A GRAPH-THEORETIC CRITERION FOR ABSOLUTE IRREDUCIBILITY OF INTEGER-VALUED POLYNOMIALS WITH SQUARE-FREE DENOMINATOR

SOPHIE FRISCH AND SARAH NAKATO

Abstract. An irreducible element of a commutative ring is absolutely irreducible if no power of it has more than one (essentially different) factorization into irreducibles. In the case of the ring $\mathrm{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}$, of integer-valued polynomials on a principal ideal domain D with quotient field K, we give an easy to verify graph-theoretic sufficient condition for an element to be absolutely irreducible and show a partial converse: the condition is necessary and sufficient for polynomials with square-free denominator.

1. Introduction

An intriguing feature of non-unique factorization (of elements of an integral domain into irreducibles) is the existence of non-absolutely irreducible elements, that is, irreducible elements some of whose powers allow several essentially different factorizations into irreducibles [1, 5, 6, 7, 8].

For rings of integers in number fields, their existence actually characterizes non-unique factorization, as Chapman and Krause [3] have shown.

Here, we investigate absolutely and non-absolutely irreducible elements in the context of non-unique factorization into irreducibles in the ring of integer-valued polynomials on D

$$\mathrm{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\},$$

where D is a principal ideal domain and K is its quotient field.

In an earlier paper [4, Remark 3.9] we already hinted at a graph-theoretic sufficient condition for $f \in \mathrm{Int}(D)$ to be irreducible. We spell this out more fully in Theorem 1. The condition is not, however, necessary.

We formulate a similar graph-theoretic sufficient condition for $f \in \mathrm{Int}(D)$ to be absolutely irreducible in Theorem 2, and show a partial converse. Namely, our criterion for absolute irreducibility is necessary and sufficient in the special case of polynomials with square-free denominator, cf. Theorem 3.

First, we recall some terminology. Let R be a commutative ring with identity.

(i) $r \in R$ is called *irreducible* in R (or, an *atom* of R) if it is a non-zero non-unit that is not a product of two non-units of R.

(ii) A *factorization* (into irreducibles) of r in R is an expression

$$r = a_1 \cdots a_n \tag{1}$$

where $n \geq 1$ and a_i is irreducible in R for $1 \leq i \leq n$.

(iii) $r, s \in R$ are *associated* in R if there exists a unit $u \in R$ such that $r = us$. We denote this by $r \sim s$.

2010 *Mathematics Subject Classification.* 13A05, 13B25, 13F20, 11R09, 11C08.

Key words and phrases. factorization, non-unique factorization, irreducible elements, absolutely irreducible elements, atoms, strong atoms, atomic domains, integer-valued polynomials, simple graphs, connected graphs.

S. Frisch is supported by the Austrian Science Fund (FWF): P 30934.

S. Nakato is supported by the Austrian Science Fund (FWF): P 30934.

(iv) Two factorizations into irreducibles of the same element,
$$r = a_1 \cdots a_n = b_1 \cdots b_m, \tag{2}$$
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 (2) are called *essentially different.*

Definition 1.1. Let R be a commutative ring with identity. An irreducible element $c \in R$ is called *absolutely irreducible* (or, a *strong atom*), if no power c^n with $n \geq 1$ has more than one essentially different factorization into irreducibles.

Note the following fine distinction: an element of R that is called *"not absolutely irreducible"* might not be irreducible at all, whereas a *"non-absolutely irreducible"* element is assumed to be irreducible, but not absolutely irreducible.

We now concentrate on integer-valued polynomials over a principal ideal domain.

Recall that a polynomial in $D[x]$, where D is a principal ideal domain, is called *primitive* if the greatest common divisor of its coefficients is 1.

Definition 1.2. Let D be a principal ideal domain with quotient field K, and $f \in K[x]$ a non-zero polynomial. We write f as
$$f = \frac{a \prod_{i \in I} g_i}{b},$$
where $a, b \in D \setminus \{0\}$ with $\gcd(a, b) = 1$, I a finite (possibly empty) set, and each g_i primitive and irreducible in $D[x]$ and call this the *standard form* of f.

We refer to b as the *denominator*, to a as the *constant factor*, and to $a \prod_{i \in I} g_i$ as the *numerator* of f, keeping in mind that each of them is well-defined and unique only up to multiplication by units of D.

Definition 1.3. For $f \in \mathrm{Int}(D)$, the *fixed divisor* of f, denoted $\mathsf{d}(f)$, is the ideal of D generated by $f(D)$.

An integer-valued polynomial $f \in \mathrm{Int}(D)$ with $\mathsf{d}(f) = D$ is called *image-primitive.*

When D is a principal ideal domain, we may, by abuse of notation, write the generator for the ideal, as in $\mathsf{d}(f) = c$ meaning $\mathsf{d}(f) = cD$.

Remark 1.4. Let D be a principal ideal domain with quotient field K, and $f \in K[x]$ written in standard form as in Definition 1.2. Then f is in $\mathrm{Int}(D)$ if and only if b divides $\mathsf{d}(\prod_{i \in I} g_i)$.

Remark 1.5. Let D be a principal ideal domain with quotient field K. Then any non-constant irreducible element of $\mathrm{Int}(D)$ is necessarily image-primitive. Otherwise, if a prime element $p \in D$ divides $\mathsf{d}(f)$, then
$$f = p \cdot \frac{f}{p}$$
is a non-trivial factorization of f.

Furthermore, $f \in K[x] \setminus \{0\}$ (written in standard form as in Definition 1.2) is an image-primitive element of $\mathrm{Int}(D)$ if and only if (up to multiplication by units) $a = 1$ and $b = \mathsf{d}(\prod_{i \in I} g_i)$.

Definition 1.6. Let D be a principal ideal domain. For $f \in \mathrm{Int}(D)$, and p a prime element in D, we let
$$\mathsf{d}_p(f) = v_p(\mathsf{d}(f))$$

Remark 1.7. By the above definition,
$$\mathsf{d}(f) = \prod_{p \in \mathbb{P}} p^{\mathsf{d}_p(f)} \quad \text{and} \quad \mathsf{d}_p(f) = \min_{c \in D} v_p(f(c))$$

where $\mathbb{P}$ is a set of representatives of the prime elements of D up to multiplication by units.

By the nature of the minimum function, the fixed divisor is not multiplicative:

$$\mathsf{d}_p(f) + \mathsf{d}_p(g) \leq \mathsf{d}_p(fg),$$

but the inequality may be strict. Accordingly,

$$\mathsf{d}(f)\mathsf{d}(g) \,\big|\, \mathsf{d}(fg),$$

but the division may be strict. Note, however, that

$$\mathsf{d}(f^n) = \mathsf{d}(f)^n$$

for all $f \in \mathrm{Int}(D)$ and $n \in \mathbb{N}$.

2. Graph-theoretic irreducibility criteria

Definition 2.1. Let D be a principal ideal domain, $I \neq \emptyset$ a finite set and for $i \in I$, let $g_i \in D[x]$ be non-constant and primitive. Let $g(x) = \prod_{i\in I} g_i$, and $p \in D$ be prime.

(i) We say that g_i is *essential* for p among the g_j with $j \in I$ if $p \,\big|\, \mathsf{d}(g)$ and there exists a $w \in D$ such that $v_p(g_i(w)) > 0$ and $v_p(g_j(w)) = 0$ for all $j \in I \setminus \{i\}$. Such a w is then called a witness for g_i being essential for p.

(ii) We say that g_i is *quintessential* for p among the g_j with $j \in I$ if $p \,\big|\, \mathsf{d}(g)$ and there exists $w \in D$ such that $v_p(g_i(w)) = v_p(\mathsf{d}(g))$ and $v_p(g_j(w)) = 0$ for all $j \in I \setminus \{i\}$. Such a w is called a witness for g_i being quintessential for p.

We will omit saying "among the g_j with $j \in I$" if the indexed set of polynomials is clear from the context.

Remark 2.2. When we consider an indexed set of polynomials g_i with $i \in I$, we are not, in general, requiring $g_i \neq g_j$ for $i \neq j$. Note, however, that g_i being essential (among the g_j with $j \in I$) for some prime element $p \in D$ implies $g_i \not\sim g_j$ in $D[x]$ for all $j \in I \setminus \{i\}$.

Definition 2.3. Let D be a principal ideal domain, $p \in D$ a prime element, $I \neq \emptyset$ a finite set and for each $i \in I$, $g_i \in D[x]$ primitive and irreducible.

(i) The *essential graph* of the indexed set of polynomials $(g_i \mid i \in I)$ is the simple undirected graph whose set of vertices is I, and in which (i, j) is an edge if and only if there exists a prime element p in D such that both g_i and g_j are essential for p.

(ii) The *quintessential graph* of the indexed set of polynomials $(g_i \mid i \in I)$ is the simple undirected graph whose set of vertices is I, and in which (i, j) is an edge if and only if there exists a prime element p in D such that both g_i and g_j are quintessential for p.

Lemma 2.4. *Let D be a principal ideal domain and $f \in \mathrm{Int}(D)$ a non-constant image-primitive integer-valued polynomial, written in standard form according to Definition 1.2 as*

$$f = \frac{\prod_{i\in I} g_i}{\prod_{p\in T} p^{e_p}},$$

where T is a finite set of pairwise non-associated primes of D, and let $n \in \mathbb{N}$.

Every $h \in \mathrm{Int}(D)$ dividing f^n can be written as

$$h(x) = \frac{\prod_{i\in I} g_i^{\gamma_i(h)}}{\prod_{p\in T} p^{\beta_p(h)}},$$

with $\gamma_i(h) \in \mathbb{N}_0$ for $i \in I$ and unique $\beta_p(h) \in \mathbb{N}_0$ for $p \in T$. Moreover, every such representation of h satisfies:

(i) *If $q \in T$ and $j \in I$ such that g_j is quintessential for q among the $i \in I$, then*
$$\beta_q(h) = e_q\gamma_j(h).$$

(ii) *In particular, whenever g_j and g_k are both quintessential for the same prime $q \in T$, then $\gamma_j(h) = \gamma_k(h)$.*

Proof. We know $\mathsf{d}(f^n) = \mathsf{d}(f)^n$ (cf. Remark 1.7). So, f^n is image-primitive, and, therefore, all polynomials in $\mathrm{Int}(D)$ dividing f^n are image-primitive. Let $f^n = hk$ with $h, k \in \mathrm{Int}(D)$. When h is written in standard form as in Definition 1.2, the fixed divisor of the numerator equals the denominator, and the constant factor is a unit. The same holds for k. This is so because h and k are image-primitive; see Remark 1.5.

Now let $q \in D$ be prime and $j \in I$ such that g_j is quintessential for q. Note that, by Remark 2.2 and unique factorization in $K[x]$, the exponent of g_j in the numerator of any factor of f^n is unique.

Writing $f^n = hk$ as
$$\frac{\prod_{i\in I} g_i^n}{\prod_{p\in T} p^{ne_p}} = \frac{\prod_{i\in I} g_i^{\gamma_i(h)}}{\prod_{p\in T} p^{\beta_p(h)}} \cdot \frac{\prod_{i\in I} g_i^{\gamma_i(k)}}{\prod_{p\in T} p^{\beta_p(k)}},$$
we observe equalities and inequalities of the exponents, which, together, imply $e_q\gamma_j(h) = \beta_q(h)$ and $e_q\gamma_j(k) = \beta_q(k)$; namely:

(i) $ne_q = \beta_q(h) + \beta_q(k)$
(ii) $n = \gamma_j(h) + \gamma_j(k)$ and hence $ne_q = e_q\gamma_j(h) + e_q\gamma_j(k)$
(iii) $e_q\gamma_j(h) \geq \beta_q(h)$ and $e_q\gamma_j(k) \geq \beta_q(k)$

(i) follows from unique factorization in D.
(ii) follows from unique factorization in $K[x]$ and Remark 2.2.

To see (iii), consider a witness w for g_j being quintessential for q. Since f is image-primitive, $e_q = v_q(\mathsf{d}(\prod_{i\in I} g_i))$, by Remark 1.5. From Definition 2.1 and Remark 1.4 we deduce
$$e_q\gamma_j(h) = v_q(g_j(w))\gamma_j(h) = v_q(g_j^{\gamma_j(h)}(w)) = v_q\left(\prod_{i\in I} g_i(w)^{\gamma_i(h)}\right) \geq \beta_q(h)$$
(and similarly for k instead of h). □

Theorem 1. *Let D be a principal ideal domain with quotient field K. Let $f \in \mathrm{Int}(D)$ be a non-constant image-primitive integer-valued polynomial, written in standard form as $f = g/b$ with $b \in D \setminus \{0\}$, and $g = \prod_{i\in I} g_i$, where each g_i is primitive and irreducible in $D[x]$.*

If the essential graph of $(g_i \mid i \in I)$ is connected, then f is irreducible in $\mathrm{Int}(D)$.

Proof. If $|I| = 1$, then f is irreducible in $K[x]$, and, by being image-primitive, also irreducible in $\mathrm{Int}(D)$.

Now assume $|I| > 1$, and suppose f can be expressed as a product of m non-units $f = f_1 \cdots f_m$ in $\mathrm{Int}(D)$. Since $\mathsf{d}(f) = 1$, we see immediately that no f_i is a constant, and that $\mathsf{d}(f_k) = 1$ for every $1 \leq k \leq m$.

Write $f_k = h_k/b_k$ with $b_k \in D$ and h_k primitive in $D[x]$. Then $b = b_1 \cdots b_m$ and there exists a partition of I into non-empty pairwise disjoint subsets $I = \bigcup_{i=1}^m I_k$, such that $h_k = \prod_{i\in I_k} g_i$.

Select $i \in I_1$ and $j \in I$ with $j \neq i$. We show that also $j \in I_1$. Let $i = i_0, i_1, \ldots, i_s = j$ be a path from i to j in the essential graph of $(g_i \mid i \in I)$. For some prime element p in D dividing b, g_{i_0} and g_{i_1} are both essential for p. As g_i

is essential for p, p cannot divide any b_k with $k \neq 1$ and, hence, p divides b_1. For any g_k essential for p it follows that $k \in I_1$, and, in particular, $i_1 \in I_1$. The same argument shows for any two adjacent vertices i_k and i_{k+1} in the path that they pertain to the same I_k, and, finally, that $j \in I_1$.

As $j \in I$ was arbitrary, $I_1 = I$ and $m = 1$. □

Theorem 2. *Let D be a principal ideal domain and $f \in \mathrm{Int}(D)$ be non-constant and image-primitive, written in standard form as*

$$f = \frac{\prod_{i\in I} g_i}{\prod_{p\in T} p^{e_p}},$$

where $I \neq \emptyset$ is a finite set and for $i \in I$, $g_i \in D[x]$ is primitive and irreducible in $D[x]$.

If the quintessential graph G of $(g_i \mid i \in I)$ is connected, then f is absolutely irreducible.

Proof. Suppose

$$f^n = \prod_{l=1}^{s} f_l, \quad \text{where} \quad f_l = \frac{\prod_{i\in I} g_i^{m_l(i)}}{\prod_{p\in T} p^{k_l(p)}}$$

and $0 \leq m_l(i) \leq n$, $0 \leq k_l(p) \leq ne_p$ and for all i, $\sum_{l=1}^{s} m_l(i) = n$ and for all p, $\sum_{l=1}^{s} k_l(p) = ne_p$.

Fix t with $0 \leq t \leq s$. We show that f_t is a power of f by showing that each g_i with $i \in I$ occurs in the numerator of f_t with the same exponent.

Let $i, j \in I$. By the connectedness of the quintessential graph, there exists a sequence of indices in I, $i = i_0, i_1, i_2, \ldots, i_k = j$ and for each h, a prime element p_h in T such that g_{i_h} and $g_{i_{h+1}}$ are both quintessential for p_h. By Lemma 2.4, g_{i_h} and $g_{i_{h+1}}$ occur in the numerator of f_t with the same exponent. Eventually, g_i and g_j occur in the numerator of f_t with the same exponent, for arbitrary $i, j \in I$. In an image-primitive polynomial, the numerator determines its denominator (as in Remark 1.5) and, hence, f_t is a power of f. Since f_t is irreducible, $f_t = f$. □

Corollary 2.5. *The binomial polynomial*

$$\binom{x}{p} = \frac{x(x-1)\cdots(x-p+1)}{p!}$$

where $p \in \mathbb{Z}$ is a prime, is absolutely irreducible in $\mathrm{Int}(\mathbb{Z})$.

Theorem 3. *Let D be a principal ideal domain and $f \in \mathrm{Int}(D)$ be non-constant and image-primitive, with square-free denominator, written in standard form as*

$$f = \frac{\prod_{i\in I} g_i}{\prod_{p\in T} p},$$

where $I \neq \emptyset$ is a finite set and for $i \in I$, $g_i \in D[x]$ is primitive and irreducible in $D[x]$.

Then f is absolutely irreducible if and only if the quintessential graph G of $(g_i \mid i \in I)$ is connected.

Proof. In view of Theorem 2, we only need to show necessity. If $|I| = 1$, then G is connected. Now assume $|I| > 1$, and suppose G is not connected.

I is the disjoint union of J_1 and J_2 (both non-empty) such that there is no edge (i, j) with $i \in J_1$ and $j \in J_2$. Let S_1 be the set of those primes p in T such that some g_i with $i \in J_1$ is quintessential for p, and S_2 defined similarly in relation to J_2. Then $S_1 \cap S_2 = \emptyset$. We express T as a disjoint union of T_1 and T_2 with $S_i \subseteq T_i$ for $i = 1, 2$ (assigning the primes not in $S_1 \cup S_2$ to T_1 or T_2 arbitrarily).

Then f^3 factors in $\mathrm{Int}(D)$ as follows:

$$f^3 = \frac{\left(\prod_{i\in J_1} g_i\right)^2 \prod_{j\in J_2} g_j}{\left(\prod_{p\in T_1} p\right)^2 \prod_{q\in T_2} q} \cdot \frac{\left(\prod_{j\in J_2} g_j\right)^2 \prod_{i\in J_1} g_i}{\left(\prod_{q\in T_2} q\right)^2 \prod_{p\in T_1} p}.$$

As $\mathrm{Int}(D)$ is atomic (cf. [2]), the fact that J_1 and J_2 are both non-empty implies the existence of a factorization of f^3 into irreducibles essentially different from $f \cdot f \cdot f$. □

If $f(x) = \prod_{i\in I} g_i(x)/p$, where D is a principal ideal domain, p a prime of D and $g_i \in D[x]$ primitive and irreducible in $D[x]$ for $i \in I$, then it is easy to see that f is an irreducible element of $\mathrm{Int}(D)$ if and only if $\mathsf{d}(\prod_{i\in I} g_i(x)) = p$ and for each $i \in I$ there exists $w_i \in D$ such that $v_p(g_i(w_i)) > 0$ and $v_p(g_j(w_i)) = 0$ for all $j \in I \setminus \{i\}$. We can now state the following refinement:

Corollary 2.6. *Let D be a principal ideal domain, $p \in D$ a prime element and $I \neq \emptyset$ a finite set. For $i \in I$, let $g_i \in D[x]$ be primitive and irreducible in $D[x]$. Let*

$$f(x) = \frac{\prod_{i\in I} g_i(x)}{p}.$$

Then f is an absolutely irreducible element of $\mathrm{Int}(D)$ if and only if $\mathsf{d}(\prod_{i\in I} g_i(x)) = p$ and for each $i \in I$ there exists $w_i \in D$ such that $v_p(g_i(w_i)) = 1$ and $v_p(g_j(w_i)) = 0$ for all $j \in I \setminus \{i\}$.

Proof. If $\mathsf{d}(\prod_{i\in I} g_i(x)) = p$, then $f \in \mathrm{Int}(D)$ with $\mathsf{d}(f) = 1$, and Theorem 3 applies. If, on the other hand, f is in $\mathrm{Int}(D)$ and is absolutely irreducible, then f is, in particular, irreducible and therefore $\mathsf{d}(f) = 1$, and, again, Theorem 3 applies. Now the statement follows from the fact that, whenever $\mathsf{d}(\prod_{i\in I} g_i(x)) = p$, the quintessential graph of $(g_i \mid i \in I)$ is connected if and only if every g_i is quintessential for p. □

References

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

[2] Paul-Jean Cahen and Jean-Luc Chabert. Elasticity for integral-valued polynomials. *J. Pure Appl. Algebra*, 103(3):303–311, 1995.

[3] Scott T. Chapman and Ulrich Krause. A closer look at non-unique factorization via atomic decay and strong atoms. In Christopher Francisco, Lee Klingler, Sean Sather-Wagstaff, and Janet C. Vassilev, editors, *Progress in commutative algebra 2 — Closures, Finiteness and Factorization*, pages 301–315. Walter de Gruyter, Berlin, 2012.

[4] Sophie Frisch, Sarah Nakato, and Roswitha Rissner. Sets of lengths of factorizations of integer-valued polynomials on dedekind domains with finite residue fields. *Journal of Algebra*, 528:231 – 249, 2019.

[5] Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations*, volume 278 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.

[6] J. Kaczorowski. A pure arithmetical characterization for certain fields with a given class group. *Colloq. Math.*, 45(2):327–330, 1981.

[7] Sarah Nakato. Non-absolutely irreducible elements in the ring of integer-valued polynomials. *https://arxiv.org/abs/1910.10278v1*, 2019.

[8] David E. Rush. An arithmetic characterization of algebraic number fields with a given class group. *Math. Proc. Cambridge Philos. Soc.*, 94(1):23–28, 1983.

Institut für Analysis und Zahlentheorie, Graz University of Technology
Kopernikusgasse 24, 8010 Graz, Austria
Email address: `frisch@math.tugraz.at`

Institut für Analysis und Zahlentheorie, Graz University of Technology
Kopernikusgasse 24, 8010 Graz, Austria
Email address: `snakato@tugraz.at`