Journal of Algebra 633 (2023) 696–721

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

Characterizing absolutely irreducible integer-valued polynomials over discrete valuation domains

Moritz Hiebler[a], Sarah Nakato[b,1], Roswitha Rissner[a,*,2]

[a] *Department of Mathematics, University of Klagenfurt, Universitätsstraße 65-67, 9020 Klagenfurt am Wörthersee, Austria*

[b] *Department of Mathematics, Kabale University, Plot 364 Block 3 Kikungiri Hill, Kabale, Uganda*

A R T I C L E I N F O

Article history:
Received 29 November 2022
Available online 13 July 2023
Communicated by Steven Dale Cutkosky

MSC:
13A05
11S05
11R09
13B25
13F20
11C08

Keywords:
Non-unique factorization
Irreducible elements
Absolutely irreducible elements
Integer-valued polynomials

A B S T R A C T

Rings of integer-valued polynomials are known to be atomic, non-factorial rings furnishing examples for both irreducible elements for which all powers factor uniquely (*absolutely irreducibles*) and irreducible elements where some power has a factorization different from the trivial one.

In this paper, we study irreducible polynomials $F \in \mathrm{Int}(R)$ where R is a discrete valuation domain with finite residue field and show that it is possible to explicitly determine a number $S \in \mathbb{N}$ that reduces the absolute irreducibility of F to the unique factorization of F^S.

To this end, we establish a connection between the factors of powers of F and the kernel of a certain linear map that we associate to F. This connection yields a characterization of absolute irreducibility in terms of this so-called *fixed divisor kernel*. Given a non-trivial element $\boldsymbol{v}$ of this kernel, we explicitly construct non-trivial factorizations of F^k, provided that $k \geq L$, where L depends on F as well as the choice of $\boldsymbol{v}$. We further show that this bound cannot be improved in general. Additionally, we provide other (larger) lower bounds

* Corresponding author.
E-mail addresses: moritz.hiebler@gmx.at (M. Hiebler), snakato@kab.ac.ug (S. Nakato), roswitha.rissner@aau.at (R. Rissner).

[1] S. Nakato is supported by the Austrian Science Fund (FWF): P 30934.
[2] R. Rissner is supported by the Austrian Science Fund (FWF): DOC 78.

https://doi.org/10.1016/j.jalgebra.2023.06.026

for k, one of which only depends on the valuation of the denominator of F and the size of the residue class field of R.

1. Introduction

In atomic domains which allow non-unique factorizations, powers of irreducible elements c may or may not have a factorization other than the trivial one, that is, $c \cdots c$. Those irreducible elements all of whose powers (essentially) factor uniquely are the so-called *absolutely irreducible* elements, a notion that "bridges" the gap between prime and irreducible elements. A thorough understanding of the factorization behavior of such a ring necessarily requires comprehension of its irreducible elements and the factorization behavior of their powers.

Rings of integer-valued polynomials,

$$\operatorname{Int}(D) = \{F \in K[x] \mid F(D) \subseteq D\}$$

where D is a domain with quotient field K, are known to provide examples for both absolutely irreducible elements and irreducible elements that are not absolutely irreducible, see Angermüller's recent publication [2] and, for example, Nakato's article [24] for explicit constructions in $\operatorname{Int}(\mathbb{Z})$. Note that in the literature, absolutely irreducible elements have also been called completely irreducible [20] and strong atoms [4,11].

In this paper, we study factorizations of powers of (non-constant) irreducible elements $F \in \operatorname{Int}(R)$ where (R, pR) is a discrete valuation domain with finite residue field. In order to prove that F is not absolutely irreducible, it suffices to allege a non-trivial factorization of some power F^k. Proving absolute irreducibilty, on the other hand, requires to get a handle on the (unique) factorizations of all exponents k for which the powers F^k potentially factor non-uniquely. We establish lower bounds S such that whenever F is not absolutely irreducible, then F^k factors non-uniquely for $k \geq S$. In other words, to determine whether F is absolutely irreducible or not, it suffices to check the factorization behavior of F^S, that is, we only need to treat one power of F instead of infinitely many. Our approach yields a full characterization of all absolutely irreducible polynomials in $\operatorname{Int}(R)$ in terms of the kernel of a certain linear map, which we call the *fixed divisor kernel*.

The focus of factorization theoretic studies has layed on Krull monoids to a large extent so far. For integral domains, Krull domains are exactly those domains whose multiplicative monoid is Krull.

For a discrete valuation domain R with finite residue field, the ring $\operatorname{Int}(R)$ is not Krull but Prüfer, cf. [10,21]. Reinhart [26], however, showed that they are monadically

Krull, that is, he proved that for each $F \in \mathrm{Int}(D)$ (for factorial domains D), the monadic submonoid generated by F,

$$\llbracket F \rrbracket = \{G \in \mathrm{Int}(D) \mid G \text{ divides } F^n \text{ for some } n \in \mathbb{N}\},$$

is Krull and Frisch [15] extended this result to Krull domains. Note that an irreducible polynomial $F \in \mathrm{Int}(D)$ is absolutely irreducible if and only if $\llbracket F \rrbracket$ is factorial.

Factorization-theoretic properties of rings of integer-valued polynomials have been studied over the last decades. The papers of Anderson, Cahen, Chapman and Smith [1], Cahen and Chabert [7] and Chapman and McClain [12] can be considered as the starting point of this line of research and have encouraged further research activity in the area, e.g., [3,13,14,17,25].

Recently, there has been perceptible progress in the study of absolutely irreducible elements in rings of integer-valued polynomials. In addition to the already mentioned references, Rissner and Windisch [27] have confirmed the decade-long open conjecture that the binomial polynomials $\binom{x}{n}$ are absolutely irreducible for all $n \in \mathbb{N}$. The special case where n is a prime number has been verified before by McClain [23] and also follows from Frisch and Nakato's graph-theoretic criterion [16]. The latter provides a characterization of absolutely irreducible integer-valued polynomials over principal ideal domains whose denominators are square-free. One of the consequences of this criterion is that for such polynomials F one can determine absolute irreducibility by checking the unique factorizations of F^3. For integer-valued polynomials whose denominators contain square factors, this criterion is known to be a sufficient, but not a necessary condition for absolute irreducibility. Adding to an overall understanding of absolutely irreducible integer-valued polynomials is the characterization of the class of completely split absolutely irreducible elements of $\mathrm{Int}(R)$ where R is a discrete valuation domain R with finite residue field by Frisch, Nakato, and Rissner [18].

The last two references form the motivational starting point for the paper at hand. We fully characterize the absolutely irreducible elements in $\mathrm{Int}(R)$ where R is a discrete valuation domain with finite residue field and we determine different (explicit) exponents k such that F^k factors uniquely if and only if F is absolutely irreducible. This is not only interesting from a theoretical point of view but also provide means to approach the subject from a computational perspective.

Note that while the bound resulting from the graph-theoretic criterion [16] cannot be improved for integer-valued polynomials over principal ideal domains, it is not tight in the case when the underlying ring is a discrete valuation domain R with finite residue field. Indeed, in the case of a single prime element p in the denominator, it even suffices to check the factorizations of F^2 to determine absolute irreducibility. That is, if $F = \frac{f}{p} \in \mathrm{Int}(R)$ is irreducible but not absolutely irreducible, then, by [16, Theorem 1 and 3], there exists a non-constant irreducible divisor h of f in $R[x]$ such that for all roots a of h modulo p, we have $\mathsf{v}(f(a)) > 1$. Therefore, if $f = gh$ with $g \in R[x]$, we obtain that

$$F^2 = \frac{g^2 h}{p^2} \cdot h$$

is a factorization (not necessarily into irreducibles) of F^2 different from $F \cdot F$.

2. Results

As $\mathrm{Int}(R)$ is trivial for discrete valuation domains R with infinite residue field, we restrict our attention to those with finite residue field, cf. [8, Corollary I.3.7].

Given a (non-constant) irreducible $F \in \mathrm{Int}(R)$, we determine an exponent $S \in \mathbb{N}$ such that F is absolutely irreducible if and only if F^S factors uniquely. We show that integer-valued factors of powers of F are encoded as non-trivial elements of what we call the *fixed divisor kernel*. This allows us not only to determine lower bounds for S (non-unique factorizations trivially transfer to higher powers), but also yields a neat characterization of absolute irreducibility in terms of this special kernel.

As usual in factorization theory, we are only interested in essentially different factorizations, which is why we will not distinguish between associated elements (cf. Remark 3.9). Hence, it suffices to consider polynomials $F \in \mathrm{Int}(R)$ which are of the form $F = \frac{f}{p^n}$ with *fixed divisor* $\mathrm{d}(f) = p^n$ (Definition 3.5) where $f = \prod_{g\in\mathcal{P}} g^{m_g} \in R[x]$ with *irreducible divisor set* $\mathcal{P}$ (Definition 3.4) and the vector of the corresponding multiplicities $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$.

An integer-valued factor of F^j always has to be of the form $H = \frac{\prod_{g\in\mathcal{P}} g^{k_g}}{p^r}$ where $r \leq jn$ (Fact 3.10). Roughly speaking, whether or not F^j has a non-trivial factorization is asking whether it is possible to “suitably re-distribute” the jm_g respective copies of the polynomials g. This, in turn, heavily depends on the values of $(\mathsf{v}(g(a)))_{g\in\mathcal{P}}$ for all $a \in R$.

However, the relevant information about all these valuation vectors can be encoded in the kernel of a certain linear map, the *fixed divisor kernel* $\text{fd-ker}(f)$ of f (Definition 4.1).

Indeed, in Section 4, we show how to use a non-trivial element $\boldsymbol{v} \in \text{fd-ker}(f)$ to explicitly engineer a non-trivial factorization of F^k for $k \geq L$ where L is a bound depending on n, $\boldsymbol{v}$, and the vector of multiplicities $\boldsymbol{m}$, leading to our first main result. Regarding notation, $\boldsymbol{v}^+$ and $\boldsymbol{v}^-$ are the positive and negative part of $\boldsymbol{v}$, respectively, and $\|\lceil \boldsymbol{x} \rceil\|_\infty = \lceil \max_g |x_g| \rceil$.

Theorem 1. *Let (R, pR) be a discrete valuation domain with valuation v and finite residue field. Further, let $f = \prod_{g\in\mathcal{P}} g^{m_g} \in R[x]$ be a primitive, non-constant polynomial with irreducible divisor set $\mathcal{P}$ and $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ the vector of the corresponding multiplicities and assume that $\mathsf{v}(\mathrm{d}(f)) = n \in \mathbb{N}$.*

If $\text{fd-ker}(f) \neq \boldsymbol{0}$, then $F = \frac{f}{p^n}$ is not absolutely irreducible. In fact, if F is irreducible and $\boldsymbol{0} \neq \boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}$, then F^j factors non-uniquely for all $j \in \mathbb{N}$ with $j \geq (n+1)\left(\left\|\left\lceil \frac{\boldsymbol{v}^+}{\boldsymbol{m}} \right\rceil\right\|_\infty + \left\|\left\lceil \frac{\boldsymbol{v}^-}{\boldsymbol{m}} \right\rceil\right\|_\infty\right)$.

We also show that the reverse implication holds, that is, whenever the fixed divisor kernel of f is trivial, then F is absolutely irreducible (where we need to impose a condition on f which is trivially satisfied whenever F is irreducible). This yields our next main result, a characterization of absolutely irreducible polynomials in $\mathrm{Int}(R)$ in terms of the fixed divisor kernel.

Theorem 2. *Let (R, pR) be a discrete valuation domain with valuation v and finite residue field. Further, let $f \in R[x]$ be a primitive, non-constant polynomial with $\mathsf{v}(\mathrm{d}(f)) = n \in \mathbb{N}$ and assume that f is not a proper power of another polynomial in $R[x]$.*

Then $\frac{f}{p^n}$ is absolutely irreducible if and only if $\text{fd-ker}(f) = \mathbf{0}$.

In the remaining paper, we have a closer look at the bound given in Theorem 1. In Section 5, we are able to give an upper bound for

$$\min\{\|\boldsymbol{v}\|_\infty \mid \mathbf{0} \neq \boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}\}$$

using a tailored version of Siegel's lemma (Lemma 5.2). For this purpose, we introduce the notion of a *reduced fdp matrix* $A \in \mathbb{Q}^{W \times \mathcal{P}}$ which is a full row-rank matrix satisfying $\ker(A) = \text{fd-ker}(f)$, where W is a certain finite set of so-called *fixed divisor witnesses* of f (Definitions 4.1 and 5.1). This further allows us to determine other exponents S, one of which depends only on n and the size of the finite residue field of R such that an irreducible polynomial $F = \frac{f}{p^n} \in \mathrm{Int}(R)$ is absolutely irreducible if and only if F^S factors uniquely.

Theorem 3. *Let (R, pR) be a discrete valuation domain with valuation v and let $q = |R/pR|$ be the cardinality of the finite residue field of R. Further, let $f \in R[x]$ be a non-constant, primitive polynomial with irreducible divisor set $\mathcal{P}$ and $(m_g)_{g \in \mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ the vector of the corresponding multiplicities, that is, $f = \prod_{g \in \mathcal{P}} g^{m_g}$. Let $\mathsf{v}(\mathrm{d}(f)) = n \in \mathbb{N}$ and $A \in \mathbb{Q}^{W \times \mathcal{P}}$ (with $W \subseteq \mathcal{W}(f)$) be a reduced fdp matrix of f containing u rows with only one non-zero entry.*

Assume that F is irreducible. Then the following assertions are equivalent:

(i) *F^j factors uniquely for all $j \in \mathbb{N}$, that is, F is absolutely irreducible.*
(ii) *F^S factors uniquely for $S = 2(n+1)n^{q^{\lceil \frac{n}{2} \rceil}}$.*
(iii) *F^S factors uniquely for $S = 2(n+1)n^{\mathrm{rank}(A)-u}$.*

Finally, in Section 6, we discuss the tightness of the given bounds. We show that the bound in Theorem 1 cannot be improved in general. Indeed, for any $n \geq 2$, there exists a discrete valuation domain (R, pR) with finite residue field and an irreducible, integer-valued polynomial $F = \frac{f}{p^n} \in \mathrm{Int}(R)$ such that the minimal S for which F^S factors non-uniquely is exactly the bound given in Theorem 1, minimized over all feasible $\boldsymbol{v}$. We are not only able to determine S explicitly, but also show that it can be made larger than any predefined constant. We point out that, given the numbers in Theorem 3, it follows that the size of the residue field has to grow with the size of S.

Theorem 4. *Let r, $n \geq 2$ be integers.*

*Then there exists a discrete valuation domain (R, pR) with finite residue field and a polynomial $F = \frac{f}{p^n} \in \operatorname{Int}(R)$ which is irreducible, but **not** absolutely irreducible in $\operatorname{Int}(R)$ (both R and F depending on r) such that the minimal exponent S for which F^S does not factor uniquely satisfies*

- (i) $S = (n+1)\left((n-1)^{r-1} + (n-1)^{r-2}\right)$ *where r is the rank of a (reduced) fdp matrix of f and*
- (ii) $S = (n+1)\min\left\{\|\boldsymbol{v}^+\|_\infty + \|\boldsymbol{v}^-\|_\infty \;\middle|\; \mathbf{0} \neq \boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}\right\}$.

In particular, it follows that the lower bound given in Theorem 1 cannot be improved in general.

3. Preliminaries

3.1. Factorizations

We define the factorization terms that we need in this paper, and refer to the textbook of Geroldinger and Halter-Koch [19] for a systematic introduction to non-unique factorizations.

Definition 3.1. Let R be a commutative ring with identity.

- (i) We say that $r \in R$ is *irreducible* in R if it is a non-zero non-unit and it cannot be written as the product of two non-units of R.
- (ii) A *factorization* of $r \in R$ is an expression of r as a product of irreducibles, that is,

$$r = a_1 \cdots a_n$$

  where $n \geq 1$ and a_i is irreducible in R for $1 \leq i \leq n$.
- (iii) We say that r, $s \in R$ are *associated* in R if there exists a unit $u \in R$ such that $r = us$. We denote this by $r \sim s$.
- (iv) Two factorizations of the same element,

$$r = a_1 \cdots a_n = b_1 \cdots b_m, \tag{3.1}$$

  are called *essentially the same* if $n = m$ and, after a suitable re-indexing, $a_j \sim b_j$ for $1 \leq j \leq m$. Otherwise, the factorizations in (3.1) are called *essentially different*.

Definition 3.2. Let R be a commutative ring with identity. An irreducible element $r \in R$ is called *absolutely irreducible* if for all natural numbers n, every factorization of r^n is essentially the same as $r^n = r \cdots r$.

Remark 3.3. A straight-forward verification shows that an irreducible element r is absolutely irreducible if and only if for every $n \in \mathbb{N}$ and every factorization $r^n = c \cdot d$ into the product of (not necessarily irreducible) elements c and $d \in R$, it follows that $c \sim r^k$ and $d \sim r^\ell$ for some k, $\ell \in \mathbb{N}_0$.

3.2. (Integer-valued) polynomials

We shortly summarize definitions, notation and facts surrounding (integer-valued) polynomials over a discrete valuation domain (R, pR) which we need throughout this paper. For a deeper study of the theory of integer-valued polynomials, we refer to the textbook of Cahen and Chabert [8] and their recent survey [9].

Definition 3.4. Let $f \in R[x]$ be a polynomial.

(i) We call f *primitive* if the coefficients of f generate R as ideal.
(ii) We call a representative set $\mathcal{P}$ of the associate classes of the irreducible divisors of f an *irreducible divisor set of* f.

Definition 3.5. Let K be the quotient field of R. The *ring of integer-valued polynomials* on R is

$$\mathrm{Int}(R) = \{F \in K[x] \mid F(R) \subseteq R\}\,.$$

For $F \in \mathrm{Int}(R)$, the *fixed divisor* of F is defined as

$$\mathrm{d}(F) = \gcd(F(a) \mid a \in R)\,.$$

Remark 3.6. Every polynomial $F \in \mathrm{Int}(R)$ is of the form $F = \frac{f}{p^n}$ for some $f \in R[x]$ and $n \in \mathbb{N}$.

(i) $F \in \mathrm{Int}(R)$ if and only if $p^n \mid \mathrm{d}(f)$.
(ii) If $F \in \mathrm{Int}(R)$ is irreducible in $\mathrm{Int}(R)$, then $\mathrm{d}(f) = p^n$.

Convention 3.7. Throughout this paper, unless explicitly stated otherwise, let (R, pR) be a discrete valuation domain with valuation v and let $q = |R/pR|$ be the cardinality of the finite residue field of R.

Further, let $f \in R[x]$ be a non-constant, primitive polynomial with $\mathrm{d}(f) = p^n$ and irreducible divisor set $\mathcal{P}$ and let $F = \frac{f}{p^n}$.

As we encounter products of a set of irreducible elements quite frequently, we adopt a new abbreviated notation to emphasize the focus on the exponents (inspired by the standard notation $X^{\boldsymbol{a}}$ in multivariate polynomial rings).

Notation 3.8. Let $\mathcal{P} \subseteq R[x]$ be a non-empty, finite set of polynomials. For any $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}_0^{\mathcal{P}}$, we write

$$\mathcal{P}^{\boldsymbol{m}} = \prod_{g\in\mathcal{P}} g^{m_g}.$$

Remark 3.9. Using the notation of Convention 3.7, let $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ be the vector of the multiplicities with which $g \in \mathcal{P}$ occur as factors of f.

Then, considering the fact that the units of $\mathrm{Int}(R)$ are exactly the units of R,

$$F = \frac{f}{p^n} \sim \frac{\mathcal{P}^{\boldsymbol{m}}}{p^n} = \frac{\prod_{g\in\mathcal{P}} g^{m_g}}{p^n}$$

and the (essentially different) factorizations of F correspond to the (essentially different) factorizations of $\frac{\prod_{g\in\mathcal{P}} g^{m_g}}{p^n}$. Having this in mind, we restrict our investigation to polynomials of the latter form for simplicity.

The following well-known fact deals with the factorizations at issue. It follows from the proof [12, Theorem 2.8], which takes advantage of the fact that $\mathrm{Int}(R)$ is a subring of the polynomial ring over the quotient field of R, where we encounter unique factorization.

Fact 3.10 *([12, Theorem 2.8]).* Let (R, pR) be a discrete valuation domain with finite residue field and $F \in \mathrm{Int}(R)$ of the form

$$F \sim \frac{\mathcal{P}^{\boldsymbol{m}}}{p^n} = \frac{\prod_{g\in\mathcal{P}} g^{m_g}}{p^n} \quad \text{with} \quad \mathrm{d}(\mathcal{P}^{\boldsymbol{m}}) = p^n$$

where $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ for $g \in \mathcal{P}$, $n \in \mathbb{N}_0$, and $\mathcal{P} \subseteq R[x]$ is a non-empty, finite set of irreducible, non-constant polynomials which are pairwise non-associated.

If $F = F_1 \cdots F_r$ is a factorization of F into (not necessarily irreducible) non-units in $\mathrm{Int}(R)$, then, for each $1 \le j \le r$,

$$F_j \sim \frac{\mathcal{P}^{\boldsymbol{m_j}}}{p^{k_j}} = \frac{\prod_{g\in\mathcal{P}_j} g^{m_{j,g}}}{p^{k_j}}$$

where $\emptyset \ne \mathcal{P}_j \subseteq \mathcal{P}$, $\boldsymbol{m_j} = (m_{j,g})_{g\in\mathcal{P}} \in \mathbb{N}_0^{\mathcal{P}}$, and $k_j \in \mathbb{N}_0$ such that $\sum_{j=1}^{r} k_j = k$ and $\sum_{j=1}^{r} m_{j,g} = m_g$ for all $g \in \mathcal{P}$.

We conclude this section with a straight-forward observation on the properties of Notation 3.8.

Remark 3.11. Let $\boldsymbol{\ell} = (\ell_g)_{g\in\mathcal{P}}$, $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}_0^{\mathcal{P}}$. Using the notation of Convention 3.7, we infer

$$\mathcal{P}^{\boldsymbol{\ell}} = \mathcal{P}^{\boldsymbol{m}} \iff \boldsymbol{\ell} = \boldsymbol{m}$$

as well as

$$\mathcal{P}^{\boldsymbol{\ell}} \cdot \mathcal{P}^{\boldsymbol{m}} = \mathcal{P}^{\boldsymbol{\ell}+\boldsymbol{m}} \quad \text{and} \quad (\mathcal{P}^{\boldsymbol{m}})^j = \mathcal{P}^{j\boldsymbol{m}} \quad \text{for } j \in \mathbb{N}_0$$

from the definition and the fact that $R[x]$ is factorial.

Note also that all divisors of $\mathcal{P}^{\boldsymbol{m}}$ in $R[x]$ are given by the elements of $R[x]$ which are associated to $\mathcal{P}^{\boldsymbol{k}}$ for some $\boldsymbol{k} \in \mathbb{N}_0^{\mathcal{P}}$ with $\boldsymbol{k} \leq \boldsymbol{m}$ componentwise.

4. The fixed divisor kernel of a polynomial

Definition 4.1. Using the notation of Convention 3.7, we define the *set of fixed divisor witnesses of* f as

$$\mathcal{W}(f) = \{a \in R \mid \mathsf{v}(f(a)) = n\},$$

where we recall that $n = \mathsf{v}(\mathrm{d}(f))$. Further, we define the *fixed divisor kernel of* f to be

$$\text{fd-ker}(f) = \bigcap_{a\in\mathcal{W}(f)} \ker\big(\boldsymbol{m} \in \mathbb{Q}^{\mathcal{P}} \mapsto \langle \boldsymbol{m}, \mathsf{v}_{\mathcal{P}}(a)\rangle\big)$$

where $\langle\cdot,\cdot\rangle$ is the standard inner product and $\mathsf{v}_{\mathcal{P}}(a) = (\mathsf{v}(g(a)))_{g\in\mathcal{P}}$ for $a \in R$. (Note that the choice of $\mathcal{P}$ only affects the indexing, but not the values of valuations.)

Remark 4.2. Unraveling the definition yields $\langle \boldsymbol{m}, \mathsf{v}_{\mathcal{P}}(a)\rangle = \sum_{g\in\mathcal{P}} m_g \mathsf{v}(g(a))$ as well as

$$\text{fd-ker}(f) = \Big\{\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{Q}^{\mathcal{P}} \;\Big|\; \forall a \in \mathcal{W}(f)\colon \sum_{g\in\mathcal{P}} m_g \mathsf{v}(g(a)) = 0\Big\}.$$

Remark 4.3. The following observations are easily verified:

(i) Whenever r, $s \in R$ with $\mathsf{v}(r-s) \geq \mathsf{v}(r)+1$, then $\mathsf{v}(s) = \mathsf{v}(r)$.
(ii) Let $g \in R[x]$, a, $w \in R$, and $n \in \mathbb{N}$. If $\mathsf{v}(a-w) \geq n$, then $\mathsf{v}(g(a)-g(w)) \geq n$.
(iii) The combination of the items above implies that whenever $\mathsf{v}(a-w) \geq \mathsf{v}(g(a))+1$, then $\mathsf{v}(g(a)) = \mathsf{v}(g(w))$.

By Remark 4.3(iii), the set $\mathcal{W}(f)$ of witnesses is always infinite, since $\mathcal{W}(f) \neq \emptyset$ and with every $w \in \mathcal{W}(f)$ the (infinite) residue class $w + p^{\mathsf{v}(\mathrm{d}(f))+1}R$ is a subset of $\mathcal{W}(f)$.

However, as a subspace of $\mathbb{Q}^{\mathcal{P}}$, fd-ker(f) has finite dimension and hence fd-ker(f) is the kernel of a linear map $\mathbb{Q}^{\mathcal{P}} \to \mathbb{Q}^{W}$ for a finite set $W \subseteq \mathcal{W}(f)$, or equivalently, it can be represented as the kernel of a matrix.

Definition 4.4. Let W be a finite set. With the notation of Convention 3.7, we say that a matrix $A \in \mathbb{Q}^{W\times\mathcal{P}}$ is an *fdp matrix* (short for *fixed divisor partition matrix*) of f if $\ker(A) = \text{fd-ker}(f)$ (where we consider the kernel of A to be the kernel of the vector space homomorphism $\mathbb{Q}^{\mathcal{P}} \to \mathbb{Q}^{W}$ associated to A).

Next, we specify how an fdp matrix of f can be determined.

Lemma 4.5. *With the notation of Convention 3.7, let W be a set of representatives of the witness set $\mathcal{W}(f)$ modulo $p^{\lceil \frac{n}{2} \rceil}R$.*

Then, for each $a \in \mathcal{W}(f)$, there exists $w \in W$ such that $\mathsf{v}_{\mathcal{P}}(a) = \mathsf{v}_{\mathcal{P}}(w)$.

In particular, the matrix $(\mathsf{v}_{\mathcal{P}}(w))_{w\in W} \in \mathbb{Q}^{W\times\mathcal{P}}$ is an fdp matrix of f.

Proof. Let $w \in W$ be the representative of a modulo $p^{\lceil \frac{n}{2} \rceil}R$. We demonstrate that $\mathsf{v}_{\mathcal{P}}(a) = \mathsf{v}_{\mathcal{P}}(w)$ holds. Remark 4.3(iii) implies that $\mathsf{v}(g(a)) = \mathsf{v}(g(w))$ provided that $\mathsf{v}(g(a)) < \lceil \frac{n}{2} \rceil$.

It remains to consider the elements of

$$J = \left\{ g \in \mathcal{P} \;\middle|\; \mathsf{v}(g(a)) \geq \left\lceil \frac{n}{2} \right\rceil \right\}.$$

Let $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ be the vector of the multiplicities with which the polynomials $g \in \mathcal{P}$ occur as divisors of f so that $f = \mathcal{P}^{\boldsymbol{m}}$ (see Notation 3.8). Then

$$n = \mathsf{v}(f(a)) = \sum_{g\in\mathcal{P}} m_g \mathsf{v}(g(a)) \tag{4.1}$$

holds, which implies that the set J contains at most two elements since $m_g \in \mathbb{N}$. We split the remainder of the proof into two cases, $|J| = 1$ and $|J| = 2$.

If $J = \{h\}$, then

$$m_h \mathsf{v}(h(a)) = n - \sum_{g\in\mathcal{P}\setminus J} m_g \mathsf{v}(g(a)) = n - \sum_{g\in\mathcal{P}\setminus J} m_g \mathsf{v}(g(w)) = m_h \mathsf{v}(h(w))$$

and hence $\mathsf{v}(h(a)) = \mathsf{v}(h(w))$.

Finally, we assume that $J = \{h_1, h_2\}$ with $h_1 \neq h_2$. Due to Equation (4.1), this is only possible if n is even and $\mathsf{v}(h_1(a)) = \mathsf{v}(h_2(a)) = \frac{n}{2}$. Moreover, by Remark 4.3, $\mathsf{v}(h_1(w))$, $\mathsf{v}(h_2(w))$ are both at least $\frac{n}{2}$. As w is a fixed divisor witness, it follows that

$$n = \mathsf{v}(f(w)) = \sum_{g\in\mathcal{P}} m_g \mathsf{v}(g(w)) \geq m_{h_1} \mathsf{v}(h_1(w)) + m_{h_2} \mathsf{v}(h_2(w)) \geq n$$

holds. We conclude that $\mathsf{v}(h_1(w)) = \mathsf{v}(h_2(w)) = \frac{n}{2}$, which proves the claim. $\square$

Example 4.6. Let $f = (x^2+9)(x-5)^3(x-1)(x-7) \in \mathbb{Z}_{(3)}[x]$ where $\mathbb{Z}_{(3)}$ is the localization of $\mathbb{Z}$ at 3. A straight-forward verification shows that the fixed divisor of f is 9. In order to find an fdp matrix, it suffices to find a set of representatives modulo 3 of all the fixed divisor witnesses of f. By evaluating f at 0 and 4, we can verify that both are in $\mathcal{W}(f)$. Also, the factor $(x-5)^3$ of f guarantees that no fixed divisor witness is congruent to 2 modulo 3. We set $W = \{0, 4\}$ and apply Lemma 4.5 to conclude that

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \in \mathbb{Q}^{W \times \mathcal{P}}$$

is a fixed divisor partition matrix of f where $\mathcal{P} = \{x^2+9, x-5, x-1, x-7\}$ (and for the purpose of writing down the matrix, we impose the order on W and $\mathcal{P}$ with which their elements are given here).

In the following, we discuss the connection between fd-ker(f) and the question whether $F = \frac{f}{p^n}$ is absolutely irreducible (where $\mathsf{v}(\mathrm{d}(f)) = n$). We start with the connection to integer-valued divisors of powers of F.

Lemma 4.7. *Using the notation of Convention 3.7, let $f = \prod_{g \in \mathcal{P}} g^{m_g} \in R[x]$ where $\boldsymbol{m} = (m_g)_{g \in \mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ is the vector of the corresponding multiplicities.*

If $\mathbf{0} \neq \boldsymbol{k} = (k_g)_{g \in \mathcal{P}} \in \mathbb{N}_0^{\mathcal{P}}$ and $\ell \in \mathbb{N}_0$ such that $\frac{\prod_{g \in \mathcal{P}} g^{k_g}}{p^\ell}$ divides F^j in $\mathrm{Int}(R)$ for some $j \in \mathbb{N}$, then

$$\boldsymbol{k} \in \frac{\ell}{n}\boldsymbol{m} + \text{fd-ker}(f).$$

Proof. Using the abbreviated notation for products of polynomials, cf. Notation 3.8, we write $f = \mathcal{P}^{\boldsymbol{m}}$ and set $f_1 = \mathcal{P}^{\boldsymbol{k}}$ and $f_2 = \mathcal{P}^{j\boldsymbol{m}-\boldsymbol{k}}$. Then $\frac{f_2}{p^{jn-\ell}}$ is the cofactor to $\frac{f_1}{p^\ell}$ of F^j in $\mathrm{Int}(R)$ and $\mathsf{v}(f_1(a)) \geq \ell$ and $\mathsf{v}(f_2(a)) \geq jn - \ell$ hold for all $a \in R$.

If $w \in \mathcal{W}(f)$ is a fixed divisor witness of f, Remark 4.2 yields

$$\begin{aligned} jn = j\mathsf{v}(f(w)) = j\langle \boldsymbol{m}, \mathsf{v}_{\mathcal{P}}(w)\rangle &= \langle \boldsymbol{k}, \mathsf{v}_{\mathcal{P}}(w)\rangle + \langle j\boldsymbol{m} - \boldsymbol{k}, \mathsf{v}_{\mathcal{P}}(w)\rangle \\ &= \mathsf{v}(f_1(w)) + \mathsf{v}(f_2(w)) \geq \ell + (jn - \ell) = jn, \end{aligned}$$

implying equality throughout, in particular $\ell = \mathsf{v}(f_1(w)) = \langle \boldsymbol{k}, \mathsf{v}_{\mathcal{P}}(w)\rangle$. Then $\boldsymbol{k}$ is a solution to the linear equation $\langle \boldsymbol{x}, \mathsf{v}_{\mathcal{P}}(w)\rangle = \ell$. Since $\frac{\ell}{n}\boldsymbol{m}$ is another solution to it (cf. Remark 4.2), it follows that

$$\boldsymbol{k} - \frac{\ell}{n}\boldsymbol{m} \in \ker\big(\boldsymbol{x} \in \mathbb{Q}^{\mathcal{P}} \mapsto \langle \boldsymbol{x}, \mathsf{v}_{\mathcal{P}}(w)\rangle\big)$$

for all $w \in \mathcal{W}(f)$ and thus $\boldsymbol{k} - \frac{\ell}{n}\boldsymbol{m} \in \text{fd-ker}(f)$. $\square$

Next, we show how we can use non-zero elements in fd-ker(f) to construct specific polynomials in $\mathrm{Int}(R)$, which will turn out to be non-trivial divisors of $\frac{f}{p^n}$.

Definition 4.8. Let $\boldsymbol{u}$, $\boldsymbol{v} \in \mathbb{Q}^{\mathcal{P}}$. The positive and negative part of $\boldsymbol{u}$ are defined by

$$\boldsymbol{u}^+ = \max(\boldsymbol{u}, \boldsymbol{0}) \quad \text{and} \quad \boldsymbol{u}^- = -\min(\boldsymbol{u}, \boldsymbol{0}),$$

respectively, where max and min are to be understood componentwise and $\boldsymbol{0} = (0)_{g\in\mathcal{P}}$ denotes the zero vector. We further write $\|\boldsymbol{u}\|_\infty = \max_{g\in\mathcal{P}}|u_g|$ for the usual infinity norm of $\boldsymbol{u} = (u_g)_{g\in\mathcal{P}}$ and

$$\|\lceil \boldsymbol{u} \rceil\|_\infty = \lceil \|\boldsymbol{u}\|_\infty \rceil.$$

Finally, for $\boldsymbol{u} = (u_g)_{g\in\mathcal{P}}$ and $\boldsymbol{v} = (v_g)_{g\in\mathcal{P}}$ in $\mathbb{Q}^{\mathcal{P}}$, we define

$$\boldsymbol{u} \cdot \boldsymbol{v} = (u_g \cdot v_g)_{g\in\mathcal{P}} \qquad \text{and} \qquad \frac{\boldsymbol{u}}{\boldsymbol{v}} = \left(\frac{u_g}{v_g}\right)_{g\in\mathcal{P}},$$

where the latter is only defined whenever all v_g are non-zero. The unit element with respect to this multiplication is $\boldsymbol{1} = (1)_{g\in\mathcal{P}}$.

Proposition 4.9. *Using the notation of Convention 3.7, let $f = \prod_{g\in\mathcal{P}} g^{m_g} \in R[x]$ where $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ is the vector of the corresponding multiplicities.*

If $\boldsymbol{0} \neq \boldsymbol{v} = (v_g)_{g\in\mathcal{P}} \in$ fd-ker$(f) \cap \mathbb{Z}^{\mathcal{P}}$ and $k \in \mathbb{N}$ with $k \geq (n+1)\|\lceil \frac{\boldsymbol{v}^+}{\boldsymbol{m}} \rceil\|_\infty$, then

$$H = \frac{\prod_{g\in\mathcal{P}} g^{km_g - v_g}}{p^{kn}} \in \mathrm{Int}(R).$$

Moreover, H is not a power of $\frac{f}{p^n}$.

Remark 4.10. Set $s^+ = \|\lceil \frac{\boldsymbol{v}^+}{\boldsymbol{m}} \rceil\|_\infty$ and note that all components of $\boldsymbol{m}$ are positive. By definition of $\boldsymbol{v}^+$, the identity

$$s^+ = \max\left\{ \left\lceil \frac{v_g}{m_g} \right\rceil \;\middle|\; g \in \mathcal{P} \text{ with } v_g \geq 0 \right\}$$

holds and we have $s^+ > 0$ since $\boldsymbol{0} \neq \mathsf{v}_{\mathcal{P}}(w) \in \mathbb{N}_0^{\mathcal{P}}$ for all fixed divisor witnesses w of f.

The definition also immediately implies $s^+\boldsymbol{m} \geq \boldsymbol{v}^+$.

Observe further that $k\boldsymbol{m} - \boldsymbol{v}$ only consists of positive integers because the positivity of k entails either $k > 0 \geq \frac{v_g}{m_g}$, if $v_g \leq 0$, or $k \geq (n+1)s^+ \geq (n+1)\frac{v_g}{m_g} > \frac{v_g}{m_g}$, if $v_g > 0$.

Proof. Again, we switch to the abbreviation for writing polynomial products (Notation 3.8) and set $\tilde{f} = \mathcal{P}^{k\boldsymbol{m}-\boldsymbol{v}}$ to be the numerator of H.

We need to show

$$\mathsf{v}(\tilde{f}(a)) \geq kn \qquad \text{for all } a \in R. \tag{4.2}$$

Assume first that $\mathsf{v}(h(a)) = \infty$ for some $h \in \mathcal{P}$, that is, at least one entry of $\mathsf{v}_{\mathcal{P}}(a)$ is equal to ∞. Then the strict positivity of $k\boldsymbol{m} - \boldsymbol{v}$, as observed in Remark 4.10, assures that the component of $k\boldsymbol{m} - \boldsymbol{v}$ corresponding to h is positive and hence

$$\mathsf{v}(\tilde{f}(a)) = \langle k\boldsymbol{m} - \boldsymbol{v}, \mathsf{v}_{\mathcal{P}}(a)\rangle = \infty \geq kn.$$

For the remainder of the proof we may thus assume that $\mathsf{v}(g(a)) < \infty$ for all $g \in \mathcal{P}$. Then we obtain

$$\begin{aligned}\mathsf{v}(\tilde{f}(a)) = \langle k\boldsymbol{m} - \boldsymbol{v}, \mathsf{v}_{\mathcal{P}}(a)\rangle &= k\langle \boldsymbol{m}, \mathsf{v}_{\mathcal{P}}(a)\rangle - \langle \boldsymbol{v}, \mathsf{v}_{\mathcal{P}}(a)\rangle \\ &= k \cdot \mathsf{v}(f(a)) - \langle \boldsymbol{v}, \mathsf{v}_{\mathcal{P}}(a)\rangle\end{aligned} \tag{4.3}$$

from Remark 4.2, as the difference is now well-defined.

If a is a fixed divisor witness, then $\langle \boldsymbol{v}, \mathsf{v}_{\mathcal{P}}(a)\rangle = 0$, so $\mathsf{v}(\tilde{f}(a)) = k\mathsf{v}(f(a)) = kn$ by (4.3).

It remains to show (4.2) for all $a \in R$ with $\mathsf{v}(f(a)) \geq n + 1$. We claim that

$$k\mathsf{v}(f(a)) \geq kn + \langle \boldsymbol{v}^+, \mathsf{v}_{\mathcal{P}}(a)\rangle \tag{4.4}$$

holds in that case.

Assume the validity of (4.4) for the moment. Then we obtain

$$\mathsf{v}(\tilde{f}(a)) = k\mathsf{v}(f(a)) - \langle \boldsymbol{v}, \mathsf{v}_{\mathcal{P}}(a)\rangle \geq kn + \langle \boldsymbol{v}^+, \mathsf{v}_{\mathcal{P}}(a)\rangle - \langle \boldsymbol{v}, \mathsf{v}_{\mathcal{P}}(a)\rangle \geq kn$$

from Equation (4.3) and $\boldsymbol{v}^+ \geq \boldsymbol{v}$, which finishes the proof of (4.2).

We only need to prove Inequality (4.4). Set $s^+ = \left\| \left\lceil \frac{\boldsymbol{v}^+}{\boldsymbol{m}} \right\rceil \right\|_\infty$, as in Remark 4.10, and $\mathsf{v}(f(a)) = n + j$ for some $j \in \mathbb{N}$. Since $k \geq (n+1)s^+$ and $s^+\boldsymbol{m} \geq \boldsymbol{v}^+$, we conclude that

$$\begin{aligned}k\big(\mathsf{v}(f(a)) - n\big) = kj \geq (n+1)s^+j &= ns^+j + s^+j \\ &\geq ns^+ + s^+j = s^+(n+j) = s^+\mathsf{v}(f(a)) \\ &= s^+\langle \boldsymbol{m}, \mathsf{v}_{\mathcal{P}}(a)\rangle = \langle s^+\boldsymbol{m}, \mathsf{v}_{\mathcal{P}}(a)\rangle \geq \langle \boldsymbol{v}^+, \mathsf{v}_{\mathcal{P}}(a)\rangle,\end{aligned}$$

which is equivalent to (4.4).

Finally, we show that H is not a power of F. Suppose the contrary. Then

$$\frac{\mathcal{P}^{k\boldsymbol{m}-\boldsymbol{v}}}{p^{kn}} = \frac{\mathcal{P}^{t\boldsymbol{m}}}{p^{tn}} \iff p^{tn}\mathcal{P}^{k\boldsymbol{m}-\boldsymbol{v}} = p^{kn}\mathcal{P}^{t\boldsymbol{m}}$$

for some $t \in \mathbb{N}_0$, which entails $t = k$ and $\mathcal{P}^{k\boldsymbol{m}-\boldsymbol{v}} = \mathcal{P}^{t\boldsymbol{m}} = \mathcal{P}^{k\boldsymbol{m}}$ since p is also a prime element in $R[x]$. But then $\boldsymbol{v} = \boldsymbol{0}$ since $R[x]$ is factorial (cf. Remark 3.11), contradicting the assumption on $\boldsymbol{v}$. □

We are now ready to prove the main results of this section.

Theorem 1. *Let (R, pR) be a discrete valuation domain with valuation v and finite residue field. Further, let $f = \prod_{g\in\mathcal{P}} g^{m_g} \in R[x]$ be a primitive, non-constant polynomial with irreducible divisor set $\mathcal{P}$ and $\boldsymbol{m} = (m_g)_{g\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ the vector of the corresponding multiplicities and assume that $\mathsf{v}(\mathrm{d}(f)) = n \in \mathbb{N}$.*

If $\text{fd-ker}(f) \neq \boldsymbol{0}$, then $F = \frac{f}{p^n}$ is not absolutely irreducible. In fact, if F is irreducible and $\boldsymbol{0} \neq \boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}$, then F^j factors non-uniquely for all $j \in \mathbb{N}$ with $j \geq (n+1)\left(\left\|\left\lceil\frac{\boldsymbol{v}^+}{\boldsymbol{m}}\right\rceil\right\|_\infty + \left\|\left\lceil\frac{\boldsymbol{v}^-}{\boldsymbol{m}}\right\rceil\right\|_\infty\right)$.

Remark. Observe that $(-\boldsymbol{v})^+ = \boldsymbol{v}^-$, so that the second summand of the lower bound corresponds to the lower bound from Proposition 4.9 for $-\boldsymbol{v}$.

Proof. We can assume that F is irreducible since otherwise it is also not absolutely irreducible. Let $\boldsymbol{0} \neq \boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}$. It suffices to show that F^j with $j = (n+1)\left(\left\|\left\lceil\frac{\boldsymbol{v}^+}{\boldsymbol{m}}\right\rceil\right\|_\infty + \left\|\left\lceil\frac{\boldsymbol{v}^-}{\boldsymbol{m}}\right\rceil\right\|_\infty\right)$ factors non-uniquely. Let k, $\ell \in \mathbb{N}$ with

$$k \geq (n+1)\left\|\left\lceil\frac{\boldsymbol{v}^+}{\boldsymbol{m}}\right\rceil\right\|_\infty \quad \text{and} \quad \ell \geq (n+1)\left\|\left\lceil\frac{\boldsymbol{v}^-}{\boldsymbol{m}}\right\rceil\right\|_\infty.$$

Using the abbreviated notation for polynomial products (Notation 3.8), it follows from Proposition 4.9 that

$$\frac{\mathcal{P}^{k\boldsymbol{m}-\boldsymbol{v}}}{p^{kn}} \in \mathrm{Int}(R)$$

and that this polynomial is not a power of F.

Similarly, we can apply Proposition 4.9 with $-\boldsymbol{v}$ (which is also a non-zero element of $\text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}$) and conclude that

$$\frac{\mathcal{P}^{\ell\boldsymbol{m}-(-\boldsymbol{v})}}{p^{\ell n}} = \frac{\mathcal{P}^{\ell\boldsymbol{m}+\boldsymbol{v}}}{p^{\ell n}} \in \mathrm{Int}(R),$$

again not a power of F. Therefore,

$$F^{k+\ell} = \frac{\mathcal{P}^{(k+\ell)\boldsymbol{m}}}{p^{(k+\ell)n}} = \frac{\mathcal{P}^{k\boldsymbol{m}-\boldsymbol{v}}}{p^{kn}} \cdot \frac{\mathcal{P}^{\ell\boldsymbol{m}+\boldsymbol{v}}}{p^{\ell n}}$$

is a factorization of $F^{k+\ell}$ (not necessarily into irreducibles) which yields a factorization of $F^{k+\ell}$ into irreducibles different from the trivial one $F \cdot F \cdots F$ (see Remark 3.3). It follows that F^j factors non-uniquely for every exponent j with $j \geq (n+1)\left(\left\|\left\lceil\frac{\boldsymbol{v}^+}{\boldsymbol{m}}\right\rceil\right\|_\infty + \left\|\left\lceil\frac{\boldsymbol{v}^-}{\boldsymbol{m}}\right\rceil\right\|_\infty\right)$. $\square$

Theorem 2. *Let (R, pR) be a discrete valuation domain with valuation v and finite residue field. Further, let $f \in R[x]$ be a primitive, non-constant polynomial with $\mathsf{v}(\mathrm{d}(f)) = n \in \mathbb{N}$ and assume that f is not a proper power of another polynomial in $R[x]$.*

Then $\frac{f}{p^n}$ is absolutely irreducible if and only if $\text{fd-ker}(f) = \mathbf{0}$.

Proof. Assume first $\text{fd-ker}(f) = \mathbf{0}$, let $\mathcal{P}$ be an irreducible divisor set of f, write $f \sim \mathcal{P}^{\boldsymbol{m}}$ (cf. Remark 3.9), and set $F = \frac{f}{p^n}$. Let $\tilde{F}$ be a non-constant factor of F^j in $\mathrm{Int}(R)$ for some $j \in \mathbb{N}$. We show that $\tilde{F}$ is itself (associated to) a power of F. Note that for $j = 1$ this implies that F is irreducible.

It follows from Fact 3.10, with the abbreviated notation for polynomial products (Notation 3.8), that $\tilde{F} \sim \frac{\mathcal{P}^{\boldsymbol{k}}}{p^\ell}$ for some $\ell \in \mathbb{N}_0$ and $\mathbf{0} \neq \boldsymbol{k} \in \mathbb{N}_0^{\mathcal{P}}$.

We can apply Lemma 4.7 to infer

$$\boldsymbol{k} - \frac{\ell}{n}\boldsymbol{m} \in \text{fd-ker}(f) = \mathbf{0} \quad \Longrightarrow \quad \frac{\ell}{n}\boldsymbol{m} = \boldsymbol{k} \in \mathbb{N}_0^{\mathcal{P}}.$$

Since f is assumed not a proper power of another polynomial in $R[x]$, we must have[3] $\gcd(\boldsymbol{m}) = 1$ and hence $\ell = tn$ for some $t \in \mathbb{N}_0$ and $\boldsymbol{k} = t\boldsymbol{m}$. It follows that $\tilde{F} \sim \left(\frac{\mathcal{P}^{\boldsymbol{m}}}{p^n}\right)^t \sim F^t$, which was to be shown.

Conversely, if $\text{fd-ker}(f) \neq \mathbf{0}$, then $\frac{f}{p^n}$ is not absolutely irreducible according to Theorem 1. □

Remark 4.11. Let D be a Dedekind domain, P a maximal ideal of D with finite index, and $F = \frac{f}{c} \in \mathrm{Int}(D)$ with $f \in D[x]$ primitive, non-constant, not a proper power of another polynomial and $0 \neq c \in D$. Since $\mathrm{Int}(D) \subseteq \mathrm{Int}(D_P)$ (see [8, Theorem I.2.3]), we can regard F as integer-valued polynomial over the discrete valuation domain D_P. If $\text{fd-ker}(f) = \mathbf{0}$, then F is absolutely irreducible in $\mathrm{Int}(D_P)$ and a straight-forward argument (see, for example, [18, Corollary 6.11]) shows that F is absolutely irreducible in $\mathrm{Int}(D)$,

Remark 4.12. We point out that there is a loose relation between the fdp matrices introduced here and the partition matrices defined in the paper of Frisch, Nakato and Rissner [18, Definition 5.5] on absolute irreducibility of completely split polynomials in $\mathrm{Int}(R)$. Partition matrices, however, have trivial kernel ([18, Proposition 6.5]). If the split integer-valued polynomial to which a partition matrix A is associated is absolutely irreducible, A is indeed an fdp matrix upon suitable interpretation of row and column sets. This is not the case for split polynomials which are not absolutely irreducible.

[3] To be understood as the gcd of all components of $\boldsymbol{m}$.

5. Bounds for the minimal power of a non-absolutely irreducible polynomial to factor non-uniquely

As pointed out in the introduction, for $F \in \mathrm{Int}(R)$ of the form $\frac{f}{p}$ it suffices to check whether F^2 factors uniquely to verify absolute irreducibility. This motivates the question whether an analogous statement holds if the denominator of F is not square-free: Is it possible to conclude that F is absolutely irreducible whenever F^k factors uniquely for $1 \leq k \leq S$ for some S which is yet to be determined?

Theorem 1 provides an upper bound for such S for an integer-valued polynomial F depending on the (absolute) values of coordinates of integer elements in the fixed divisor kernel of the numerator polynomial f of F.

In the following, we will provide, among others, a bound S which only depends on the valuation of the denominator of F and the size of the finite residue field of the underlying discrete valuation domain R. To do so, we look for an upper bound for

$$\min\left\{\|\boldsymbol{v}\|_\infty \;\middle|\; \mathbf{0} \neq \boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}\right\},$$

which motivates the following definition.

Definition 5.1. Let f be as in notation of Convention 3.7. We call an fdp matrix of f *reduced* if its rows are $\mathbb{Q}$-linearly independent.

We hence look for an upper bound for

$$\min\left\{\|\boldsymbol{v}\|_\infty \;\middle|\; \mathbf{0} \neq \boldsymbol{v} \in \ker(A) \cap \mathbb{Z}^{\mathcal{P}}\right\}$$

where A is a reduced fdp matrix of f. To this end, we use a Siegel-type lemma which we tailored to the type of matrices which occur as (reduced) fdp matrices. The proof below is essentially the same as the one in Baker's textbook [5, Lemma 1, Chapter 3], the modifications merely take the additional assumptions on the system matrix into account.

Lemma 5.2 *(Adapted version of Siegel's lemma). Let $r \in \mathbb{N}_0$, $s \in \mathbb{N}$, and I, J be sets with $|I| = r$, $|J| = r + s$. Let $n \in \mathbb{N}$ and $A = (a_{i,j})_{(i,j)\in I\times J} \in \mathbb{N}_0^{I\times J}$ be such that $\sum_{j\in J} a_{i,j} \leq n$ for all $i \in I$. Assume further that A contains u rows with exactly one non-zero entry.*

Then

$$\min\left\{\|\boldsymbol{v}\|_\infty \;\middle|\; \mathbf{0} \neq \boldsymbol{v} \in \ker(A) \cap \mathbb{Z}^{J}\right\} \leq \left\lfloor n^{\frac{r-u}{s}} \right\rfloor.$$

Proof. Assume first $u = 0$, set $b = \lfloor n^{\frac{r}{s}} \rfloor$ and $X = \left\{\boldsymbol{x} \in \mathbb{N}_0^J \;\middle|\; \|\boldsymbol{x}\|_\infty \leq b\right\}$. Then $\boldsymbol{x} \in X$ implies

$$0 \leq (A\boldsymbol{x})_i = \sum_{j\in J} a_{i,j}x_j \leq nb \tag{5.1}$$

for all $i \in I$. Hence, the set $\{A\boldsymbol{x} \mid \boldsymbol{x} \in X\}$ contains at most $(nb+1)^r$ elements, whereas the cardinality of X is equal to $(b+1)^{r+s}$.

Since

$$(b+1)^{r+s} = (b+1)^s(b+1)^r > n^r(b+1)^r \geq (nb+1)^r \tag{5.2}$$

holds, it follows from the pigeonhole principle that there exist $\boldsymbol{x}, \boldsymbol{y} \in X$ with $\boldsymbol{x} \neq \boldsymbol{y}$ such that $A\boldsymbol{x} = A\boldsymbol{y}$. Hence $\boldsymbol{v} = \boldsymbol{x} - \boldsymbol{y} \neq \mathbf{0}$ is an element in $\ker(A)$ whose every coordinate has absolute value at most b.

Now turn to the general case $u \geq 0$. Let E be the set of row indices for which the corresponding rows contain exactly one non-zero entry and set $C = \{j \in J \mid \exists e \in E\colon a_{e,j} \neq 0\}$. The definition of E implies $|C| \leq |E| \leq u$. Consider now the matrix B which is obtained from A by deleting the u rows corresponding to E as well as the columns corresponding to C. Then B has $r-u$ rows and $r+s-|C|$ columns. Note that if $\boldsymbol{v} \in \ker(A)$ and $k \in C$, then $v_k = 0$. Hence

$$\begin{aligned}\min\Big\{\|\boldsymbol{v}\|_\infty \;\Big|\; \mathbf{0} \neq \boldsymbol{v} \in \ker(A) \cap \mathbb{Z}^J\Big\} &= \min\Big\{\|\boldsymbol{v}\|_\infty \;\Big|\; \mathbf{0} \neq \boldsymbol{v} \in \ker(B) \cap \mathbb{Z}^{J\setminus C}\Big\} \\ &\leq \Big\lfloor n^{\frac{r-u}{s+u-|C|}} \Big\rfloor \leq \Big\lfloor n^{\frac{r-u}{s}} \Big\rfloor\end{aligned}$$

by applying the result of the first part to B. $\square$

Theorem 3. *Let (R, pR) be a discrete valuation domain with valuation v and let $q = |R/pR|$ be the cardinality of the finite residue field of R. Further, let $f \in R[x]$ be a non-constant, primitive polynomial with irreducible divisor set $\mathcal{P}$ and $(m_g)_{g\in\mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$ the vector of the corresponding multiplicities, that is, $f = \prod_{g\in\mathcal{P}} g^{m_g}$. Let $\mathsf{v}(\mathrm{d}(f)) = n \in \mathbb{N}$ and $A \in \mathbb{Q}^{W\times\mathcal{P}}$ (with $W \subseteq \mathcal{W}(f)$) be a reduced fdp matrix of f containing u rows with only one non-zero entry.*

Assume that F is irreducible. Then the following assertions are equivalent:

(i) *F^j factors uniquely for all $j \in \mathbb{N}$, that is, F is absolutely irreducible.*
(ii) *F^S factors uniquely for $S = 2(n+1)n^{q^{\lceil \frac{n}{2} \rceil}}$.*
(iii) *F^S factors uniquely for $S = 2(n+1)n^{\mathrm{rank}(A)-u}$.*

Remark 5.3. It follows from Theorem 3 that F is **not** absolutely irreducible if and only if F^j factors non-uniquely for some $1 \leq j \leq 2(n+1)n^{q^{\lceil \frac{n}{2} \rceil}}$. Note that this upper bound only depends on the fixed divisor of f and the size of the residue class field, but not the reduced fdp matrix A.

Proof. Let $r = \mathrm{rank}(A) = |W|$. By definition, (i) implies (ii) and (iii). Moreover, by Lemma 4.5, A has at most $q^{\lceil \frac{n}{2} \rceil}$ rows and hence $r - u \leq r \leq q^{\lceil \frac{n}{2} \rceil}$, so that (ii) implies (iii).

We prove by contraposition that (i) follows from (iii). Assume that F is irreducible, but not absolutely irreducible. Then $\text{fd-ker}(f) = \ker(A) \neq \mathbf{0}$ by Theorem 2 or, equivalently, $r < |\mathcal{P}|$. We apply Lemma 5.2 to A: There exists $\mathbf{0} \neq \boldsymbol{v} \in \ker(A) \cap \mathbb{Z}^{\mathcal{P}}$ with $\|\boldsymbol{v}\|_\infty \leq \left\lfloor n^{\frac{r-u}{|\mathcal{P}|-r}} \right\rfloor \leq n^{r-u}$. Since $\boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}$ and F is assumed to be irreducible, it follows from Theorem 1 that F^j factors non-uniquely for all $j \geq (n+1)\left(\left\|\left\lceil \frac{\boldsymbol{v}^+}{\boldsymbol{m}} \right\rceil\right\|_\infty + \left\|\left\lceil \frac{\boldsymbol{v}^-}{\boldsymbol{m}} \right\rceil\right\|_\infty\right)$. Because of

$$S = 2(n+1)n^{r-u} \geq 2(n+1)\|\boldsymbol{v}\|_\infty \geq (n+1)\left(\left\|\left\lceil \frac{\boldsymbol{v}^+}{\boldsymbol{m}} \right\rceil\right\|_\infty + \left\|\left\lceil \frac{\boldsymbol{v}^-}{\boldsymbol{m}} \right\rceil\right\|_\infty\right),$$

it follows that F^S factors non-uniquely so that (iii) does not hold. $\square$

6. Tightness of the bounds

By Theorem 1, we know that $F = \frac{f}{p^n}$ is not absolutely irreducible and, more accurately, that F^j factors non-uniquely whenever $\mathbf{0} \neq \boldsymbol{v} \in \text{fd-ker}(f)$ and $j \in \mathbb{N}$ with $j \geq (n+1)\left(\left\|\left\lceil \frac{\boldsymbol{v}^+}{\boldsymbol{m}} \right\rceil\right\|_\infty + \left\|\left\lceil \frac{\boldsymbol{v}^-}{\boldsymbol{m}} \right\rceil\right\|_\infty\right)$.

We show below, in Theorem 4, that this bound cannot be improved in general. Indeed, we show that for all integers $n \geq 2$ there exists a polynomial $f \in R[x]$ with $\mathsf{v}(\mathrm{d}(f)) = n$ such that $\boldsymbol{m} = \mathbf{1} = (1)_{g \in \mathcal{P}}$, $F = \frac{f}{p^n}$ is irreducible and factors uniquely up to the bound $(n+1)K$ with

$$K = \min\left\{ \|\boldsymbol{v}^+\|_\infty + \|\boldsymbol{v}^-\|_\infty \;\middle|\; \mathbf{0} \neq \boldsymbol{v} \in \ker(A) \cap \mathbb{Z}^{\mathcal{P}} \right\},$$

where A is a (reduced) fdp matrix of f. As already mentioned in the introduction, the case $n = 1$ has been covered where the bound is known to be 2.

By Lemma 5.2 (variation of Siegel's lemma) above, $K \leq 2n^{r-u}$ whenever A contains r rows, u of which contain exactly one non-zero entry. In Theorem 4, we furnish examples for every $r \geq 2$ such that

(i) $u = 1$ and
(ii) $K = (n-1)^{r-1} + (n-1)^{r-2}$.

It remains open whether this is actually optimal, in the sense that

$$(n-1)^{r-1} + (n-1)^{r-2} = \max_{A \in \mathcal{A}} \min\left\{ \|\boldsymbol{v}^+\|_\infty + \|\boldsymbol{v}^-\|_\infty \;\middle|\; \mathbf{0} \neq \boldsymbol{v} \in \ker(A) \cap \mathbb{Z}^{\mathcal{P}} \right\},$$

where $\mathcal{A}$ denotes the set of all reduced fdp matrices A of f with exactly one row with only one non-zero entry.

The next proposition establishes sufficient conditions on the polynomial f in order to achieve the asserted bound, whereas in Theorem 4 we show that such polynomials can always be realized.

Proposition 6.1. *Let r, $n \geq 2$ be integers. Using the notation of Convention 3.7, let $f = \prod_{g \in \mathcal{P}} g$ where $\mathcal{P} = \{g_1, \dots, g_{r+1}\}$ is an irreducible divisor set, $\mathsf{v}(\mathrm{d}(f)) = n$, and*

$$A = \begin{pmatrix} 1 & n-1 & & & & \\ & 1 & n-1 & & & \\ & & \ddots & \ddots & & \\ & & & 1 & n-1 & \\ & & & & & n \end{pmatrix} \in \mathbb{N}_0^{W \times \mathcal{P}}$$

is a reduced fdp matrix of f for some $W \subseteq \mathcal{W}(f)$ with $|W| = r$, where the i-th column corresponds to the polynomial g_i. In addition, we assume that there exist a_1, $a_2 \in R$ such that $\mathsf{v}(g_i(a_i)) = n+1$ and $\mathsf{v}(g_j(a_i)) = 0$ for all $i = 1, 2$ and $1 \leq j \leq r+1$ with $j \neq i$.

*Then F is irreducible, but **not** absolutely irreducible in $\mathrm{Int}(R)$. Indeed, the minimal exponent S such that F^S does not factor uniquely satisfies the two equations:*

(i) $S = (n+1)\left((n-1)^{r-1} + (n-1)^{r-2}\right)$ *with* $r = \mathrm{rank}(A)$ *and*
(ii) $S = (n+1)\min\left\{\|\boldsymbol{v}^+\|_\infty + \|\boldsymbol{v}^-\|_\infty \;\middle|\; \mathbf{0} \neq \boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}\right\}$ *(which is the minimal lower bound given in Theorem 1 applied to the current setting).*

Proof. For readability, we write $i \in [r+1]$ whenever we address $g_i \in \mathcal{P}$.

First, we determine $\ker(A)$. Let $\boldsymbol{u} = (u_i)_{i=1}^{r+1} \in \ker(A)$. It is immediately seen that $u_{r+1} = 0$. Moreover, a straight-forward computation yields that $u_i = -(n-1)u_{i+1}$ for all $1 \leq i \leq r-1$. Therefore, $u_i = (-1)^{r-i}(n-1)^{r-i}u_r$. Thus, $\ker(A) = \mathrm{span}_{\mathbb{Q}}(\boldsymbol{v})$ where $\boldsymbol{v} = (v_i)_{i=1}^{r+1}$ with

$$v_i = \begin{cases} (-1)^{r-i}(n-1)^{r-i}, & 1 \leq i \leq r, \\ 0, & i = r+1. \end{cases} \tag{6.1}$$

This implies $\dim(\ker(A)) = 1$ and hence $\mathrm{rank}(A) = r$, as claimed.

Next, we set

$$K = \min\left\{\|\boldsymbol{v}^+\|_\infty + \|\boldsymbol{v}^-\|_\infty \mid \mathbf{0} \neq \boldsymbol{v} \in \ker(A) \cap \mathbb{Z}^{\mathcal{P}}\right\}.$$

Note that Theorem 1 guarantees that $F^{(n+1)K}$ factors non-uniquely. In order to prove the whole assertion of the theorem, we need to show that

(a) $S = (n+1)K$ is the smallest power of F factoring non-uniquely,
(b) F is irreducible, and
(c) $K = (n-1)^{r-1} + (n-1)^{r-2}$.

We infer $\ker(A) \cap \mathbb{Z}^{r+1} = \mathbb{Z}\boldsymbol{v}$ by considering the r-th component of $\lambda\boldsymbol{v}$ for $\lambda \in \mathbb{Q}$. From Equation (6.1), we conclude that v_1 and v_2 have opposite signs and $|v_1| \geq |v_2| \geq |v_i|$ for $i > 2$. (Equality is only possible for $n = 2$.) Hence

$$\|\lambda \boldsymbol{v}^+\|_\infty + \|\lambda \boldsymbol{v}^-\|_\infty = |\lambda| \left(|v_1| + |v_2|\right) \geq (n-1)^{r-1} + (n-1)^{r-2}$$

for all $\lambda \in \mathbb{Z}$, $\lambda \neq 0$. Since $\mathbf{0} \neq \boldsymbol{v} \in \ker(A)$ satisfies this with equality, we have proven Item (c) from the list above.

Let $j \in \mathbb{N}$ and F_1, $F_2 \in \operatorname{Int}(D)$ (not necessarily irreducible) such that $F^j = F_1 F_2$. By Fact 3.10, we know that

$$F_1 \sim \frac{\mathcal{P}^{\boldsymbol{k}}}{p^\ell} = \frac{\prod_{i=1}^{r+1} g_i^{k_i}}{p^\ell} \quad \text{and} \quad F_2 \sim \frac{\mathcal{P}^{j\mathbf{1}-\boldsymbol{k}}}{p^{jn-\ell}} = \frac{\prod_{i=1}^{r+1} g_i^{j-k_i}}{p^{jn-\ell}} \tag{6.2}$$

for some $0 \leq \ell \leq jn$, $\boldsymbol{k} = (k_i)_{i=1}^{r+1} \in \mathbb{N}_0^{r+1}$ with $\boldsymbol{k} \leq j\mathbf{1}$ such that

$$\mathsf{v}(\mathrm{d}(\mathcal{P}^{\boldsymbol{k}})) \geq \ell \quad \text{and} \quad \mathsf{v}(\mathrm{d}(\mathcal{P}^{j\mathbf{1}-\boldsymbol{k}})) \geq jn - \ell.$$

We apply Lemma 4.7 for the factor F_1 of F^j and conclude that

$$\boldsymbol{k} = \frac{\ell}{n}\mathbf{1} + \lambda \boldsymbol{v} \tag{6.3}$$

for some $\lambda \in \mathbb{Q}$.

Observe that $k_i \in \mathbb{N}_0$ and hence if $\lambda = 0$, then F_1 is necessarily a power of F (possibly the 0-th if $\ell = 0$), resulting in a trivial factorization of F^j. Moreover, $\ell = 0$ immediately implies $\lambda = 0$, since $k_i \geq 0$ and $\boldsymbol{v}$ has positive and negative components.

Thus, we can safely assume $\ell > 0$ and $\lambda \neq 0$ from now on. From (6.3) and $v_{r+1} = 0$, we infer

$$0 < \frac{\ell}{n} = \frac{\ell}{n} + \lambda v_{r+1} = k_{r+1} \in \mathbb{N}$$

and therefore that n divides ℓ. We set $k = k_{r+1}$, so that $\ell = kn$.

This allows us to address Item (b) and show that F is irreducible. We consider non-trivial factorizations of F itself, that is, $j = 1$. Then $\boldsymbol{k} \leq \mathbf{1}$, which implies $k = k_{r+1} = 1$ and hence $\ell = kn = n$. Given the structure of A, it follows that for each choice of $J \subsetneq [r+1]$ there exists a fixed divisor witness w such that

$$\mathsf{v}\left(\prod_{i \in J} g_i(w)\right) < n,$$

which, in combination with $\mathsf{v}(\mathrm{d}(\mathcal{P}^{\boldsymbol{k}})) \geq \ell = n$, implies that each g_i has to appear as a factor of the numerator of F_1. In other words, $\boldsymbol{k} = \mathbf{1}$ and hence $F_1 = F$, that is, F is irreducible.

It remains to prove Item (a): Whenever F^j factors non-uniquely, then $j \geq (n+1)K$. At this point, we can assume that $j \geq 2$. Moreover, note that $\boldsymbol{k} \neq e\mathbf{1}$ for all $e \in \mathbb{N}_0$, since $F_1 F_2$ is a non-trivial factorization of F. To simplify the following arguments, we also assume $\lambda v_1 > 0$ (by transition from $\boldsymbol{v}$ to $-\boldsymbol{v} \in \ker(A)$ if necessary). Since v_1 and v_2 have different signs, we obtain $\lambda v_2 < 0$.

Further, Equation (6.3) yields

$$k_r = k + \lambda v_r = k + \lambda,$$

which implies $\lambda \in \mathbb{Z}$, as k_r and k are integers.

Also, we conclude from Equation (6.3)

$$k_1 = k + \lambda v_1 \quad \text{and} \quad k_2 = k + \lambda v_2.$$

By hypothesis, there exist elements $a_1, a_2 \in R$ such that $\mathsf{v}(g_i(a_i)) = n+1$ and $\mathsf{v}(g_j(a_i)) = 0$ for $1 \leq i \leq 2$ and all $1 \leq j \leq r+1$ with $j \neq i$. This further implies

$$\mathsf{v}\big(\mathcal{P}^{\boldsymbol{k}}(a_2)\big) = k_2 \mathsf{v}(g_2(a_2)) = (k + \lambda v_2)(n+1) \geq \ell.$$

Since $\ell = kn$ and $\lambda v_2 < 0$ by assumption, we conclude that

$$k \geq -\lambda v_2(n+1) = |\lambda v_2|(n+1). \tag{6.4}$$

Similarly, we evaluate f_2 at a_1 to see

$$\mathsf{v}\big(\mathcal{P}^{j\boldsymbol{1}-\boldsymbol{k}}(a_1)\big) = (j - k_1)\mathsf{v}(g_1(a_1)) = (j - k - \lambda v_1)(n+1) \geq jn - \ell.$$

This further implies

$$j - k \geq \lambda v_1(n+1) = |\lambda v_1|(n+1). \tag{6.5}$$

Summing up Equations (6.4) and (6.5) yields

$$j \geq (n+1)|\lambda|(|v_1| + |v_2|) = |\lambda|(n+1)K.$$

Due to $\lambda \in \mathbb{Z}$, $\lambda \neq 0$, we obtain $j \geq (n+1)K$ whenever F^j factors non-uniquely, which completes the proof. $\square$

For the remaining part of this section, we show that for every choice of integers r, $n \geq 2$, there exists a discrete valuation domain R with finite residue field and a set of irreducible, non-constant polynomials $\mathcal{P}$ which satisfy the hypotheses of Proposition 6.1. For the construction, we need a lemma that allows us to simultaneously replace a family of polynomials by “irreducible variants” which exhibit a similar behavior concerning the valuations when evaluating at elements of R. The following result is a slight variation of [17, Lemma 3.3]. Note that the proof is almost identical and only differs in the fact that we want to control valuations up to some prespecified point and not only up to the fixed divisor. The original result [17, Lemma 3.3] follows as a special case, as described in Remark 6.4 below.

Lemma 6.2 *(Variation of [17, Lemma 3.3]). Let D be a Dedekind domain with infinitely many maximal ideals and K its quotient field. Further, let $I \neq \emptyset$ be a finite set and $h_i \in D[x]$ for $i \in I$ be monic, non-constant polynomials and set $d = \sum_{i\in I} \deg(h_i)$.*

Then, for every $n \in \mathbb{N}_0$, there exist monic polynomials $g_i \in D[x]$ for $i \in I$ such that

(i) $\deg(g_i) = \deg(h_i)$ *for all $i \in I$,*
(ii) *the polynomials g_i are irreducible in $K[x]$ and pairwise non-associated in $K[x]$, and*
(iii) $g_i \equiv h_i \mod P^{n+1}D[x]$ *for every maximal ideal P of D of index at most d.*

Remark 6.3. Note that for any Dedekind domain D and prime ideal P of D: If $g \equiv h \mod P^{n+1}D[x]$, then $g(a) \equiv h(a) \mod P^{n+1}$ for all $a \in D$.

Remark 6.4. The original assertion [17, Lemma 3.3.] follows immediately by choosing $n = \max\{\mathsf{v}_P(\prod_{i\in I} h_i) \mid P \text{ prime ideal of } D \text{ with } |D/P| \leq d\}$ and observing that Lemma 6.2(iii) together with Remarks 4.3 and 6.3 imply that

$$\mathrm{d}\left(\prod_{i\in J_1} g_i \prod_{j\in J_2} h_i\right) = \mathrm{d}\left(\prod_{i\in I} h_i\right)$$

holds for all partitions $J_1 \uplus J_2 = I$.

Proof. Let $P_1, \ldots, P_m$ be all maximal ideals of D whose respective residue fields have cardinality less than or equal to d, cf. [28, Proposition 13] as to why there are only finitely many.

Then there exist $e_1, \ldots, e_m \in \mathbb{N}_0$ such that

$$\mathrm{d}\left(\prod_{i\in I} h_i\right) = \prod_{i=1}^{m} P_i^{e_i}.$$

Let Q be a prime ideal of D different from any of the P_i above. Further, for $i \in I$, let $h_i = x^{d_i} + \sum_{j=0}^{d_i-1} h_{i,j}x^j$ with $d_i \in \mathbb{N}$ and $h_{i,j} \in D$ the coefficient of x^j of h_i. By the Chinese Remainder Theorem, there exist $c_{i,j} \in D$ for $i \in I$ and $0 \leq j \leq d_i - 1$ such that

(a) $c_{i,j} \in \prod_{i=1}^{m} P_i^{e_i+n+1}$ for all $i \in I$ and $0 \leq j \leq d_i - 1$,
(b) $c_{i,j} \equiv -h_{i,j} \mod Q$ for all $i \in I$ and $0 \leq j \leq d_i - 1$, and
(c) $c_{i,0} \not\equiv -h_{i,0} \mod Q^2$ for all $i \in I$.

These conditions determine the elements $c_{i,j}$ only modulo $Q^2 \prod_{i=1}^{m} P_i^{e_i+n+1}$. This allows us to choose the elements in a way such that $c_{i,0} + h_{i,0} \neq c_{j,0} + h_{j,0}$ for $i \neq j$.

We set

$$g_i = h_i + \sum_{j=0}^{d_i-1} c_{i,j}x^j.$$

By construction, the polynomials g_i are monic and satisfy Assertion (i). Moreover, by choice of $c_{i,j}$, it follows that

$$g_i \equiv h_i \mod \prod_{i=1}^{m} P_i^{e_i+n+1}D[x],$$

which, in turn, implies Assertion (iii).

Finally, by construction, the polynomials g_i, $i \in I$, are irreducible in $D[x]$ according to Eisenstein's criterion (cf. [22, §29, Lemma 1]). Since the g_i are monic and D is integrally closed, it follows that the polynomials g_i are also irreducible in $K[x]$ (cf. [6, Ch. 5, §1.3, Prop. 11]). The choice of $c_{i,0}$ guarantees that the g_i are pairwise non-associated in $K[x]$. Hence Assertion (ii) holds, which completes the proof. □

Theorem 4. *Let r, $n \geq 2$ be integers.*

Then there exists a discrete valuation domain (R, pR) with finite residue field and a polynomial $F = \frac{f}{p^n} \in \mathrm{Int}(R)$ which is irreducible, but **not** *absolutely irreducible in $\mathrm{Int}(R)$ (both R and F depending on r) such that the minimal exponent S for which F^S does not factor uniquely satisfies*

(i) $S = (n+1)\left((n-1)^{r-1} + (n-1)^{r-2}\right)$ *where r is the rank of a (reduced) fdp matrix of f and*
(ii) $S = (n+1)\min\left\{\|\boldsymbol{v}^+\|_\infty + \|\boldsymbol{v}^-\|_\infty \;\middle|\; \mathbf{0} \neq \boldsymbol{v} \in \text{fd-ker}(f) \cap \mathbb{Z}^{\mathcal{P}}\right\}$.

In particular, it follows that the lower bound given in Theorem 1 cannot be improved in general.

Remark 6.5. As to the dependence of R and F on r, we point out that the size of the residue field of R in the construction below is at least $r+2$ and the polynomial f has $r+1$ non-associated, irreducible factors.

Proof. Let p be a prime number with $p \geq r+2$ and set $R = \mathbb{Z}_{(p)}$. In order to prove the assertions, we construct polynomials $g_1, \ldots, g_{r+1}$ to satisfy the hypotheses of Proposition 6.1. The construction takes place over the ring $\mathbb{Z}$ instead of $\mathbb{Z}_{(p)}$, as we would like to invoke Lemma 6.2 to find $g_j \in \mathbb{Z}[x]$ with the desired properties.

We choose $w_1, w_2, \ldots, w_r, a_1, a_2, z_{r+3}, \ldots, z_p \in \mathbb{Z}$ to be a complete system of residues modulo $p \geq r+2$. For simplicity, we assume that this choice does not contain a complete set of residues modulo any prime less than p.

Then there exist $b_1, \ldots, b_r, c_1, c_2 \in \mathbb{Z}$ satisfying the conditions

(i) $\mathsf{v}(b_i - w_i) = 1$ for all $1 \le i \le r$ and
(ii) $\mathsf{v}(c_i - a_i) = 1$ for $i = 1, 2$.

We set

$$h_j = \begin{cases} (x-b_1)(x-c_1)^{n+1} & j = 1, \\ (x-b_1)^{n-1}(x-b_2)(x-c_2)^{n+1} & j = 2, \\ (x-b_{j-1})^{n-1}(x-b_j) & 3 \le j \le r-1, \\ (x-b_{r-1})^{n-1} & j = r, \text{ and} \\ (x-b_r)^n \prod_{i=r+3}^{p}(x-z_i)^{n+1} & j = r+1. \end{cases}$$

By construction, it follows that

$$\mathsf{v}(h_j(w_i)) = \begin{cases} 1 & i = j \text{ and } 1 \le j \le r-1, \\ n-1 & i = j-1 \text{ and } 2 \le j \le r, \\ n & i = r \text{ and } j = r+1, \\ 0 & \text{otherwise}, \end{cases} \tag{6.6}$$

and, for $\ell = 1, 2$,

$$\mathsf{v}(h_j(a_\ell)) = \begin{cases} n+1 & j = \ell, \text{ and} \\ 0 & j \ne \ell \text{ and } 1 \le j \le r+1. \end{cases}$$

Moreover, if $a \in R$, then a is congruent to exactly one of the w_i, a_ℓ, or z_k with $1 \le i \le r$, $\ell = 1, 2$, and $r+3 \le k \le p$ modulo pR. This implies that a is congruent to one of the elements b_i, c_ℓ, or z_k. Thus, for all $a \in R$,

$$\mathsf{v}\left(\prod_{j=1}^{r+1} h_j(a)\right) \ge \begin{cases} 1 + (n-1) & a \equiv b_i \mod pR \text{ with } 1 \le i \le r-1, \\ n & a \equiv b_r \mod pR, \\ n+1 & a \equiv c_\ell \text{ or } a \equiv z_k \text{ with } \ell = 1, 2,\ r+3 \le k \le p, \end{cases}$$

and hence, in combination with Equation (6.6),

$$\mathsf{v}\left(\mathrm{d}\left(\prod_{j=1}^{r+1} h_j\right)\right) = n.$$

We apply Lemma 6.2 to find monic polynomials $g_j \in \mathbb{Z}[x]$ for $1 \le j \le r+1$ which are irreducible in $\mathbb{Q}[x]$ such that for all $1 \le j \le r+1$, we have

$$g_j \equiv h_j \mod p^{n+2}\mathbb{Z}[x]. \tag{6.7}$$

Note that all g_j are irreducible in $\mathbb{Q}[x]$ by Lemma 6.2, and hence all g_i are irreducible in $\mathbb{Z}_{(p)}[x] \subseteq \mathbb{Q}[x]$. Moreover, from (6.7) we conclude that

$$g_j \equiv h_j \mod p^{n+2}\mathbb{Z}_{(p)}[x]$$

holds, which, in turn, immediately implies

$$g_j(a) \equiv h_j(a) \mod p^{n+2}\mathbb{Z}_{(p)} \tag{6.8}$$

for all $a \in \mathbb{Z}_{(p)} = R$ and all $1 \leq j \leq r+1$.

We set $f = \prod_{j=1}^{r+1} g_j$. By Remark 4.3, in combination with Congruence (6.8), it follows that $\mathsf{v}(g_j(w_i)) = \mathsf{v}(h_j(w_i))$ and $\mathsf{v}(g_j(a_\ell)) = \mathsf{v}(h_j(a_\ell))$ for all $1 \leq j \leq r+1$, $1 \leq i \leq r$, and $\ell = 1, 2$. This implies that $g_1, \ldots, g_{r+1}$ satisfy the hypotheses of Proposition 6.1. The assertion follows. $\square$

Data availability

No data was used for the research described in the article.

References

[1] David F. Anderson, Paul-Jean Cahen, Scott T. Chapman, William W. Smith, Some factorization properties of the ring of integer-valued polynomials, in: Zero-Dimensional Commutative Rings, Knoxville, TN, 1994, in: Lecture Notes in Pure and Appl. Math., vol. 171, Dekker, New York, 1995, pp. 125–142, MR 1335709.

[2] Gerhard Angermüller, Strong atoms in monadically Krull monoids, Semigroup Forum 104 (1) (2022) 10–17, MR 4368918.

[3] Austin Antoniou, Sarah Nakato, Roswitha Rissner, Irreducible polynomials in int($\mathbb{Z}$), ITM Web Conf. 20 (2018) 01004.

[4] Paul Baginski, Ross Kravitz, A new characterization of half-factorial Krull monoids, J. Algebra Appl. 9 (5) (2010) 825–837, MR 2726558.

[5] Alan Baker, Transcendental Number Theory, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990, MR 1074572.

[6] Nicolas Bourbaki, Commutative Algebra, Chapters 1–7, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation. MR 1727221.

[7] Paul-Jean Cahen, Jean-Luc Chabert, Elasticity for integral-valued polynomials, J. Pure Appl. Algebra 103 (3) (1995) 303–311, MR 1357791.

[8] Paul-Jean Cahen, Jean-Luc Chabert, Integer-Valued Polynomials, Mathematical Surveys and Monographs, vol. 48, American Mathematical Society, Providence, RI, 1997, MR 1421321.

[9] Paul-Jean Cahen, Jean-Luc Chabert, What you should know about integer-valued polynomials, Am. Math. Mon. 123 (4) (2016) 311–337, MR 3493376.

[10] Paul-Jean Cahen, Jean-Luc Chabert, Sophie Frisch, Interpolation domains, J. Algebra 225 (2) (2000) 794–803, MR 1741562.

[11] Scott T. Chapman, Ulrich Krause, A closer look at non-unique factorization via atomic decay and strong atoms, in: Progress in Commutative Algebra 2, Walter de Gruyter, Berlin, 2012, pp. 301–315, MR 2932599.

[12] Scott T. Chapman, Barbara A. McClain, Irreducible polynomials and full elasticity in rings of integer-valued polynomials, J. Algebra 293 (2) (2005) 595–610, MR 2173716.

[13] Victor Fadinger, Sophie Frisch, Daniel Windisch, Integer-valued polynomials on discrete valuation rings of global fields with prescribed lengths of factorizations, 2022 (submitted).

[14] Sophie Frisch, A construction of integer-valued polynomials with prescribed sets of lengths of factorizations, Monatshefte Math. 171 (3–4) (2013) 341–350, MR 3090795.
[15] Sophie Frisch, Relative polynomial closure and monadically Krull monoids of integer-valued polynomials, in: Multiplicative Ideal Theory and Factorization Theory, in: Springer Proc. Math. Stat., vol. 170, Springer, Cham, 2016, pp. 145–157, MR 3565807.
[16] Sophie Frisch, Sarah Nakato, A graph-theoretic criterion for absolute irreducibility of integer-valued polynomials with square-free denominator, Commun. Algebra 48 (9) (2020) 3716–3723 .
[17] Sophie Frisch, Sarah Nakato, Roswitha Rissner, Sets of lengths of factorizations of integer-valued polynomials on Dedekind domains with finite residue fields, J. Algebra 528 (2019) 231–249.
[18] Sophie Frisch, Sarah Nakato, Roswitha Rissner, Split absolutely irreducible integer-valued polynomials over discrete valuation domains, J. Algebra 602 (2022) 247–277, MR 4403611.
[19] Alfred Geroldinger, Franz Halter-Koch, Non-unique factorizations, in: Algebraic, Combinatorial and Analytic Theory, in: Pure and Applied Mathematics (Boca Raton), vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006, MR 2194494.
[20] Jerzy Kaczorowski, Completely irreducible numbers in algebraic number fields, Funct. Approx. Comment. Math. 11 (1981) 95–104, MR 692718.
[21] K. Alan Loper, A classification of all D such that $\mathrm{Int}(D)$ is a Prüfer domain, Proc. Am. Math. Soc. 126 (3) (1998) 657–660, MR 1459137.
[22] Hideyuki Matsumura, Commutative Ring Theory, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid, MR 1011461.
[23] Barbara Anne McClain, Factorisation properties of integer-valued polynomials, Honors thesis at Trinity University, 2004.
[24] Sarah Nakato, Non-absolutely irreducible elements in the ring of integer-valued polynomials, Commun. Algebra 48 (4) (2020) 1789–1802.
[25] Giulio Peruginelli, Factorization of integer-valued polynomials with square-free denominator, Commun. Algebra 43 (1) (2015) 197–211, MR 3240414.
[26] Andreas Reinhart, On monoids and domains whose monadic submonoids are Krull, in: Commutative Algebra, Springer, New York, 2014, pp. 307–330, MR 3330226.
[27] Roswitha Rissner, Daniel Windisch, Absolute irreducibility of the binomial polynomials, J. Algebra 578 (2021) 92–114.
[28] Pierre Samuel, About Euclidean rings, J. Algebra 19 (1971) 282–301, MR 0280470.