INTEGER-VALUED POLYNOMIALS ON VALUATION RINGS OF GLOBAL FIELDS WITH PRESCRIBED LENGTHS OF FACTORIZATIONS

VICTOR FADINGER, SOPHIE FRISCH, AND DANIEL WINDISCH

Abstract. Let V be a valuation ring of a global field K. We show that for all positive integers k and $1 < n_1 \leq \ldots \leq n_k$ there exists an integer-valued polynomial on V, that is, an element of $\mathrm{Int}(V) = \{f \in K[X] \mid f(V) \subseteq V\}$, which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lenghts are exactly $n_1, \ldots, n_k$. In fact, we show more, namely that the same result holds true for every discrete valuation domain V with finite residue field such that the quotient field of V admits a valuation ring independent of V whose maximal ideal is principal or whose residue field is finite. If the quotient field of V is a purely transcendental extension of an arbitrary field, this property is satisfied. This solves an open problem proposed by Cahen, Fontana, Frisch and Glaz in these cases.

1. Introduction

Non-unique factorization in integral domains has been a recurring topic in commutative ring theory ever since the phenomenon was first discovered in rings of integers in algebraic number fields. The machinery developed in this setting generalizes to Dedekind domains and their (potentially) higher-dimensional analogues, Krull domains. Factorizations in Krull domains (more generally in Krull monoids) are well-studied and can be described by combinatorial structure depending only on the divisor class group and the distribution of prime divisors in the classes, see the monograph by Geroldinger and Halter-Koch [11].

In contrast to this, the (potentially) non-Noetherian generalizations of Dedekind domains, namely, Prüfer domains, are not amenable to the existing methods and (so far) there is no general theory of non-unique factorization in this case. For this reason, the study of non-unique factorizations in Prüfer domains relies on ad-hoc arguments in each particular case.

The non-Noetherian Prüfer domain where non-unique factorization was first studied is the ring of integer-valued polynomials on $\mathbb{Z}$, that is, $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$. Building on results by Cahen and Chabert [2] and Chapman and MacLane [5], the second author [7] showed that every finite multiset of integers > 1 occurs as the set of lengths (of factorizations into irreducibles) of some polynomial in $\mathrm{Int}(\mathbb{Z})$. This result was generalized to rings of integer-valued polynomials on Dedekind domains with infinitely many maximal ideals of finite index by Nakato, Rissner and the second author [9].

The analogous question for integer-valued polynomials on discrete valuation domains with finite residue field is an open problem:

Mathematics subject classification. primary 11R09, 11C08, 13A05; secondary 12E05, 13F20, 13F05.

Key words. integer-valued polynomials, global fields, irreducible polynomials, factorizations, discrete valuations domains.

V. Fadinger is supported by the Austrian Science Fund (FWF): W1230.

S. Frisch is supported by the Austrian Science Fund (FWF): P 35788.

D. Windisch is supported by the Austrian Science Fund (FWF): P 30934.

Problem. [3, Problem 39] Analyze and describe non-unique factorization in $\mathrm{Int}(V)$, where V is a DVR with finite residue field.

Note that if V has an infinite residue field then $\mathrm{Int}(V) = V[X]$, which has unique factorizations. In the non-trivial case of finite residue fields not much is known yet. Nakato, Rissner and the second author [8, 10] characterized when certain irreducible elements are absolutely irreducible in $\mathrm{Int}(V)$. The binomial polynomials in $\mathrm{Int}(\mathbb{Z})$ were shown to be absolutely irreducible by Rissner and the third author [14].

Returning to sets of lengths in $\mathrm{Int}(D)$, the methods used so far [7, 9] rely heavily on the existence of prime ideals of arbitrarily large index and, hence, do not apply to the case of discrete valuation domains.

Using combinatorial linear algebra, we are able to approach this problem for discrete valuation domains in certain fields, obtaining the following

Theorem. Let V be a discrete valuation domain with finite residue field. Suppose that the quotient field K of V admits a valuation ring independent from V whose maximal ideal is principal. Let k be a positive integer and $1 < n_1 \leq \ldots \leq n_k$ integers.

Then there exists an integer-valued polynomial $H \in \mathrm{Int}(V)$ which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lengths are exactly $n_1, \ldots, n_k$.

It is implicit in our proof that the monic irreducible polynomials of degree n lie dense (with respect to the V-adic topology on K) in the set of all monic polynomials of degree n over a field K as above. So this is true in particular for global fields, but fails for local field as we show in Remark 5.6. From the above theorem, we immediately obtain the following three corollaries.

Corollary. Let V be a valuation ring of a global field. Let k be a positive integer and $1 < n_1 \leq \ldots \leq n_k$ integers.

Then there exists an integer-valued polynomial $H \in \mathrm{Int}(V)$ which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lengths are exactly $n_1, \ldots, n_k$.

Corollary. Let V be a discrete valuation domain with finite residue field such that the quotient field of V is a purely transcendental extension of an arbitrary field. Let k be a positive integer and $1 < n_1 \leq \ldots \leq n_k$ integers.

Then there exists an integer-valued polynomial $H \in \mathrm{Int}(V)$ which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lengths are exactly $n_1, \ldots, n_k$.

Corollary. Let V be a discrete valuation domain with finite residue field. Suppose that the quotient field K of V is a finite extension of a field L that admits a valuation ring independent from $V \cap L$ whose maximal ideal is principal or whose residue field is finite. Let k be a positive integer and $1 < n_1 \leq \ldots \leq n_k$ integers.

Then there exists an integer-valued polynomial $H \in \mathrm{Int}(V)$ which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lengths are exactly $n_1, \ldots, n_k$.

Finally, in Remark 5.6, we point out that discretely valued henselian fields are not approachable by our methods.

2. Preliminaries

Factorizations. We give an informal presentation of factorizations. The interested reader is refered to the monograph by Geroldinger and Halter-Koch [11] for a systematic introduction.

Let R be an integral domain and $r \in R$. We say that r is *irreducible* (in R) if it cannot be written as the product of two nonunits of R. A *factorization* of r is a decomposition

$$r = a_1 \cdots a_n$$

into irreducible elements a_i of R. In this case n is called the *length* of this factorization of r. Let s be a further element of R. We say that r and s are associated if there exists a unit $\epsilon \in R$ such that $r = \epsilon s$. We want to consider factorizations up to order and associates. In other words two factorizations

$$r = a_1 \cdots a_n = u_1 \cdots u_m$$

of r are *essentially the same* if $n = m$ and, after renumbering if necessary, u_i is associated to a_i for all $i \in \{1, \ldots, n\}$. Otherwise, they are called *essentially different.*

Valuations. Let K be a field. A valuation v on K is a map

$$\mathsf{v} : K^\times \to G$$

where $(G, +, \leq)$ is a totally ordered Abelian group, subject to the following conditions for all $a, b \in K^\times$:

(1) $\mathsf{v}(a \cdot b) = \mathsf{v}(a) + \mathsf{v}(b)$ and
(2) $\mathsf{v}(a + b) \geq \inf\{\mathsf{v}(a), \mathsf{v}(b)\}$.

If $G \cong \mathbb{Z}$ then v is called a *discrete (rank one) valuation.* The set $\{0\} \cup \{x \in K^\times \mid \mathsf{v}(x) \geq 0\}$ is a subring of K and called the *valuation ring* of v. If v is a discrete (rank one) valuation on K, then there exists a valuation $\mathsf{w} : K^\times \to \mathbb{Z}$ with the same valuation ring. We call w the *normalized valuation* of this valuation ring.

We will use frequently using the following fact without further mention, which is to find in [1, Chapter VI, § 3, Proposition 1]: If v is a valuation on K and $a, b \in K$ are such that $\mathsf{v}(a) \neq \mathsf{v}(b)$ then $\mathsf{v}(a + b) = \inf\{\mathsf{v}(a), \mathsf{v}(b)\}$.

For a general introduction to valuations, see [1].

Discrete valuation domains. An integral domain V with quotient field K is said to be a *discrete (rank one) valuation domain* (DVR) if it satisfies one of the following equivalent statements:

(1) V is the valuation ring of a discrete (rank one) valuation on K.
(2) V is a unique factorization domain with a unique prime element up to associates.
(3) V is a principal ideal domain with a unique non-zero prime ideal.
(4) V is a local Dedekind domain but not a field.

If V is a DVR with normalized valuation v then the prime elements of V (which are all associated) are precisely the elements $p \in V$ with $\mathsf{v}(p) = 1$.

If M is the unique maximal ideal of V then V/M is called its *residue field.*

Fields. By a *global field* we mean a finite extension either of the field of rational numbers $\mathbb{Q}$ or of a field of rational functions $\mathbb{F}(T)$ in one variable over a finite field $\mathbb{F}$. The first type is refered to as *algebraic number field* and the second as *algebraic function field.* Note that every valuation ring of a global field is a discrete (rank one) valuation domain.

Integer-valued polynomials. Let R be an integral domain with quotient field K. The set

$$\operatorname{Int}(R) = \{f \in K[X] \mid f(R) \subseteq R\}$$

is a subring of $K[X]$ and called the *ring of integer-valued polynomials* on R. Let V be a valuation domain with valuation v on its quotient field K. Every element $f \in K[X]$ can be written in the form $f = \frac{g}{d}$, where $g \in V[X]$ and $d \in V \setminus \{0\}$. It is immediate that $f \in \operatorname{Int}(V)$ if and only if $\min_{a \in V} \mathsf{v}(f(a)) \geq \mathsf{v}(d)$.

For a detailed treatment of integer-valued polynomials we refer to the monograph by Cahen and Chabert [4].

3. Glueing of polynomials

Let V be a discrete valuation domain with finite residue field. Let K be the quotient field of V. The purpose of this section is to construct monic polynomials in $V[X]$ of a given degree that are irreducible over K and behave similarly as a given product of linear factors with respect to the valuation of V. We can solve this problem in two cases, see Lemma 3.3 and Lemma 3.4. We understand this as a sort of glueing process of linear factors into something indecomposable.

Remark 3.1. Let K be a field and W a valuation domain of K with corresponding valuation w and maximal ideal M. The following are easily seen to be equivalent:

(a) M is principal and W is not a field.
(b) The value group of w has a minimal element > 0.
(c) $M \neq M^2$.

Therefore we use these three properties interchangeably throughout the manuscript.

Proof. We only have to argue that (a) is equivalent to (c). Suppose that $M = M^2$ and let $x \in M$, that is, $\mathsf{w}(x) > 0$. Since $x \in M^2$, there exist $x_1, \ldots, x_n, y_1, \ldots, y_n \in M$ such that $x = \sum_{i=1}^n x_i y_i$. Now,

$$\mathsf{w}(x) \geq \min_i \mathsf{w}(x_i y_i)$$

and hence $\mathsf{w}(x) \geq \mathsf{w}(x_i) + \mathsf{w}(y_i)$ for some i. Since $\mathsf{w}(x_i), \mathsf{w}(y_i) > 0$, it follows that $\mathsf{w}(x)$ cannot be minimal > 0.

Conversely, suppose that the value group of w does not have a minimal element > 0. Let $x \in M$ and $y \in M$ with $\mathsf{w}(x) > \mathsf{w}(y) > 0$. Pick $z \in M$ with $\mathsf{w}(z) = \mathsf{w}(x) - \mathsf{w}(y) > 0$. Then $\mathsf{w}(x) = \mathsf{w}(yz)$ and therefore there exists $\varepsilon \in W^\times$ such that $x = (\varepsilon y) \cdot z \in M^2$. □

Lemma 3.2. Let W be a local and integrally closed domain with quotient field K and let N be the maximal ideal of W. Let $F = \sum_{i=0}^n d_i X^i \in W[X]$ with the following properties:

(i) $d_n \notin N$.
(ii) $d_i \in N$ for all $i \in \{0, \ldots, n-1\}$.
(iii) $d_0 \notin N^2$.

Then F is irreducible in $K[X]$.

Proof. We first show that F is not a product of two non-constants in $W[X]$. Assume to the contrary that $F = ST$ where $S, T \in W[X] \setminus W$. Then

$$\overline{S} \cdot \overline{T} = \overline{F} = \overline{d_n} X^n,$$

where $\overline{\cdot}$ denotes the reduction modulo N. Since W/N is a field, it follows that

$$\overline{S} = \overline{b} X^s, \overline{T} = \overline{c} X^t,$$

where $\overline{b} \cdot \overline{c} = \overline{d_n} \neq 0$ and $s + t = n$, $s \neq n \neq t$. So the constant terms of S and T lie in M, contradicting $d_0 \notin M^2$.

Since $d_n \notin N$, we can assume without loss of generality that F is monic. Now W is integrally closed, whence F is also irreducible in $K[X]$ by [1, Chapter 5, § 1.3, Proposition 11]. □

Lemma 3.3. Let V be a discrete valuation domain whose quotient field K admits a valuation domain independent from V whose maximal ideal is principal. Let $\mathsf{v} : K^\times \to \mathbb{Z}$ be the normalized valuation of V and $R_1, \dots, R_q$ be the residue classes of V. For each $k \in \{1, \dots, q\}$ choose $r_k \in R_k$ arbitrary. Let $a_1, \dots, a_n \in V$ with $\mathsf{v}(r_k - a_i) \in \{0, 1\}$ for all i, k and set $f = \prod_{i=1}^{n}(X - a_i)$.

Then there exists $F \in V[X]$ irreducible over K with $\deg(F) = n$ such that $\min\{\mathsf{v}(f(a)) \mid a \in R_k\} = \min\{\mathsf{v}(F(a)) \mid a \in R_k\} = \mathsf{v}(F(r_k))$ for all $k \in \{1, \dots, q\}$.

Proof. Let $b_0, \dots, b_n \in V$ such that $f = \sum_{i=0}^{n} b_i X^i$. Let w be a valuation on K independent from v whose value group admits a minimal element $1 > 0$, see Remark 3.1. Choose $c_0, \dots, c_{n-1} \in K$ such that $\mathsf{v}(c_i) = n + 1$ and $\mathsf{w}(b_i + c_i) = 1$ for all $i \in \{0, \dots, n - 1\}$ which is possible by [12, Theorem 22.9]. Let $F = f + \sum_{i=0}^{n-1} c_i X^i$ which is irreducible over K by applying Lemma 3.2 with respect to w. Clearly, $\deg(F) = n$.

Let $k \in \{1, \dots, q\}$. Then $\mathsf{v}(f(r_k)) = \min\{\mathsf{v}(f(a)) \mid a \in R_k\}$. Also

$$\mathsf{v}(F(r_k)) = \min\{\mathsf{v}(f(r_k)), \mathsf{v}(\sum_{i=0}^{n-1} c_i r_k^i)\} = \mathsf{v}(f(r_k))$$

because $\mathsf{v}(c_i) = n + 1$ and therefore $\mathsf{v}(f(r_k)) \leq n < \mathsf{v}(\sum_{i=0}^{n-1} c_i r_k^i)$. If now $a \in R_k$ then

$$\begin{aligned} \mathsf{v}(F(a)) &= \mathsf{v}(f(a) + \sum_{i=0}^{n-1} c_i a^i) \\ &\geq \min\{\mathsf{v}(f(a)), \mathsf{v}(\sum_{i=0}^{n-1} c_i a^i)\} \\ &\geq \mathsf{v}(f(r_k)) = \mathsf{v}(F(r_k)). \end{aligned}$$

□

Lemma 3.4. Let V be a discrete valuation domain whose quotient field K admits a valuation domain W independent from V whose residue field is finite. Let $\mathsf{v} : K^\times \to \mathbb{Z}$ be the normalized valuation of V and $R_1, \dots, R_q$ be the residue classes of V. For each $k \in \{1, \dots, q\}$ choose $r_k \in R_k$ arbitrary. Let $a_1, \dots, a_n \in V$ with $\mathsf{v}(r_k - a_i) \in \{0, 1\}$ for all i, k and set $f = \prod_{i=1}^{n}(X - a_i)$.

Then there exists $F \in V[X]$ irreducible over K with $\deg(F) = n$ such that $\min\{\mathsf{v}(f(a)) \mid a \in R_k\} = \min\{\mathsf{v}(F(a)) \mid a \in R_k\} = \mathsf{v}(F(r_k))$ for all $k \in \{1, \dots, q\}$.

Proof. Let $b_0, \dots, b_{n-1} \in V$ such that $f = X^n + \sum_{i=0}^{n-1} b_i X^i$. Let w be a valuation on K with valuation ring W, P the maximal ideal of W and $R = V \cap W$. We construct a monic polynomial $F = X^n + \sum_{i=0}^{n-1} F_i X^i \in R[X]$ that is irreducible in $K[X]$ and satisfies $\mathsf{v}(b_i - F_i) > n$ for $i \in \{0, \dots, n - 1\}$. Afterwards, we show that this suffices for the assertion of the lemma.

It is well-known that there exist irreducible polynomials of every degree over a finite field. In particular, we can choose $g = X^n + \sum_{i=0}^{n-1} g_i X^i \in W[X]$ a monic polynomial of degree n that is irreducible in $(W/P)[X]$. By [12, Theorem 22.9], there exist $F_0, \dots, F_{n-1} \in K$ such that $\mathsf{v}(b_i - F_i) > n$ and $\mathsf{w}(g_i - F_i) > 0$. Let $F = X^n + \sum_{i=0}^{n-1} F_i X^i$. Then $F \in R[X]$ and F is irreducible in $(W/P)[X]$, because its reduction $\overline{F}$ modulo P is the same as the one of g.

We first show that F is irreducible in $W[X]$. Let $F = ST$ where $S, T \in W[X]$. Then $\overline{S} \cdot \overline{T} = \overline{F}$. Since $\overline{F}$ is irreducible, it follows that either $\overline{S}$ or $\overline{T}$ is a unit in $(W/P)[X]$. Since F is monic, it follows that either S or T is in fact a unit in $W[X]$, whence F is irreducible in $W[X]$. W is integrally closed and, therefore, F is also irreducible in $K[X]$ by [1, Chapter 5, § 1.3, Proposition 11].

Now, for each $k \in \{1, \ldots, q\}$,

$$\mathsf{v}(f(r_k) - F(r_k)) = \mathsf{v}(\sum_{i=0}^{n-1}(b_i - F_i)r_k^i) > n \geq \mathsf{v}(f(r_k)) \geq \min\{\mathsf{v}(f(r_k)), \mathsf{v}(F(r_k))\}.$$

It follows that $\mathsf{v}(f(r_k)) = \mathsf{v}(F(r_k))$. It remains to prove that $\min\{\mathsf{v}(F(a)) \mid a \in R_k\} = \mathsf{v}(F(r_k))$. So let $b \in R_k$ such that $\mathsf{v}(F(b)) = \min\{\mathsf{v}(F(a)) \mid a \in R_k\}$. Then

$$\mathsf{v}(f(b) - F(b)) = \mathsf{v}(\sum_{i=0}^{n-1}(b_i - F_i)b^i) > n \geq \mathsf{v}(f(r_k)) = \mathsf{v}(F(r_k)) \geq \mathsf{v}(F(b)),$$

so $\mathsf{v}(F(r_k)) = \mathsf{v}(f(r_k)) \leq \mathsf{v}(f(b)) = \mathsf{v}(F(b))$. □

4. Combinatorial toolbox

Notation 4.1. Let n be a positive integer. We write $[n] = \{1, \ldots, n\}$.

Notation 4.2. Let $2 \leq k$, $2 \leq n_1 \leq \ldots \leq n_k$ be integers, $i, j \in \{1, \ldots, k\}$ with $i < j$, $S \subseteq [n_i]$, and $T \subseteq [n_j]$. We set

$$H_{i,j}(S, T) = H_{j,i}(T, S) = [n_1] \times \ldots \times [n_{i-1}] \times S \times [n_{i+1}] \times \ldots \times [n_{j-1}] \times T \times [n_{j+1}] \times \ldots \times [n_k].$$

For $s \in [n_i]$, we define $H_{i,j}(s, T) = H_{i,j}(\{s\}, T)$. Moreover, we write $H_{i,j}(S, [n_j]) = H_i(S)$.

Note that the $H_i(s)$ are $(k-1)$-dimensional hyperplanes in the grid $[n_1] \times \ldots \times [n_k]$. Analogously, the $H_{i,j}(s, t)$ are $(k-2)$-dimensional hyperplanes.

Lemma 4.3. Let $k > 2$ and $1 < n_1 \leq \ldots \leq n_k$ be integers. Let $I \subseteq [n_1] \times \ldots \times [n_k]$. Assume that for every $i \in \{1, \ldots, k\}$ and $r \in [n_i]$ there exists $j \in \{1, \ldots, k\} \setminus \{i\}$ and $T \subseteq [n_j]$ such that $I \cap H_i(r) = H_{i,j}(r, T)$. In other words, every intersection of I with a $(k-1)$-dimensional hyperplane is the union of $(k-2)$-dimensional parallel hyperplanes.

Then there exists $\ell \in \{1, \ldots, k\}$ and $S \subseteq [n_\ell]$ such that $I = H_\ell(S)$. That is, I is the union of $(k-1)$-dimensional parallel hyperplanes.

Proof. If $I = \emptyset$ then the statement is trivial. Assume that $I \neq \emptyset$. Let $s \in [n_1]$ such that $H_1(s) \cap I \neq \emptyset$. By the hypothesis of the lemma there exists $j \in \{2, \ldots, k\}$ and $T_j \subseteq [n_j]$ such that $H_1(s) \cap I = H_{1,j}(s, T_j)$.

Case 1. $T_j = [n_j]$. If we can prove for every $m \in [n_1]$ with $H_1(m) \cap I \neq \emptyset$ that $H_1(m) \subseteq I$, we are done by setting $\ell = 1$ and $S = \{m \in [n_1] \mid H_1(m) \cap I \neq \emptyset\}$. So let $m \in [n_1]$ with $H_1(m) \cap I \neq \emptyset$ and $(m, m_2, \ldots, m_k) \in H_1(m) \cap I$. For $i \in \{2, \ldots, k\}$, we obtain

$$H_{1,i}(s, m_i) \cap I = H_i(m_i) \cap H_1(s) \cap I = H_i(m_i) \cap H_1(s) = H_{1,i}(s, m_i),$$

where the second equality follows from $T_j = [n_j]$. Hence, $H_{i,1}(m_i, s) = H_{1,i}(s, m_i) \subseteq I$ for every $i \in \{2, \ldots, k\}$.

For fixed $i \in \{2, \ldots, k\}$, by the hypothesis of the lemma, there exist $j_i \in \{1, \ldots, k\} \setminus \{i\}$ and $T_i \subseteq [n_{j_i}]$ such that $I \cap H_i(m_i) = H_{i,j_i}(m_i, T_i)$. Now $H_{i,1}(m_i, s) \subseteq I \cap H_i(m_i) = H_{i,j_i}(m_i, T_i)$, and therefore $j_i = 1$ and $m \in T_i$. So $I \cap H_i(m_i) = H_{i,1}(m_i, T_i) \supseteq H_{i,1}(m_i, m) = H_{1,i}(m, m_i)$ for every $i \in \{2, \ldots, k\}$.

Again, by the hypothesis of the lemma, there exists $j \in \{2, \ldots, k\}$ and $L \subseteq [n_j]$ such that $H_1(m) \cap I = H_{1,j}(m, L)$. Choose $i \in \{2, \ldots, k\} \setminus \{j\}$. Then $H_{1,i}(m, m_i) \subseteq H_1(m) \cap I = H_{1,j}(m, L)$. It follows that $L = [n_j]$ and hence $H_1(m) \cap I = H_1(m)$.

Case 2. $T_j \neq [n_j]$. Let $i \in \{1, \ldots, k\} \setminus \{1, j\}$. Choose $x \in [n_i]$ arbitrary. Then $H_i(x) \cap I \neq \emptyset$. By the hypothesis of the lemma, there exist $j' \in \{1, \ldots, k\} \setminus \{i\}$ and $L \subseteq [n_{j'}]$ such that $H_i(x) \cap I = H_{i,j'}(x, L)$. Clearly, $H_1(s) \cap H_{i,j'}(x, L) \subseteq I \cap H_1(s) = H_{1,j}(s, T_j)$. Since $j \notin \{1, i\}$ and $T_j \neq [n_j]$, it follows that $j' = j$ and $L \subseteq T_j$ (for otherwise, $H_1(s) \cap H_{i,j'}(x, L) \subseteq H_{1,j}(s, T_j)$ would contain an element whose j-th coordinate is in $[n_j] \setminus T_j$). Hence $H_i(x) \cap I = H_{i,j}(x, T_j)$.

Since $x \in [n_i]$ was chosen arbitrary, we obtain

$$I = \bigcup_{x \in [n_i]} (H_i(x) \cap I) = \bigcup_{x \in [n_i]} H_{i,j}(x, T_j) = H_j(T_j)$$

and we are done choosing $\ell = j$ and $S = T_j$. □

Notation 4.4. Let $k > 1$ and $1 < n_1 \leq \ldots \leq n_k$ be integers. By $\mathbb{Q}^{n_1 \times \ldots \times n_k}$ we denote the set of all $(n_1 \times \ldots \times n_k)$–tensors, that is, the k-dimensional analogues of matrices over $\mathbb{Q}$. Let $M \in \mathbb{Q}^{n_1 \times \ldots \times n_k}$. For $i \in [n_1] \times \ldots \times [n_k]$, we write M_i for the entry of M indexed by i.

For $I \subseteq [n_1] \times \ldots \times [n_k]$, let $Z_I = \{M \in \mathbb{Q}^{n_1 \times \ldots \times n_k} \mid \sum_{i \in I} M_i = 0\}$. Moreover,

$$Z := \bigcap_{\substack{\ell \in \{1, \ldots k\} \\ r \in [n_\ell]}} Z_{H_\ell(r)}.$$

For instance, if $k = 2$ then Z is the set of all $(n_1 \times n_2)$–matrices with all row and column sums equal to 0.

Since the elements of Z are defined by the property that sums over hyperplanes are 0, clearly, sums over disjoint unions of hyperplanes are also 0. The next lemma shows that no other sum of a subset of the entries of $M \in Z$ is necessarily 0. We will use it to show the existence of a tensor $M \in \mathbb{Q}^{n_1 \times \ldots \times n_k}$ such that the sum over a subset of the entries of M is 0 if and only if the corresponding index set is a disjoint union of hyperplanes.

Lemma 4.5. Let $k > 1$ and $1 < n_1 \leq \ldots \leq n_k$ be integers. Let $I \subseteq [n_1] \times \ldots \times [n_k]$ be non-empty such that $I \neq H_\ell(S)$ for all $\ell \in \{1, \ldots, k\}$ and $S \subseteq [n_\ell]$.

Then $Z \setminus Z_I \neq \emptyset$.

Proof. We do an induction on k. If $k = 2$, we deal with $(n_1 \times n_2)$–matrices and we have to show that there exists a matrix $M \in \mathbb{Q}^{n_1 \times n_2}$ all whose row and column sums are 0 and such that $\sum_{i \in I} M_i \neq 0$.

Let $I' = I \setminus \bigcup_{H_1(s) \subseteq I} H_1(s)$. Note that I' originates from I when removing all rows fully contained in I. It suffices to show the assertion for I', so assume without loss of generality that $I = I'$. Now, note that there exists $(i_1, j_1) \in I$ such that neither the i_1-th row nor the j_1-th column is contained in I. Let $i_2 \in [n_1]$ such that $(i_2, j_1) \notin I$. In the same way, let $j_2 \in [n_2]$ such that $(i_1, j_2) \notin I$. Define the matrix $M \in Z$ via

$$M_i = \begin{cases} 1 \text{ if } i \in \{(i_1, j_1), (i_2, j_2)\}, \\ -1 \text{ if } i \in \{(i_1, j_2), (i_2, j_1)\}, \\ 0 \text{ otherwise.} \end{cases}$$

Then $\sum_{i\in I} M_i \in \{1,2\}$, hence $M \in Z \setminus Z_I$.

Now, let $k > 2$. By Lemma 4.3, there exist $i \in \{1,\dots,k\}$ and $r \in [n_i]$ such that $J := I \cap H_i(r) \neq H_{i,j}(r,T)$ for every $j \in \{1,\dots,k\}$ and $T \subseteq [n_j]$. By the induction hypothesis, we find a $(k-1)$-dimensional tensor N indexed by elements of $H_i(r)$ such that $\sum_{d\in H_{i,j}(r,s)} N_d = 0$ and $\sum_{d\in J} N_d \neq 0$. We define

$$M_d = \begin{cases} N_d \text{ if } d \in H_i(r), \\ 0 \text{ otherwise.} \end{cases}$$

Then $M \in Z \setminus Z_I$. ☐

We use the following fact from combinatorial linear algebra.

Fact 4.6. Let K be an infinite field and V a finite-dimensional K-vector space. Let $W, W_1, \dots, W_n$ be linear subspaces of V such that $W \subseteq \bigcup_{j=1}^n W_j$.

Then there exists $j \in \{1,\dots,n\}$ such that $W \subseteq W_j$.

Proof. This is a known fact of combinatorial linear algebra [6, Theorem 4]. ☐

Proposition 4.7. Let k be a positive integer and $1 < n_1 \leq \ldots \leq n_k$ integers. Then there exists $M \in Z$ such that $M \in Z_I$ only if I is a disjoint union of hyperplanes, that is, $I = H_\ell(S)$ for some $\ell \in \{1,\dots,k\}$ and $S \subseteq [n_\ell]$.

Proof. Note that Z_I is a subspace of $\mathbb{Q}^{n_1\times\ldots\times n_k}$ for every $I \subseteq [n_1]\times\ldots\times[n_k]$. Assume that the statement of the proposition does not hold. Then there are finitely many non-empty $I_1,\dots,I_n \subseteq [n_1]\times\ldots\times[n_k]$ such that for each $j \in \{1,\dots,n\}$ it holds that $I_j \neq H_\ell(S)$ whenever $\ell \in \{1,\dots,k\}$ and $S \subseteq [n_\ell]$ and $Z \subseteq \bigcup_{j=1}^n Z_{I_j}$. It follows by Fact 4.6 that $Z \subseteq Z_{I_j}$ for some j. This is a contradiction to Lemma 4.5. ☐

5. Sets of lengths of integer-valued polynomials over a DVR

Lemma 5.1. Let V be a discrete valuation domain with finite residue field of cardinality q. Let K be the quotient field of V, $\mathsf{v} : K^\times \to \mathbb{Z}$ its normalized valuation and $\pi \in V$ a prime element, that is, $\mathsf{v}(\pi) = 1$. By $R_1,\dots,R_q$ denote the residue classes of V modulo the maximal ideal.

Let $F_1,\dots,F_r,G_1,\dots,G_s \in V[X]$ irreducible over K such that

(i) $e := \min\{\sum_{i=1}^r \mathsf{v}(F_i(a)) \mid a \in R_1\} = \min\{\sum_{j=1}^s \mathsf{v}(G_j(a)) \mid a \in R_k\}$ for all $k \in \{2,\dots,q\}$,

(ii) $\min\{\mathsf{v}(G_j(a)) \mid a \in R_1\} = 0$ for all $j \in \{1,\dots,s\}$,

(iii) $\min\{\mathsf{v}(F_i(a)) \mid a \in R_k\} = 0$ for all $i \in \{1,\dots,r\}$ and $k \in \{2,\dots,q\}$.

Define

$$H = \frac{(\prod_{i=1}^r F_i)(\prod_{j=1}^s G_j)}{\pi^e}.$$

Then $H \in \mathrm{Int}(V)$. Furthermore, H is a product of two non-units in $\mathrm{Int}(V)$ if and only if there exist non-empty $I \subsetneqq \{1,\dots,r\}$ and $J \subsetneqq \{1,\dots,s\}$ such that $\min\{\sum_{i\in I} \mathsf{v}(F_i(a)) \mid a \in R_1\} = \min\{\sum_{j\in J} \mathsf{v}(G_j(a)) \mid a \in R_k\}$ for all $k \in \{2,\dots,q\}$.

Proof. Clearly H is integer-valued over V. If there exist I and J as in the lemma, define $e' = \min_{a\in R_1} \sum_{i\in I} \mathsf{v}(F_i(a)) = \min_{a\in R_k} \sum_{j\in J} \mathsf{v}(G_j(a))$ (for $k \in \{2,\dots,q\}$). Then clearly

$$H = \frac{(\prod_{i\in I} F_i)(\prod_{j\in J} G_j)}{\pi^{e'}} \cdot \frac{(\prod_{i\in\{1,\dots,r\}\setminus I} F_i)(\prod_{j\in\{1,\dots,s\}\setminus J} G_j)}{\pi^{e-e'}}$$

is a decomposition into two non-units in $\mathrm{Int}(V)$.

Conversely, if $H = H_1 \cdot H_2$ is a decomposition of H where H_1 and H_2 are non-units of $\mathrm{Int}(V)$, then, by [9, Lemma 3.4], there exist non-empty $I \subsetneqq \{1,\dots,r\}$ and $J \subsetneqq \{1,\dots,s\}$ such that

$$H_1 = \frac{(\prod_{i\in I} F_i)(\prod_{j\in J} G_j)}{\pi^{e'}} \text{ and } H_2 = \frac{(\prod_{i\in\{1,\dots,r\}\setminus I} F_i)(\prod_{j\in\{1,\dots,s\}\setminus J} G_j)}{\pi^{e-e'}}$$

for some $e' \in \{0,\dots,e\}$. Assume to the contrary that $\min_{a\in R_1}\sum_{i\in I}\mathsf{v}(F_i(a)) \neq \min_{a\in R_k}\sum_{j\in J}\mathsf{v}(G_j(a))$ for some $k \in \{2,\dots,q\}$. Exchanging, if necessary, the roles of I and $\{1,\dots,r\}\setminus I$ respectively J and $\{1,\dots,s\}\setminus J$, we may assume without loss of generality that $\min_{a\in R_1}\sum_{i\in I}\mathsf{v}(F_i(a)) > \min_{a\in R_k}\sum_{j\in J}\mathsf{v}(G_j(a))$. Since H_1 is an integer-valued polynomial on V, it follows that

$$\min_{a\in R_1}\sum_{i\in I}\mathsf{v}(F_i(a)) > \min_{a\in R_k}\sum_{j\in J}\mathsf{v}(G_j(a)) \geq e'.$$

Hence we get

$$\min_{a\in R_1}\sum_{i\in\{1,\dots,r\}\setminus I}\mathsf{v}(F_i(a)) < \min_{a\in R_k}\sum_{j\in\{1,\dots,s\}\setminus J}\mathsf{v}(G_j(a)) \leq e-e',$$

which is a contradiction because $H_2 \in \mathrm{Int}(V)$. □

Lemma 5.2. Let V be a discrete valuation domain with finite residue field of cardinality q and residue classes $R_1,\dots,R_q$. Let K be the quotient field of V, $\mathsf{v}: K^\times \to \mathbb{Z}$ its normalized valuation and $\pi \in V$ a prime element, that is, $\mathsf{v}(\pi) = 1$. Let $F_1,\dots,F_r,G_1,\dots,G_s \in V[X]$ irreducible over K and pairwise non-associated over K such that

(i) $e := \min\{\sum_{i=1}^r \mathsf{v}(F_i(a)) \mid a \in R_1\} = \min\{\sum_{j=1}^s \mathsf{v}(G_j(a)) \mid a \in R_k\}$ for all $k \in \{2,\dots,q\}$,
(ii) $\min\{\mathsf{v}(G_j(a)) \mid a \in R_1\} = 0$ for all $j \in \{1,\dots,s\}$,
(iii) $\min\{\mathsf{v}(F_i(a)) \mid a \in R_k\} = 0$ for all $i \in \{1,\dots,r\}$ and $k \in \{2,\dots,q\}$.

Define

$$H = \frac{(\prod_{i=1}^r F_i)(\prod_{j=1}^s G_j)}{\pi^e}.$$

Then there is a bijective correspondence of the pairs of partitions $\{1,\dots,r\} = I_1 \cup \ldots \cup I_\ell$ and $\{1,\dots,s\} = J_1 \cup \ldots \cup J_\ell$ with the properties that

(1) $e_\lambda := \min\{\sum_{i\in I_\lambda}\mathsf{v}(F_i(a)) \mid a \in R_1\} = \min\{\sum_{j\in J_\lambda}\mathsf{v}(G_j(a)) \mid a \in R_k\}$ for all $k \in \{2,\dots,q\}$ and $\lambda \in \{1,\dots,\ell\}$ and
(2) for all $\lambda \in \{1,\dots,\ell\}$ and all non-empty $I \subsetneqq I_\lambda$ and $J \subsetneqq J_\lambda$ there is $k \in \{2,\dots,q\}$ such that $\min\{\sum_{i\in I}\mathsf{v}(F_i(a)) \mid a \in R_1\} \neq \min\{\sum_{j\in J}\mathsf{v}(G_j(a)) \mid a \in R_k\}$

and of the essentially different factorizations of H into irreducible elements of $\mathrm{Int}(V)$ via

$$(I_1 \cup \ldots \cup I_\ell, J_1 \cup \ldots \cup J_\ell) \mapsto \frac{(\prod_{i\in I_1} F_i)(\prod_{j\in J_1} G_j)}{\pi^{e_1}} \cdot \ldots \cdot \frac{(\prod_{i\in I_\ell} F_i)(\prod_{j\in J_\ell} G_j)}{\pi^{e_\ell}}.$$

Proof. This follows immediately from Lemma 5.1. □

Theorem 1. Let V be a discrete valuation domain with finite residue field. Suppose that the quotient field K of V admits a valuation ring independent from V whose maximal ideal is principal or whose residue field is finite. Let k be a positive integer and $1 < n_1 \leq \ldots \leq n_k$ integers.

Then there exists an integer-valued polynomial $H \in \mathrm{Int}(V)$ which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lengths are exactly $n_1,\dots,n_k$.

Proof. If $k = 1$ then $H = X^{n_1}$ has the desired property. So let $k \geq 2$. By Lemma 5.2 it suffices to construct polynomials F_i and G_j as in the hypothesis of this lemma such that there are exactly k different partitions of the index sets and their cardinalities are exactly $n_1, \dots, n_k$.

We set $r = s = n_1 \cdots n_k$. By Proposition 4.7, there exists a tensor $M \in \mathbb{Q}^{n_1 \times \dots \times n_k}$ such that $M \in Z$ and $M \notin Z_I$ for all non-empty $I \subseteq [n_1] \times \dots \times [n_k]$ such that $I \neq H_\ell(S)$ whenever $\ell \in \{1, \dots, k\}$ and $S \subseteq [n_\ell]$ (see Notation 4.2 and 4.4). Multiplying M with a common denominator of its entries, we may assume without loss of generality that all entries of M are in $\mathbb{Z}$. Then we can write $M = M_F - M_G$ where M_F, M_G are tensors of the same dimensions as M whose entries are positive integers. Recall that $(M_F)_i$ for $i \in [n_1] \times \dots \times [n_k]$ denotes the i-th entry of M_F.

Let $R_1, \dots, R_q$ be the residue classes of V and $\mathsf{v} : K^\times \to \mathbb{Z}$ its normalized valuation. Let $r_m \in R_m$ arbitrary for each $m \in \{1, \dots, q\}$. Since the R_m are infinite, we can pick, for each $i \in [n_1] \times \dots \times [n_k]$, a set of $(M_F)_i$ distinct elements $a_1^{i,1}, \dots, a_{(M_F)_i}^{i,1} \in V$ with $\mathsf{v}(r_1 - a_j^{i,1}) = 1$ for all j, and for each $m \in \{2, \dots, q\}$ a set of $(M_G)_i$ distinct elements $a_1^{i,m}, \dots, a_{(M_G)_i}^{i,m} \in V$ with $\mathsf{v}(r_m - a_j^{i,m}) = 1$ for all j, and such that $a_{j_1}^{i_1,m_1} = a_{j_2}^{i_2,m_2}$ implies $j_1 = j_2$, $i_1 = i_2$ and $m_1 = m_2$.

For each $i \in [n_1] \times \dots \times [n_k]$, we set

$$f_i = \prod_{j=1}^{(M_F)_i} (X - a_j^{i,1}),$$

$$g_i = \prod_{m=2}^{q} \prod_{j=1}^{(M_G)_i} (X - a_j^{i,m}).$$

By Lemma 3.3 respectively Lemma 3.4, there exist, for each $i \in [n_1] \times \dots \times [n_k]$, polynomials $F_i, G_i \in V[X]$ which are all pairwise non-associated and irreducible over K. Moreover, by the choice of f_i and g_i, for all non-empty $I \subseteq [n_1] \times \dots \times [n_k]$ the equality $\min_{a \in R_1} \sum_{i \in I} \mathsf{v}(F_i(a)) = \min_{a \in R_m} \sum_{j \in J} \mathsf{v}(G_j(a))$ holds for all $m \in \{2, \dots, q\}$ if and only if $I = H_r(S)$ for some $r \in \{1, \dots, k\}$ and $S \subseteq [n_r]$.

So the only admissible (in the sense of Lemma 5.2) partitions of the index set $[n_1] \times \dots \times [n_k]$, namely those that correspond to factorizations into irreducibles, are the ones of the form $H_r(1) \cup \dots \cup H_r(n_r)$ for $r \in \{1, \dots, k\}$. These are exactly k many of cardinalities $n_1, \dots, n_k$. $\square$

Corollary 5.3. Let V be a valuation ring of a global field. Let k be a positive integer and $1 < n_1 \leq \dots \leq n_k$ integers.

Then there exists an integer-valued polynomial $H \in \mathrm{Int}(V)$ which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lengths are exactly $n_1, \dots, n_k$.

Proof. Note that a global field has infinitely many non-equivalent discrete valuations. $\square$

Corollary 5.4. Let V be a discrete valuation domain with finite residue field such that the quotient field of V is a purely transcendental extension of an arbitrary field. Let k be a positive integer and $1 < n_1 \leq \dots \leq n_k$ integers.

Then there exists an integer-valued polynomial $H \in \mathrm{Int}(V)$ which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lengths are exactly $n_1, \dots, n_k$.

Proof. The quotient field K of V is also the quotient field of a polynomial ring in one variable over some field and, therefore, K admits infinitely many discrete valuations. $\square$

Corollary 5.5. Let V be a discrete valuation domain with finite residue field. Suppose that the quotient field K of V is a finite extension of a field L that admits a valuation ring independent from $V \cap L$ whose maximal ideal is principal or whose residue field is finite. Let k be a positive integer and $1 < n_1 \leq \ldots \leq n_k$ integers.

Then there exists an integer-valued polynomial $H \in \mathrm{Int}(V)$ which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lengths are exactly $n_1, \ldots, n_k$.

Proof. Let W_L be a valuation domain of L independent from $V \cap L$. Let W be a valuation domain of K extending W_L. Then W and V are independent. In each of the two cases of the assumption, namely, that the maximal ideal of W_L is principal respectively its residue field is finite, the same property follows for W by [1, Chapter VI, § 8.3, Theorem 1] and Remark 3.1. □

Remark 5.6. Unfortunately, our construction (including Lemma 3.3 and Lemma 3.4) fails for henselian valued fields, so, in particular, for local fields.

Let K be a field discretely valued by a henselian valuation v with valuation ring V. Suppose further that V has a finite residue field. Let q, R_k, r_k, a_i and $f = \prod_{i=1}^{n}(X - a_i)$ as in Lemma 3.3. Moreover, let $F \in K[X]$ with $\deg(F) = n$ such that $\min\{\mathsf{v}(f(a)) \mid a \in R_k\} = \min\{\mathsf{v}(F(a)) \mid a \in R_k\} = \mathsf{v}(F(r_k))$ for all $k \in \{1, \ldots, q\}$.

Denote by M the maximal ideal of V and let $r_1 \in M$, that is, $R_1 = M$. Note that in the concrete application of Lemma 3.3 in Theorem 1 at least one of the a_i is in the maximal ideal of V and one is not. In particular, we can assume that $\mathsf{v}(F(r_1)) > 0$ and $\mathsf{v}(F(r_k)) > 0$ for some $k \neq 0$. Based on this, we show that F can never be irreducible over K.

Let $F_0, \ldots, F_{n-1} \in K$ such that $F = X^n + \sum_{j=0}^{n-1} F_j X^j$. Let L be a splitting field of F over K and $c_i \in L$ such that $F = \prod_{i=1}^{n}(X - c_i)$. Since L is a finite extension of K, there exists a unique extension of v to L which we also denote by v. It is clear that

$$\mathsf{v}(F_0) = \mathsf{v}(F(0)) \geq \mathsf{v}(F(r_1)) > 0.$$

Note that there exists a c_i such that $\mathsf{v}(c_i) = 0$, for otherwise $\mathsf{v}(F(r_k)) = 0$. After renumbering if necessary, let $\mathsf{v}(c_1) = \ldots = \mathsf{v}(c_m) = 0$ and $\mathsf{v}(c_i) > 0$ for $i > m$. Then $c_1 \cdots c_m$ is the unique summand of F_{n-m} that has valuation 0, hence $\mathsf{v}(F_{n-m}) = 0$. Therefore the Newton polygon of F has at least two different slopes and thus F is not irreducible over K [13, p. 147].

Based on our results and the previous remark, it is natural to pose the following

Problem 5.7. Determine lengths of factorizations of elements $f \in \mathrm{Int}(V)$ where V is the discrete valuation ring of a henselian valued field.

References

[1] N. Bourbaki, *Commutative algebra: Chapters 1-7*, Elements of Mathematics, Springer, 1989.

[2] Paul-Jean Cahen and Jean-Luc Chabert, *Elasticity for integral-valued polynomials*, J. Pure Appl. Algebra **103** (1995), no. 3, 303–311.

[3] Paul-Jean Cahen, Marco Fontana, Sophie Frisch, and Sarah Glaz, *Open problems in commutative ring theory*, Commutative algebra, Springer, New York, 2014, pp. 353–375.

[4] P.J. Cahen, J.L. Chabert, and American Mathematical Society, *Integer-valued polynomials*, American Mathematical Society Translations, American Mathematical Society, 1997.

[5] Scott T. Chapman and Barbara A. McClain, *Irreducible polynomials and full elasticity in rings of integer-valued polynomials*, J. Algebra **293** (2005), no. 2, 595–610.

[6] Pete L. Clark, *Covering numbers in linear algebra*, The American Mathematical Monthly **119** (2012), no. 1, 65–67.

[7] Sophie Frisch, *A construction of integer-valued polynomials with prescribed sets of lengths of factorizations*, Monatsh. Math. **171** (2013), no. 3-4, 341–350.

[8] Sophie Frisch and Sarah Nakato, *A graph-theoretic criterion for absolute irreducibility of integer-valued polynomials with square-free denominator*, Comm. Algebra **48** (2020), no. 9, 3716–3723.
[9] Sophie Frisch, Sarah Nakato, and Roswitha Rissner, *Sets of lengths of factorizations of integer-valued polynomials on dedekind domains with finite residue fields*, J. Algebra **528** (2019), 231–249.
[10] Sophie Frisch, Sarah Nakato, and Roswitha Rissner, *Split absolutely irreducible integer-valued polynomials over discrete valuation domains*, J. Algebra **602** (2022), 247–277.
[11] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: Algebraic, combinatorial and analytic theory*, Chapman & Hall/CRC Pure and Applied Mathematics, CRC Press, 2006.
[12] Robert Gilmer, *Multiplicative Ideal Theory*, Queen's papers in pure and applied mathematics, Queen's University, 1992.
[13] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, Springer Berlin Heidelberg, 1999.
[14] Roswitha Rissner and Daniel Windisch, *Absolute irreducibility of the binomial polynomials*, J. Algebra **578** (2021), 92–114.

Victor Fadinger, Institute for Mathematics and Scientific Computing, Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria
E-mail address: victor.fadinger@uni-graz.at

Sophie Frisch, Department of Analysis and Number Theory (5010), Technische Universität Graz, Kopernikusgasse 24, 8010 Graz, Austria
E-mail address: frisch@math.tugraz.at

Daniel Windisch, Department of Analysis and Number Theory (5010), Technische Universität Graz, Kopernikusgasse 24, 8010 Graz, Austria
E-mail address: dwindisch@math.tugraz.at