m = I_N$ for $m \geq N$. Define a_n for $n < [R:I_N]$ as above. Then, in the first case, set $a_m = a_q{}^{(N)} + a_r$ for $m = q\,[R:I_N] + r$ with $0 \leq r < [R:I_N]$, and $a_m = a_r$ in the second. □

2.2 Facts.

(i) *For $I \in \mathcal{I}$ of finite index in R, any $[R:I]$ consecutive terms of an $\mathcal{I}$-sequence form a complete set of representatives of R mod I.*

(ii) *If $(a_i)_{i=1}^n$ is an $\mathcal{I}$-sequence in R then $(r - a_i)_{i=1}^n$ is an $\mathcal{I}$-sequence for every $r \in R$ and $(a_n - a_{n-i})_{i=0}^{n-1}$ is a homogeneous $\mathcal{I}$-sequence.*

The following lemma will be needed for globalization.

2.3 Lemma. *If $a_1, ..., a_l$ is an $\mathcal{I}$-sequence for a chain of ideals $\mathcal{I}$, $J \in \mathcal{I}$ with $[R : J] > l$, and $b_1, ..., b_l \in R$ such that $b_n \equiv a_n \bmod J$ for $1 \le n \le l$, then (b_n) is also an $\mathcal{I}$-sequence, and homogeneous if (a_n) is.*

Proof. Let $I \in \mathcal{I}$ and $1 \le n, m \le l$. First suppose $n \equiv m \bmod [R:I]$. Then $n = m$ or $[R:I] < l$. In the latter case $J \subseteq I$, so $b_n \equiv a_n \equiv a_m \equiv b_m \bmod I$. Now suppose $n \not\equiv m \bmod [R:I]$. Either $J \subseteq I$ or $I \subseteq J$. If $J \subseteq I$ then $b_n \equiv a_n \not\equiv a_m \equiv b_m \bmod I$. If $I \subseteq J$ then $b_n \equiv a_n \not\equiv a_m \equiv b_m \bmod J$ (because $0 \ne n - m < [R : J]$), hence $b_n \not\equiv b_m \bmod I$. Homogeneity is shown similarly. □

From now on, R is always an infinite subring of a discrete valuation ring R_v. Note that the definitions of $\alpha_{v,R}(n)$ and v-sequence below depend only on M_v and R, and thus not distinguish between equivalent valuations.

2.4 Definition. A *v-sequence for R* is a $\{M_v^n \cap R \mid n \in \mathbb{N}\}$-sequence in R. In other words, (a_n) is a v-sequence for R if and only if for all $n \in \mathbb{N}$ and all i, j,

$$a_i - a_j \in {M_v}^n \quad\iff\quad [R : {M_v}^n \cap R] \mid i - j$$

and a *homogeneous* v-sequence if in addition, for all $n \in \mathbb{N}$ and all $j \ge 1$,

$$a_j \in {M_v}^n \quad\iff\quad [R : {M_v}^n \cap R] \mid j\,.$$

If $[R : {M_v}^n \cap R]$ is infinite, distinct elements of a v-sequence must be incongruent mod ${M_v}^n \cap R$. Proposition 2.1 guarantees the existence of an infinite homogeneous v-sequence for every infinite subring R of every discrete valuation ring R_v.

2.5 Definition. For $n \in \mathbb{N}_0$, R an infinite subring of R_v and $q \in \mathbb{N}$, let

$$\alpha_{v,R}(n) = \sum_{j \ge 1} \left[\frac{n}{[R : {M_v}^j \cap R]}\right] \qquad \text{and} \qquad \alpha_q(n) = \sum_{j\ge 1} \left[\frac{n}{q^j}\right].$$

Infinite indices are allowed; $\frac{n}{\infty} = 0$. Since R is infinite, $\alpha_{v,R}(n)$ is always a finite number. We will frequently use the fact that $\alpha_{v,R}(n) > 0$ if and only if $n \ge [R : M_v \cap R]$. If Q is a prime ideal in a domain D, such that D_Q is a discrete valuation ring, we write v_Q for the corresponding valuation with value group $\mathbb{Z}$.

2.6 Facts.

(i) *If Q is a prime ideal of finite index q in R such that R_Q is a discrete valuation ring, then $\alpha_{v_Q,R}(n) = \alpha_q(n)$ for all n.*

(ii) *If v is a discrete valuation, R an infinite subring of R_v and v' an extension of v with $[\Gamma_{v'}:\Gamma_v]=e$ finite, then $\alpha_{v',R}(n)=e\cdot\alpha_{v,R}(n)$ for all n.*

Proof. (i) Since Q is maximal, $(QR_Q)^n\cap R=Q^n$ for all n. Using the fact that Q contains a generator of QR_Q one sees that $[R:Q^n]=[R_Q:(QR_Q)^n]=q^n$ for all n.
(ii) For $k\in\mathbb{N}$, ${M_{v'}}^k\cap R=({M_{v'}}^k\cap R_v)\cap R={M_v}^{\lceil\frac{k}{e}\rceil}\cap R$, where $\lceil x\rceil$ denotes the smallest integer greater or equal x. Each number $\left[\frac{n}{[R:{M_v}^j\cap R]}\right]$ appears e times, as $\left[\frac{n}{[R:{M_{v'}}^k\cap R]}\right]$ for $k=(j-1)e+1,\,\ldots,\,je$, in the sum for $\alpha_{v',R}(n)$. □

In the remainder of section two, v is assumed to have value-group $\mathbb{Z}$.

2.7 Lemma. *Let $(a_i)_{i=1}^{n+1}$, $(b_i)_{i=1}^{n}$ and $(c_i)_{i=1}^{n}$ be v-sequences for R, and $(c_i)_{i=1}^{n}$ homogeneous, then*

(a) $v(c_1\cdot\ldots\cdot c_n)=\alpha_{v,R}(n)\le v(b_1\cdot\ldots\cdot b_n)\le\alpha_{v,R}(n)+\max_{1\le i\le n}v(b_i)$,

(b) $v\left(\prod_{i=1}^{n}(a_{n+1}-a_i)\right)=\alpha_{v,R}(n)\le v\left(\prod_{i=1}^{n}(r-b_i)\right)$ *for all $r\in R$.*

Proof. $v(c_1\cdot\ldots\cdot c_n)=\sum_{j\ge1}\left|\{i\mid 1\le i\le n,\ v(c_i)\ge j\}\right|$ and similarly for the b_i. Since for finite index ${M_v}^j\cap R$ every $[R:{M_v}^j\cap R]$ successive terms of a v-sequence form a complete residue system of R mod ${M_v}^j\cap R$, we have $\forall j\in\mathbb{N}$

$$\left|\{i\mid v(c_i)\ge j\}\right|=\left[\frac{n}{[R:{M_v}^j\cap R]}\right]\le\left|\{i\mid v(b_i)\ge j\}\right|\le\left[\frac{n}{[R:{M_v}^j\cap R]}\right]+1$$

This implies (a) (and, since the 1 on the right can only occur if $[R:{M_v}^j\cap R]\nmid n$, $v(b_1\cdot\ldots\cdot b_n)\le\alpha_{v,R}(n)+\max_{1\le i\le n}v(b_i)-\max\{j\mid[R:{M_v}^j\cap R]\text{ divides }n\}$). By Fact 2.2 (ii) about $\mathcal{I}$-sequences, (b) is a special case of (a). □

2.8 Theorem. *Let R be an infinite subring of R_v. An R_v-basis of* $\mathrm{Int}(R,R_v)$ *is given by*

$$f_0=1\qquad\textit{and}\qquad f_n(x)=\frac{\prod_{i=1}^{n}(x-a_i)}{\prod_{i=1}^{n}(a_{n+1}-a_i)}\qquad(n\ge1),$$

where $(a_n)_{n=1}^{\infty}$ is a v-sequence for R.

Proof. An infinite v-sequence $(a_n)_{n=1}^{\infty}$ in R exists by Proposition 2.1 applied to $\{{M_v}^n\cap R\,|\,n\in\mathbb{N}\}$. The f_n, being a K-basis of $K[x]$, are free generators of the R_v-module they generate in $K[x]$, call this module F. Since by Lemma 2.7 every f_n maps R to R_v, $F\subseteq\mathrm{Int}(R,R_v)$. For the reverse inclusion we show the stronger statement that $\mathrm{Int}(A,R_v)\subseteq F$, where $A=\{a_n\,|\,n\in\mathbb{N}\}$. Let $f\in\mathrm{Int}(A,R_v)$, $f=\sum_{j=0}^{N}l_jf_j$ with $l_j\in K$. We show inductively that the l_j are in R_v. $l_0=f(a_1)\in R_v$. The induction hypothesis is $l_j\in R_v$ for $0\le j<n$. Using this and the facts that $f_j(a_i)=0$ for $j\ge i$ and $f_j(a_{j+1})=1$, we see that $f(a_{n+1})=l_n+\sum_{j=0}^{n-1}l_jf_j(a_{n+1})$. Since $f_j(a_i)\in R_v$ for all i, j (by Lemma 2.7) and $f\in\mathrm{Int}(A,R_v)$, the sum on the right as well as $f(a_{n+1})$ is in R_v, therefore $l_n\in R_v$. □

Remark. For an infinite subring R of R_v and $A\subseteq R$, the proof of Theorem 2.8 shows that if A contains an infinite v-sequence for R, then $\mathrm{Int}(A,R_v)=\mathrm{Int}(R,R_v)$. The converse holds, too (the criterion for $\mathrm{Int}(A,R_v)=\mathrm{Int}(R,R_v)$ in [7] is easily seen to be equivalent to A containing an infinite v-sequence for R).

Corollary 1. *$\alpha_{v,R}(n) = \max\{ \min_{r\in R} v(f(r)) \mid f$ monic $\in K[x]$, $\deg f = n\}$ and $M_v^{-\alpha_{v,R}(n)} = \{$ leading coefficients of n-th degree polynomials in $\mathrm{Int}(R, R_v)\ \} \cup \{0\}$.*

Proof. The second statement can be read off the theorem using Lemma 2.7 (b), the first one then follows by Theorem 1.2. □

Pólya's Satz IV [16] is a special case: if P is a prime ideal in a domain R such that R_P is a discrete valuation ring and $[R : P] = q$, then (by Proposition 1.4 with $B = R$ and Fact 2.6 i) $\alpha_q(n) = \max\{ \min_{r\in R} v_P(f(r)) \mid f \in R[x] \setminus P[x],\ \deg f = n\}$.

Corollary 2. *Let $g_n(x) = \prod_{i=1}^{n}(x - a_i{}^{(n)})$, where $(a_i{}^{(n)})_{i=1}^{n}$ is a v-sequence for R when $n \geq [R : M_v \cap R]$, and let g_n be any monic polynomial in $R_v[x]$ of degree n for $0 \leq n < [R : M_v \cap R]$. Further let, for $n \in \mathbb{N}_0$, $c_n \in K$ with $v(c_n) = -\alpha_{v,R}(n)$. Then $(c_n g_n)_{n\in\mathbb{N}_0}$ is an R_v-basis of $\mathrm{Int}(R, R_v)$.*

Proof. For all $n\in\mathbb{N}_0$, $r\in R$, $v(g_n(r))\geq\alpha_{v,R}(n)$ (by Lemma 2.7, when $n\geq[R:M_v\cap R]$, and because $g_n \in R_v[x]$ and $\alpha_{v,R}(n) = 0$ otherwise). By the maximality of $\alpha_{v,R}(n)$ (Corollary 1), $\min_{r\in R} v(g_n(r)) = \alpha_{v,R}(n)$. Therefore $(c_n g_n)_{n\in\mathbb{N}_0}$ is an R_v-basis of $\mathrm{Int}(R, R_v)$ by Corollary 1 and Theorem 1.2 (ii). □

3. Polynomials mapping a subring into a Krull Ring

Notation. Let S be a domain with quotient field K, such that $S = \bigcap_{v\in\mathcal{V}} R_v$, $\mathcal{V}$ a set of discrete valuations (with value-group $\mathbb{Z}$) on K; and R an infinite subring of S. We put $I_n = \{$leading coefficients of n-th degree polynomials in $\mathrm{Int}(R, S)\} \cup \{0\}$ and introduce names for recurring additional conditions:

(F) $\forall\, q \in \mathbb{N}\ \{Q \trianglelefteq R \mid [R : Q] = q$ *and* $Q = M_v \cap R$ *for some* $v \in \mathcal{V}\}$ is a finite set.

(C) For every prime ideal Q of finite index in R, the set of $M_v{}^n \cap R$ with $n \in \mathbb{N}$, $v \in \mathcal{V}$, and $M_v \cap R = Q$, if not empty, forms a descending chain of ideals.

Note that (C) holds naturally in two cases: when there is only one M_v such that $M_v \cap R = Q$, and when every $M_v{}^n \cap R$ with $M_v \cap R = Q$ is a power of Q.

3.0 Lemma. (Cahen [4]) *If R is an infinite subring of a Krull ring S and $q \in \mathbb{N}$, then S has at most finitely many height 1 prime ideals P with $[R : P \cap R] = q$.*

Proof. There exists $r \in R$ with $r^q - r \neq 0$. For every P with $Q = R \cap P$ of index q in R, $r^q - r \in Q \subseteq P$, so the statement follows by the definition of Krull ring. □

3.1 Lemma. *Let $v \in \mathcal{V}$ such that $M_v \cap R = Q \neq (0)$ and L the quotient field of R. If R_Q is a valuation ring, then it is a discrete valuation ring and $R_Q = R_v \cap L$. If Q is also a maximal ideal then, for every $n \in \mathbb{N}$, $M_v^n \cap R$ is a power of Q.*

Proof. For any valuation ring V with quotient field L and maximal ideal M we have $L\setminus V = \{r \in L^* \mid r^{-1} \in M\}$. Put $R_v \cap L = R_w$ and $M_v \cap L = M_w$, then R_w and R_Q are valuation rings with quotient field L and maximal ideals M_w and QR_Q, respectively. $R \subseteq R_w$ and $M_w \cap R = M_v \cap R = Q$ imply $R_Q \subseteq R_w$ and also $QR_Q \subseteq M_w$. By the latter inclusion $L \setminus R_Q = \{r \in L^* \mid r^{-1} \in QR_Q\} \subseteq \{r \in L^* \mid r^{-1} \in M_w\} = L \setminus R_w$. This shows $R_Q = R_w = R_v \cap L$, so R_Q is a discrete valuation ring and every $M_v^n \cap R_Q$ is a power of QR_Q. If Q is maximal, then $(QR_Q)^k \cap R = Q^k$ for all k, so $M_v^n \cap R$ is a power of Q. □

3.2 Lemma. (C) *implies: For every finite set $\mathcal{M}$ of prime ideals of finite index in R and every $m \in \mathbb{N}$, there exists a sequence $(a_i)_{i=0}^m$ in R that is a homogeneous v-sequence for all v in $\mathcal{V}$ with $M_v \cap R \in \mathcal{M}$, simultaneously.*

Proof. For every $Q \in \mathcal{M}$, $\mathcal{I}_Q = \{{M_v}^n \cap R \mid v \in \mathcal{V},\ n \in \mathbb{N},\ M_v \cap R = Q\}$ (if not empty) is a descending chain by (C), so there exists a homogeneous $\mathcal{I}_Q$-sequence $({a_i}^{(Q)})_{i=0}^{\infty}$ in R by Proposition 2.1. For each Q with $\mathcal{I}_Q \neq \emptyset$ let I_Q be an element of $\mathcal{I}_Q$ with $[R\colon I_Q] > m$. $I_Q = {M_v}^n \cap R$ for some v and n and therefore contains Q^n. Since different Q are co-prime, there exists, by the Chinese Remainder Theorem, a sequence $(a_i)_{i=0}^m$ in R that is congruent to $({a_i}^{(Q)})_{i=0}^m$ modulo I_Q for all $Q \in \mathcal{M}$. By Lemma 2.3, this a homogeneous $\mathcal{I}_Q$-sequence for all $Q \in \mathcal{M}$, i.e., a homogeneous v-sequence for all v with $M_v \cap R \in \mathcal{M}$. □

From Lemma 3.0, Lemma 3.1 and the fact that the powers of an ideal Q form a descending sequence, we conclude that the hypothesis of Theorem 3.4 below is satisfied in at least one natural setting:

3.3 Fact. *If S is a Krull ring, $\mathcal{V} = \{v_P \mid P \in \mathrm{Spec}^1(S)\}$, and R an infinite subring such that R_Q is a valuation ring for every finite index $Q = P \cap R$, $P \in \mathrm{Spec}^1(S)$, then (C) and (F) both hold.*

In the following theorem, the case where S is a Dedekind ring and $R = S$ is due to Cahen [4] (also pertinent: [5]).

3.4 Theorem. *Let R be an infinite subring of $S = \bigcap_{v\in\mathcal{V}} R_v$. If* (C) *and* (F) *hold, then*

$$I_n = \bigcap\nolimits_{v\in\mathcal{V}} M_v^{-\alpha_{v,R}(n)} \qquad (n \in \mathbb{N}_0)$$

and there exists a regular sequence of monic polynomials (g_n) in $R[x]$ such that

$$\mathrm{Int}(R,S) = \sum\nolimits_{n\geq 0} I_n g_n,$$

namely, $g_n(x) = \prod_{i=1}^n (x - {a_i}^{(n)})$, where $({a_i}^{(n)})_{i=1}^n$ is a simultaneous v-sequence for all $v \in \mathcal{V}$ with $[R : M_v \cap R] \leq n$.

Proof. $\mathrm{Int}(R, \bigcap_{v\in\mathcal{V}} R_v) = \bigcap_{v\in\mathcal{V}} \mathrm{Int}(R, R_v)$, therefore $I_n \subseteq \bigcap_{v\in\mathcal{V}} {M_v}^{-\alpha_{v,R}(n)}$ (by Theorem 2.8, Corollary 1). For the reverse inclusion, let $c \in \bigcap_{v\in\mathcal{V}} M_v^{-\alpha_{v,R}(n)}$. Set $\mathcal{V}_n = \{v \in \mathcal{V} \mid \alpha_{v,R}(n) > 0\} = \{v \in \mathcal{V} \mid [R : M_v \cap R] \leq n\}$ then $\{M_v \cap R \mid v \in \mathcal{V}_n\}$ is finite by (F). Let $({a_i}^{(n)})_{i=1}^n$ in R be a homogeneous v-sequence for all $v \in \mathcal{V}_n$ simultaneously (which exists by Lemma 3.2) and $g_n(x) = \prod_{i=1}^n (x - {a_i}^{(n)})$. Then $\min_{r\in R} v(g(r)) \geq \alpha_{v,R}(n)$ for all $v \in \mathcal{V}$ (by Lemma 2.7 when $v \in \mathcal{V}_n$, and because $\alpha_{v,R}(n) = 0$ and $g_n \in R[x]$ otherwise) which means $cg(x) \in \mathrm{Int}(R, \bigcap_{v\in\mathcal{V}} R_v)$ and hence $c \in I_n$. This completes the proof of the first statement and also shows, for all $n \geq 0$, that $I_n g_n \subseteq \mathrm{Int}(R, \bigcap_{v\in\mathcal{V}} R_v)$, so the second follows by Lemma 0.1. □

From now on, S is a Krull ring. By convention, the empty intersection or product of ideals of S equals S. We denote the set of height 1 prime ideals of S by $\mathrm{Spec}^1(S)$ or $\mathcal{P}$. If $P \in \mathcal{P}$, we write $\alpha_{P,R}$ for $\alpha_{v_P,R}$ and, if $j \in \mathbb{N}_0$, $P^{(j)}$ for $(PS_P)^j \cap S$. With this notation we have, for $n \in \mathbb{N}_0$ and $P \in \mathcal{P}$:

$$\alpha_{P,R}(n) = \sum_{j\geq 1} \left[\frac{n}{[R : P^{(j)} \cap R]} \right].$$

3.5 Lemma. *Let S be a Krull ring and $\mathcal{V} = \{v_P \mid P \in \mathcal{P}\}$. If* (C) *holds, then* $\mathrm{Int}(R,S)$ *has a regular basis* $\iff \bigcap_{\substack{P\in\mathcal{P}\\ [R:P\cap R]\le n}} P^{(\alpha_{P,R}(n))}$ *is principal for all n.*

Proof. $\alpha_{P,R}(n) \neq 0$ if and only if $[R : P \cap R] \le n$. Since (F) holds by Lemma 3.0, this only happens for finitely many P for each n. If $\{a_P \mid P \in \mathcal{P}\}$ is a set of integers, only finitely many of them non-zero, then $\bigcap_{P\in\mathcal{P}} (PS_P)^{-a_P}$ is principal if and only if $\bigcap_{P\in\mathcal{P}} (PS_P)^{a_P}$ is, namely if there exists $c \in K$ with $v_P(c) = a_P$ for all $P \in P$. If all a_P are non-negative then $\bigcap_{P\in\mathcal{P}} (PS_P)^{a_P} = \bigcap_{a_P>0} P^{(a_P)}$. Applied to $\bigcap_{P\in\mathcal{P}} (PS_P)^{-\alpha_{P,R}(n)}$, which is I_n by Theorem 3.4, with Lemma 0.1 (iii) in mind, this proves the claim. □

3.6 Theorem. *Let R be an infinite subring of a Krull ring S, $\mathcal{P} = \mathrm{Spec}^1(S)$, $\mathcal{P}^* = \{P \in \mathcal{P} \mid [R : P \cap R]$ finite$\}$ and $\mathcal{Q} = \{R \cap P \mid P \in \mathcal{P}^*\}$. If R_Q is a valuation ring for all $Q \in \mathcal{Q}$, then R_Q is a discrete valuation ring for all $Q \in \mathcal{Q}$ and*

$$\mathrm{Int}(R,S) \text{ has a regular basis } \iff \forall\, q \in \mathbb{N} \bigcap_{\substack{P\in\mathcal{P}\\ [R:R\cap P]=q}} P^{(e_P)} \text{ is a principal ideal of } S,$$

where e_P is the ramification index of PS_P over QR_Q, for $P \in \mathcal{P}^*$, $Q = P \cap R$.

Proof. Let $\mathcal{P}_q = \{P \in \mathcal{P} \mid [R:P\cap R] = q\}$, $P \in \mathcal{P}_q$, $Q = P\cap R$, L the quotient field of R, then by Lemma 3.1 $R_Q = S_P \cap L$ and R_Q is a discrete valuation ring. $v'_P = (1/e_P)v_P$ is equivalent to v_P and is an extension of v_Q to K with $[\Gamma_{v'_P} : \Gamma_{v_Q}] = e_P$. By the Facts 2.6 (ii) and (i), $\alpha_{P,R}(n) = \alpha_{v'_P,R}(n) = e_P\alpha_{Q,R}(n) = e_P\alpha_q(n)$.

If we call left and right side of the claimed equivalence (l) and (r), respectively, then (l) is equivalent to (l') '$\forall n \bigcap_{\substack{P\in\mathcal{P}\\ [R:P\cap R]\le n}} P^{(\alpha_{P,R}(n))}$ is principal' by Lemma 3.5 (whose condition (C) holds by Fact 3.3). We know that $\bigcap_{\substack{P\in\mathcal{P}\\ [R:P\cap R]\le n}} P^{(\alpha_{P,R}(n))} = \bigcap_{q\le n}\bigcap_{P\in\mathcal{P}_q} P^{(e_P\alpha_q(n))}$. The latter is clearly principal provided all $\bigcap_{P\in\mathcal{P}_q} P^{(e_P)}$ are; thus (r) $\Rightarrow$ (l').

For (l') $\Rightarrow$ (r), suppose $\bigcap_{q\le n}\bigcap_{P\in\mathcal{P}_q} P^{(e_P\alpha_q(n))} = s_nS$ for all n. We see that $s_qS = \bigcap_{P\in\mathcal{P}_q} P^{(e_P)} \cap \bigcap_{l<q}\bigcap_{P\in\mathcal{P}_l} P^{(e_P\alpha_l(q))}$, because $\alpha_q(q) = 1$. This allows an induction on q: from the formula for s_qS we conclude that $\bigcap_{P\in\mathcal{P}_q} P^{(e_P)}$ is principal if $\bigcap_{P\in\mathcal{P}_l} P^{(e_P)}$ is principal for all $l < q$. □

Corollary 1. *If $R \subseteq S$ is an extension of Krull rings such that* $\mathrm{ht}(P\cap R) \le 1$ *for all height 1 prime ideals P of S then*

$$\mathrm{Int}(R,S) \text{ has a regular basis } \iff \forall\, q \in \mathbb{N} \bigcap_{\substack{Q\in\mathrm{Spec}^1(R)\\ [R:Q]=q}} \mathrm{div}(QS) \text{ is principal},$$

where $\mathrm{div}(QS)$ *means the smallest divisorial ideal containing QS.*

Proof. If $R \subseteq S$ is an extension of Krull rings with the stated property and Q is in $\mathrm{Spec}^1(R)$, then $\mathrm{div}(QS) = \bigcap_{\substack{P\in\mathrm{Spec}^1(S)\\ P\cap R=Q}} P^{(e_P)}$, where $e_P = e(P|Q)$ is the ramification index of PS_P over QR_Q [1, p183]. □

In particular, if $R \subseteq S$ is an extension of Dedekind rings, then

$$\mathrm{Int}(R,S) \text{ has a regular basis } \iff \forall\, q \in \mathbb{N} \prod_{\substack{Q\in\mathrm{Spec}(R)\\ [R:Q]=q}} QS \text{ is principal.}$$

A different specialization gives Ostrowski's criterion [15]. If S is a Krull ring,

$$\mathrm{Int}(S) \text{ has a regular basis } \iff \forall\, q \in \mathbb{N} \ \prod_{\substack{P\in \mathrm{Spec}^1(S)\\ [S:P]=q}} P \ \text{ is principal.}$$

When a regular basis exists, we can give a fairly explicit description of one. (For $\mathrm{Int}(S)$, S a Dedekind ring, there also is a different construction by Gerboud [9].)

Corollary 2. *In the situation of Theorem 3.6, if* $\bigcap_{\substack{P\in\mathcal{P}\\ [R:P\cap R]=q}} P^{(e_P)} = c_q S$ $(q \in \mathbb{N})$ *then a regular basis of* $\mathrm{Int}(R, S)$ *is given by* $f_0 = 1$*,*

$$f_n(x) = \prod_{q\le n} c_q^{-\alpha_q(n)} \prod_{i=1}^{n} (x - a_i{}^{(n)}) \qquad (n \in \mathbb{N}),$$

where $(a_i{}^{(n)})_{i=1}^n \subseteq R$ *is a* v_P*-sequence for all* $P \in \mathcal{P}$ *with* $[R : P \cap R] \le n$*.*

Proof. $v_P(c_q^{-\alpha_q(n)}) = -e_P \alpha_q(n) = -\alpha_{P,R}(n)$ for the $P \in \mathcal{P}$ with $[R : P \cap R] = q$, and zero for all other $P \in \mathcal{P}$, so $v_P(\prod_{q\le n} c_q^{-\alpha_q(n)}) = -\alpha_{P,R}(n)$ for all $P \in \mathcal{P}$ (since $\alpha_{P,R}(n) = 0$ if $n < [R : P \cap R]$). Therefore the f_n are an S_P-basis of $\mathrm{Int}(R, S_P)$ for all $P \in \mathcal{P}$ simultaneously, by Theorem 2.8, Corollary 2. □

References

[1] S. Balcerzyk and T. Józefiak, *Commutative Noetherian and Krull Rings*, Ellis Horwood, Chichester; distr. by Wiley, New York, 1989.

[2] P.-J. Cahen, *Integer-valued polynomials on a subset*, Proc. Amer. Math. Soc. **117** (1993), 919–929.

[3] P.-J. Cahen, *Parties pleines d'un anneau noethérien*, J. Algebra **157** (1993), 199–212.

[4] P.-J. Cahen, *Polynômes à valeurs entières*, Canad. J. Math. **24** (1972), 747–754.

[5] P.-J. Cahen and J.-L. Chabert, *Coefficients et valeurs d'un polynôme*, Bull. Sci. Math. 2e Sér. **95** (1971), 295–304.

[6] J.-L. Chabert and G. Gerboud, *Polynômes à valeurs entières et binômes de Fermat*, Canad. J. Math. **45** (1993), 6–21.

[7] S. Frisch, *Substitution and Closure of Sets under Integer-valued Polynomials*, J. Number Theory (to appear).

[8] G. Gerboud, *Substituabilité d'un anneau de Dedekind*, CR Acad. Sci. Paris **317** (1993), 29-32.

[9] G. Gerboud, *Construction, sur un anneau de Dedekind, d'une base régulière de polynômes à valeurs entières*, manuscripta math. **65** (1989), 167–179.

[10] R. Gilmer, *Prüfer Domains and Rings of Integer-Valued Polynomials*, J. Algebra **129** (1990), 502–517.

[11] R. Gilmer, *Sets That Determine Integer-Valued Polynomials*, J. Number Theory **33** (1989), 95–100.

[12] H. Gunji and D. L. McQuillan, *On a Class of Ideals in an Algebraic Number Field*, J. Number Theory **2** (1970), 207–222.

[13] D. L. McQuillan, *On a Theorem of R. Gilmer*, J. Number Theory **39** (1991), 245–250.

[14] D. L. McQuillan, *On Prüfer domains of polynomials*, J. reine angew. Math. **358** (1985), 162–178.

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

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

Institut für Mathematik C, Technische Universität Graz, Kopernikusgasse 24, A-8010 Graz, Austria

e-mail: frisch@blah.math.tu-graz.ac.at