Sarah Nakato, M.Sc.

# Factorization theory in rings of integer-valued polynomials on Dedekind Domains

**DOCTORAL THESIS**

to achieve the university degree of

Doktorin der Naturwissenschaften

submitted to

**Graz University of Technology**

First supervisor

Ao.Univ.-Prof. Mag.rer.nat. Dr.techn. Sophie Frisch

Second supervisor: Dipl.-Ing. Dr.techn. Roswitha Rissner

Graz, June 2020

**AFFIDAVIT**

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present doctoral thesis.

_______________________ Date

_______________________ Signature

# Contents

# Abstract

Unlike the ring $\mathbb{Z}$ of rational integers, where every non-zero non-unit has a unique factorization, there are several algebraic structures in which uniqueness of factorization of elements fails. Factorization theory involves investigating phenomena related to this failure of uniqueness of factorization of elements. In this thesis, we study various concepts of factorization theory in the ring of integer-valued polynomials on a domain $D$,

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

where $K$ is the quotient field of $D$. We focus on domains $D$ which are Dedekind. A crucial object in factorization theory is the set of lengths of a fixed element, that is, the set of all natural numbers $n$ such that a fixed element has a factorization as a product of $n$ irreducibles. We show that every finite multiset of natural numbers greater than 1 occurs as a set of lengths of a polynomial in $\mathrm{Int}(D)$, where $D$ is a Dedekind domain with infinitely many maximal ideals, all of them of finite index. This demonstrates that $\mathrm{Int}(D)$ has unusual wild factorization behaviour as compared to algebraic integers whose sets of lengths exhibit a certain arithmetic structure. Furthermore, we show that there is no transfer homomorphism from the multiplicative monoid of $\mathrm{Int}(D)$ to a block monoid. This implies that $\mathrm{Int}(D)$ is one of the few domains which are not transfer Krull domains. Our proofs are constructive and the factorizations in our constructions are square-free which is also a typical property of known related constructions in the literature. The main hindrance for using non-square-free factorizations is the existence of non-absolutely irreducible elements, that is, irreducible elements some of whose powers allow several essentially different factorizations into irreducibles. Therefore, we want to identify the so-called absolutely irreducible elements, that is, elements all of whose powers have only one (essentially different) factorization. First, we take our Dedekind domain $D$ to be $\mathbb{Z}$, and we construct non-absolutely irreducible elements in $\mathrm{Int}(\mathbb{Z})$. These are crucial in studying patterns of factorizations in $\mathrm{Int}(\mathbb{Z})$. Second, taking our Dedekind domain $D$ to be a principal ideal domain, we give a graph-theoretic sufficient condition for a polynomial $f \in \mathrm{Int}(D)$ to be absolutely irreducible. In addition, we show that our criterion is necessary and sufficient in the special case of polynomials in $\mathrm{Int}(D)$ with square-free denominator.

# Acknowledgement

Firstly, I thank the Almighty God for giving me the wisdom, strength, and perseverance throughout my journey as a student. To God forever be the glory. Secondly, I would like to extend my warmest thanks to my first supervisor, Prof. Sophie Frisch, for giving me the opportunity to further my studies, and for guiding, mentoring and sharing her expertise with me. My warm thanks also go to my second supervisor, Dr. Roswitha Rissner, for mentoring and guiding me, and for also helping me outside academics. I will forever be grateful for their mentorship and kindness. I would also like to thank Prof. Scott Chapman and Prof. Giulio Peruginelli for reviewing my thesis.

My appreciation also goes to the Austrian Science Fund (FWF) and the Institute of Analysis and Number Theory of Graz University of Technology, for the financial support. I would also like to thank the entire staff of the Institute of Analysis and Number Theory, for providing a conducive environment for my studies. In a special way, I would like to thank Prof. Peter Grabner, Prof. Robert Tichy, Mag. Hermine Panzenböck and Mag. Jochen Resch for the administrative and technical support.

I would also like to thank the members of the Algebra and Number Theory group at University of Graz for giving me a second academic home. In a special way, I thank Prof. Alfred Geroldinger, Emeritus. Franz Halter-Koch, Prof. Karin Baur, Prof. Günter Lettl, Prof. Salvatore Tringali, and Prof. Daniel Smertnig, for the useful comments, seminars, and questions.

I would also like to extend my thanks to the following mathematicians, some invited me to give talks at their universities and others shared their expertise with me and continued following up my progress: Prof. Jennifer Balakrishnan, Prof. Kramar Fijavž, Prof. Carmelo Antonio Finocchiaro, Prof. Clemens Heuberger, Prof. Irena Swanson, Prof. Balázs Szendrői, and Prof. Leonid N. Vaserstein. I also thank Dr. David Ssevviiri, my masters supervisor at Makerere University, for laying a foundation for me in algebra.

Lastly, I thank my friends and my church family for always being there for me. In a special way, I thank my dear parents, Mr. Daniel Lwanga and Ms. Gertrude Nakintu, and my sisters, Juliet, Sylvia, and Christine, for their encouragement.

# Preface

This publication-based doctoral thesis consists of three articles by the author. The first two articles were published in mathematical journals, and the third article is accepted for publication. The thesis has four main chapters: the first chapter is an introduction to the topic of the thesis, and the three subsequent chapters are each a reprint of an article. After the main chapters, there is an appendix which contains necessary factorization terms and results that are referred to in the second main chapter. The articles are in the same order as they appear in the list of publications that follows this preface. The fourth article in the list of publications is not part of this thesis.

# List of publications

I. 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), pp. 231–249. ISSN: 0021-8693. doi:10.1016/j.jalgebra.2019.02.040.

II. Sarah Nakato. "Non-absolutely irreducible elements in the ring of integer-valued polynomials". *Communications in Algebra* 48.4 (2020), pp. 1789-1802. doi:10.1080/00927872.2019.1705474

III. Sophie Frisch and Sarah Nakato. "A graph-theoretic criterion for absolute irreducibility of integer-valued polynomials with square-free denominator". *Communications in Algebra* 0.0 (2020), pp. 1-8. doi:10.1080/00927872.2020.1744618.

IV. Austin Antoniou, Sarah Nakato, and Roswitha Rissner. "Irreducible polynomials in Int($\mathbb{Z}$)". *ITMWeb Conf.* 20:01004 (2018). doi:10.1051/itmconf/20182001004

# 1. Introduction

By a factorization we mean an expression of an element of a ring as a product of irreducible elements. It is known that in a Noetherian domain, every non-zero non-unit has a factorization. In fact, this is the case in every domain which satisfies the ascending chain condition on principal ideals (in short ACCP), see for instance [36, Proposition 1.1.4]. However, in many such domains (called *atomic domains*), some elements have more than one factorization. A domain in which every non-zero non-unit has a unique factorization (up to multiplication by a unit and ordering) is called a *unique factorization domain* (or, a factorial domain). Interestingly, the factorization behaviour of a ring gives information about its arithmetic and algebraic properties. In fact, one of the aims of factorization theory is to characterize arithmetical and algebraic properties of algebraic structures in terms of factorization properties. More generally, factorization theory involves investigating phenomena related to non-uniqueness of factorizations in algebraic structures.

Factorization theory originated from algebraic number theory. In the initial attempts to solve Fermat's Last Theorem, the mathematicians in the $19^{\text{th}}$ century, pioneered by Ernst E. Kummer, discovered that not every ring of integers, $\mathcal{O}_K$, of a number field $K$ is a unique factorization domain, cf. [50, p. 19]. It was proved that $\mathcal{O}_K$ is a unique factorization domain if and only if the class number of $K$ is 1, that is, if and only if all the ideals of $\mathcal{O}_K$ are principal. Note that the mathematicians in the $19^{\text{th}}$ century did not immediately study the details of non-uniqueness of factorizations. They instead devised means to avoid it and this led to Richard Dedekind's definition of ideals. They later discovered that although unique factorization of elements fails in $\mathcal{O}_K$, the ring $\mathcal{O}_K$ has unique factorization of ideals into prime ideals. They sought comfort in this and avoided non-unique factorizations of elements.

A renewed interest in non-unique factorizations of elements was sparked off by Carlitz [22]. First recall that the number of irreducible factors in a factorization is called the *length* of that factorization. Carlitz [22] showed that for every non-zero non-unit $a \in \mathcal{O}_K$, the factorizations of $a$ have the same length if and only if $K$ has class number at most 2. Carlitz's result motivated Narkiewicz to further investigate non-unique factorizations in the rings $\mathcal{O}_K$, introducing the notion of blocks, cf. [48, Chapter 9]. Narkiewicz's work is considered as the starting point of the theory of non-unique factorizations. Several researchers, notably, Franz Halter-Koch, further investigated the factorization properties of algebraic integers motivated by the problems Narkiewicz [48] raised, cf. [42].

Zaks [60] called the domains $D$ in which for every non-zero non-unit $a \in D$, the factorizations of $a$ have the same length, *half-factorial* (in short HFD). He further investigated half-factorial domains and gave several examples of such domains, cf. [61]. He also showed in the same paper that if $R$ is a Krull domain, then the polynomial ring $R[x]$ is half factorial if and only if the class group of $R$ is either $\{1\}$ or $\mathbb{Z}/2\mathbb{Z}$. Note the similarity with Carlitz's result. Zaks also sought to answer some problems raised by Narkiewicz [49]. Several researchers have since then investigated half-factorial domains, cf. [23] for a survey.

Factorization theory was further extended to general integral domains by notably, D. D. Anderson, David F. Anderson, Scott T. Chapman, William W. Smith and Muhammad Zafrullah, and it caught a lot of attention in the 1990s, see for instance [3, 4, 2, 9, 10, 26, 27]. A crucial paper in this development was [3] in which D. Anderson, F. Anderson, and Zafrullah introduced and studied finite conditions on the non-unique factorization domains which are not half-factorial. In particular, they introduced the notions of bounded factorization domains and finite factorization domains, and characterized such domains. First recall that the *set of lengths*, $L(r)$, of a non-zero non-unit $r \in D$, is the set of all natural numbers $n$ such that $r$ has a factorization of length $n$ in $D$. In [3], D. Anderson, F. Anderson, and Zafrullah defined a *bounded factorization domain* (in short BFD) as an atomic domain in which the set of lengths $L(r)$ is finite for all $r \in D$. They called an atomic domain $D$ a *finite factorization domain* (in short FFD) if every non-zero non-unit $a \in D$ has a finite number of factorizations. It is clear that every finite factorization domain is a bounded factorization domain. A common chart of implications is Figure 1.1 whose implications again first appeared in D. Anderson, F. Anderson, and Zafrullah's paper [3].

$$
\begin{tikzcd}
& \text{HFD} \arrow[dr, Rightarrow] & & & \\
\text{UFD} \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] & & \text{BFD} \arrow[r, Rightarrow] & \text{ACCP} \arrow[r, Rightarrow] & \text{Atomic} \\
& \text{FFD} \arrow[ur, Rightarrow] & & &
\end{tikzcd}
$$

**Figure 1.1:** Interdependence of factorization properties

In the same spirit as [3], Halter-Koch [41] studied finite conditions on non-unique factorizations in the setting of monoids. He introduced notions of BF-monoids and FF-monoids analogous to BFD and FFD respectively. Note that the non-zero elements of a ring form a multiplicative monoid. In fact, Halter-Koch [41] calls an integral domain $D$ atomic (a BFD, an FFD) if and only if the multiplicative monoid $D\setminus\{0\}$ is atomic (a BF-monoid, an FF-monoid). In general, any factorization property of an integral domain $D$ can be seen by looking at the multiplicative monoid $D\setminus\{0\}$. This observation was mainly by Alfred Geroldinger and Franz Halter-Koch.

Another important observation was that some arithmetic properties and factorization properties of integral domains can be studied from suitably constructed monoids and then transferred back to the domain. This approach was sparked off by Geroldinger and Halter-Koch's notion of divisor homomorphisms in [35]. Halter-Koch [40] further introduced the concept of transfer homomorphisms and proved that these preserve sets of lengths. The monoids which have been widely utilized in the transfer approach are the block monoids (or, monoids of zero-sum sequences). We define these in Appendix A and refer to the monograph by Geroldinger and Halter-Koch [36] for details. In fact, almost everything you need to know about factorization theory can be found in their monograph [36]. It should be mentioned that the monograph [36] has had a tremendous impact on the spread of factorization theory.

Several objects of non-unique factorizations have been studied, for instance, elasticity, sets and distances of lengths, and catenary degree, cf. [36]. Recall that the elasticity of an element $r \in D$ (where $D$ in a BFD) is $\rho(r) = \frac{\max(L(r))}{\min(L(r))}$, and the elasticity of $D$ is $\rho(D) = \sup\{\rho(r) \mid r \in D\setminus\{0\}\}$. Like the class group is known to measure how far a ring $\mathcal{O}_K$ is from being a unique factorization domain, elasticity measures how far a domain is from being half-factorial. In particular, an integral domain (monoid) is half-factorial if and only if its elasticity is 1. The rings of integer-valued polynomials that we study in this thesis have infinite elasticity. See [8] for a survey on early work on elasticity of integral domains. A crucial object of study in factorization theory is the set of lengths of a fixed element, cf. [34] for a survey. The sets of lengths in a domain $D$ tell us how bad the factorization behaviour of $D$ is, and from them we can deduce other objects of non-unique factorizations like elasticity and catenary degree. Chapter 2 of this thesis focuses on sets of lengths, we shall elaborate on this later in this introduction.

Factorization theory is now an independent area of algebra and it has also branched out to several subareas, for instance, see the survey article [58] for factorization theory in non-commutative rings, and [6, 7, 1] for factorization theory in rings with zero-divisors. Here we restrict ourselves to factorization theory in integral domains. First note that the study of non-unique factorizations has mainly been in Krull domains but it has now gained attention in polynomial rings. Our focus here is on the rings of integer-valued polynomials. In fact we are ready to give a review of non-unique factorizations in rings of integer-valued polynomials.

Let $D$ be a domain with quotient field $K$. The ring of integer-valued polynomials on $D$, denoted $\mathrm{Int}(D)$, consists of polynomials in $K[x]$ which map $D$ to $D$. That is,

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

It is well known that the ring $\mathrm{Int}(D)$ is in general not a unique factorization domain. In fact, non-unique factorizations have been intensively investigated in

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}.$$

In this thesis, we investigate non-unique factorizations in $\mathrm{Int}(D)$ when $D$ is a Dedekind domain. We first give a brief history of integer-valued polynomials.

It is well known that for $n \in \mathbb{N}$, the binomial polynomial

$$\binom{x}{n} = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!}$$

is integer-valued on $\mathbb{Z}$. Actually, these form a regular basis of $\mathrm{Int}(\mathbb{Z})$ as a $\mathbb{Z}$-module, moreover, they are irreducible in $\mathrm{Int}(\mathbb{Z})$, cf. [18]. However, the binomial polynomials were first used for polynomial interpolation as early as the $17^{\text{th}}$ century. It was in 1919 that Pólya [53] introduced the concept of integer-valued polynomials. Pólya [53] sought to generalize his observation that the binomial polynomials form a regular basis of $\mathrm{Int}(\mathbb{Z})$ as a $\mathbb{Z}$-module. He considered integer-valued polynomials on the rings of integers, $\mathcal{O}_K$, of a number field $K$ and showed that $\mathrm{Int}(\mathcal{O}_K)$ has a regular basis whenever $K$ has class number 1. Ostrowski [51] further investigated regular bases in $\mathrm{Int}(\mathcal{O}_K)$ motivated by the questions Pólya [53] raised. Pólya and Ostrowski's papers, [53] and [51], are considered as the starting point of the theory of integer-valued polynomials.

Today the theory of integer-valued polynomials is an independent branch of algebra. We refer to the monograph by Cahen and Chabert [18] for a deeper study of integer-valued polynomials. For a specific study of $\mathrm{Int}(\mathbb{Z})$, see [19]. Note that there are now several generalizations of Int($D$), for instance, integer-valued polynomials on subsets, cf. [16, 20] and [18, Chapter IV], integer-valued polynomials on algebras, cf. [30, 59], and integer-valued polynomials in several indeterminates, cf. [18, Chapter XI]. However, in this thesis, we restrict ourselves to Int($D$).

The ring Int($D$) is known to provide friendly counter examples, for instance, Int($\mathbb{Z}$) is a natural example of a non-Noetherian ring. More generally, if $D$ is Noetherian and one dimensional or if $D$ is Noetherian and integrally closed, then Int($D$) is Noetherian if and only if Int$(D) = D[x]$, cf. [18, Corollary VI.2.6]. Recall that in our case $D$ is Dedekind, therefore our rings Int$(D) \neq D[x]$ in the subsequent chapters, are not Noetherian. However, our focus is on the failure of uniqueness of factorization of elements in our rings Int($D$). In fact, let us review factorization theory in Int($D$) for an arbitrary domain $D$.

The study of the factorization properties of Int($D$) begun in [17] and since then several researchers have investigated factorizations in Int($D$), see for example [11] [12], [25], [29], [32] and [52]. The monograph by Cahen and Chabert [18] summarised the early work on the factorization properties of Int($D$) and the properties we mention without reference can be found there in Chapter VI. Let us review some of these properties. First recall that $D \subsetneq D[x] \subseteq \text{Int}(D) \subseteq K[x]$. Furthermore, the units of Int($D$) are the units of $D$, and an element of $D$ is irreducible in Int($D$) if and only if it is irreducible in $D$. It then follows that if $D$ is not a unique factorization domain (not an atomic domain), then Int($D$) is also not a unique factorization domain (not an atomic domain). However, if $D$ is a unique factorization domain (an atomic domain), Int($D$) is not necessarily a unique factorization domain (an atomic domain). For instance, it is well known that Int($\mathbb{Z}$) is not a unique factorization domain. For atomicity, using Rotman's characterization [55, Proposition 1.1], one can construct an atomic domain $D$ such that Int$(D) = D[x]$ is not atomic. Although the atomicity of $D$ does not imply that of Int($D$), the ring Int($D$) satisfies the ascending chain condition on principal ideals (in short ACCP) if and only if $D$ satisfies ACCP. Therefore, if $D$ satisfies ACCP, then Int($D$) is atomic.

Several objects of non-unique factorizations have been studied in Int($D$). Cahen and Chabert [17, 18] studied elasticity in Int($D$) and showed that Int($D$) has infinite elasticity whenever $D$ is a one dimensional Noetherian domain with finite residue fields. To date there is no known example of a ring Int$(D) \neq D[x]$ with finite elasticity. They further showed that if $D$ is an infinite domain, then Int($D$) is a BFD if and only if $D$ is a BFD. This was first shown by D. Anderson, F. Anderson, and Zafrullah [5]. Note that in the subsequent chapters, $D$ is a Dedekind domain with finite residue fields. This implies that in our case, Int($D$) is atomic, a BFD (since $D$ is a BFD, see [3]), and has infinite elasticity. Furthermore, Frisch [29] showed that Int($\mathbb{Z}$) is a finite factorization domain.

Like earlier mentioned, sets of lengths is an important object of study in factorization theory. However, sets of lengths had not been studied in Int($D$). It is only recently that Frisch [29] studied sets of lengths in Int($\mathbb{Z}$) and this described the factorization behavior of Int($\mathbb{Z}$). In particular, Frisch [29] showed that every finite set of natural numbers not containing 1 occurs as the set of lengths of a polynomial in Int($\mathbb{Z}$). Similar results concerning sets of lengths have been obtained using transfer homomorphisms to block monoids, see for example [44]. Frisch [29] also showed that there is no transfer homomorphism to a block monoid from the multiplicative monoid of Int($\mathbb{Z}$). This added Int($\mathbb{Z}$) to the small list of naturally occurring rings whose multiplicative monoids do not admit transfer homomorphisms to block monoids cf. [28, 37, 38]. These results in [29] motivated our work in Chapter 2. Together with Sophie Frisch and Roswitha Rissner, we showed that every finite set of natural numbers not containing 1 occurs as the set of lengths of a polynomial in Int($D$), where $D$ is a Dedekind domain with infinitely many maximal ideals, all of finite index. We further showed that there is no transfer homomorphism to a block monoid from the multiplicative monoid of Int($D$).

To fully understand the factorization behaviour of rings with non-unique factorizations, it is important to identify the irreducible elements. Several researchers have indeed investigated the irreducible elements of Int($D$), see for example [12, 17, 25, 52]. In fact, Chapman and McClain's [25] characterization of the irreducible elements of Int($D$) where $D$ is a unique factorization domain, was instrumental in studying the sets of lengths in Int($\mathbb{Z}$). Recently, together with Antoniou and Rissner [12], we obtained a computational characterization of the irreducible elements of Int($\mathbb{Z}$) and this was crucial for the kickoff of the work in Chapter 3. Note that our computational characterization in [12] was motivated by Peruginelli's [52] algorithmic irreducibility criterion.

The factorization behaviour of Int($\mathbb{Z}$) is now fully understood in the case of square-free factorizations. However, for the non square-free factorizations, nothing is known. This is because all the investigations on the irreducible elements of Int($D$) have been on general irreducible elements. There are certain irreducible elements some of whose powers allow several essentially different factorizations into irreducibles. These are called *non-absolutely irreducibles* and their counterparts are called absolutely irreducible. That is, an irreducible element $r$ is called *absolutely irreducible* if for all natural numbers $n > 1$, each power of $r$, $r^n$, has essentially only one factorization, namely $r^n = r \cdots r$. The absolutely irreducible elements have also been called strong atoms and completely irreducible.

Several researchers have investigated absolutely irreducible elements especially in the ring $\mathcal{O}_K$ of integers in a number field $K$, see for instance [13, 24, 36, 43]. Kaczorowski studied the absolutely irreducible elements of $\mathcal{O}_K$ so as to characterize the number fields with cyclic class group, cf [43]. Actually, the concept of absolutely irreducible elements first appeared in his paper [43] in which he called these completely irreducible. Recently, Chapman and Krause [24] showed that $\mathcal{O}_K$ is a unique factorization domain if and only if every irreducible element is absolutely irreducible. The study of the absolutely irreducible and non-absolutely irreducible elements of $\mathrm{Int}(D)$ has started with the work in Chapters 3 and 4. Now since every prime element is absolutely irreducible, it follows that $\mathcal{O}_K$ contains absolutely irreducible elements even when it is a non-unique factorization domain. Similarly, our non-unique factorization domains $\mathrm{Int}(D)$ in Chapters 3 and 4 have both absolutely irreducible elements (because of unique factorization in $K[x]$) and non-absolutely irreducible elements.

Like earlier mentioned, the researchers who have studied factorizations in $\mathrm{Int}(D)$ have mostly been considering square-free factorizations. For instance, the factorizations used to realize the main results on sets of lengths in [29] and [32] were all square-free. It is not known whether $\mathrm{Int}(D)$ in those cases exhibits similar behavior for non-square-free factorizations. More generally, nothing is known about patterns of factorizations in $\mathrm{Int}(D)$. This was the motivation for the work in Chapters 3 and 4.

In Chapter 3, we construct non-absolutely irreducible elements in $\mathrm{Int}(\mathbb{Z})$, and give generalizations of these constructions. In Chapter 4, we give a graph-theoretic sufficient condition for a polynomial $f \in \mathrm{Int}(D)$ to be absolutely irreducible, when $D$ is a principal ideal domain. Furthermore, we show that our criterion is necessary and sufficient in the special case of polynomials in $\mathrm{Int}(D)$ with square-free denominator. The work in both Chapters 3 and 4 serve as a cornerstone for studying patterns of factorizations in $\mathrm{Int}(D)$. Furthermore, they lay a foundation for a complete characterization of the absolutely irreducible elements of $\mathrm{Int}(\mathbb{Z})$.

Next is Chapter 2 in which we study sets of lengths in $\mathrm{Int}(D)$, when $D$ is a

Dedekind domain with infinitely many maximal ideals, all of finite index. In particular, we show that every finite set of natural numbers not containing 1 occurs as the set of lengths of a polynomial in $\mathrm{Int}(D)$, cf. Theorem 2.4.1. We also show that there is no transfer homomorphism to a block monoid from the multiplicative monoid of $\mathrm{Int}(D)$, cf. Theorem 2.5.1.

For completeness, we define the notions of a block monoid, transfer homomorphism and related terms in Appendix A, immediately after Chapter 4. The Appendix also contains results from [36] that we refer to in Section 2.5 of Chapter 2.

# 2. Sets of lengths of factorizations of integer-valued polynomials on Dedekind domains with finite residue fields

This chapter consists of article [32] titled, "Sets of lengths of factorizations of integer-valued polynomials on Dedekind domains with finite residue fields". The article appeared in the *Journal of Algebra* in June 2019 and it is joint work with Sophie Frisch and Roswitha Rissner. The factorization terms in Section 2.5 originally referred to [36], can be found in Appendix A.


## Abstract

Let $D$ be a Dedekind domain with infinitely many maximal ideals, all of finite index, and $K$ its quotient field. Let $\mathrm{Int}(D) = \{f \in K[x] \mid f(D) \subseteq D\}$ be the ring of integer-valued polynomials on $D$. Given any finite multiset $\{k_1, \ldots, k_n\}$ of integers greater than 1, we construct a polynomial in $\mathrm{Int}(D)$ which has exactly $n$ essentially different factorizations into irreducibles in $\mathrm{Int}(D)$, the lengths of these factorizations being $k_1, \ldots, k_n$. We also show that there is no transfer homomorphism from the multiplicative monoid of $\mathrm{Int}(D)$ to a block monoid.



**Keywords:** Factorizations, sets of lengths, integer-valued polynomials, Dedekind domains, block monoid, transfer homomorphism, Krull monoid

**2010 Mathematics Subject Classification:** 13A05, 13B25, 13F20, 11R04, 11C08


## 2.1. Introduction

By factorization we mean an expression of an element of a ring as a product of irreducible elements. Until not so long ago, the fact that such a factorization, if it exists, need not be unique, was seen as a pathology. When mathematicians were shocked to find that uniqueness of factorization does not hold in rings of integers in number fields, they did not immediately study the details of this non-uniqueness, but moved on to unique factorization of ideals into prime ideals. Non-uniqueness of factorization was avoided, whenever possible.

Only in the last few decades, some mathematicians, notably Geroldinger and Halter-Koch [36], came around to the view that the precise details of non-uniqueness of factorization actually are a fascinating topic: the underlying phenomena give a lot of information about the arithmetic of a ring.

One important object of study is the set of lengths of factorizations of a fixed element, cf. [34]. The length of a factorization is the number of irreducible factors, and the set of lengths of an element is the set of all natural numbers that occur as lengths of factorizations of the element. Geroldinger and Halter-Koch [36] found that the sets of lengths of algebraic integers exhibit a certain structure.

In stark contrast to this, we show in Section 2.4 that every finite set of natural numbers not containing 1 occurs as the set of lengths of a polynomial 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 Dedekind domain with infinitely many maximal ideals, all of them of finite index, and $K$ denotes the quotient field of $D$. The special case of $D = \mathbb{Z}$ has been shown by Frisch [29].

The study of non-uniqueness of factorization has mostly concentrated on Krull monoids so far. Krull monoids are characterized by having a "divisor theory". The multiplicative monoid $D \setminus \{0\}$ of an integral domain $D$ is Krull exactly if $D$ is a Krull ring, cf. [36].

The rings $\mathrm{Int}(D)$ for which we study non-uniqueness of factorization are not Krull, but Prüfer, cf. [21, 45]. All factorizations of a single polynomial in $\mathrm{Int}(D)$, however, take place in a Krull monoid, namely, in the divisor-closed submonoid of $\mathrm{Int}(D)$ generated by $f$.

Following Reinhart [54], we call this monoid, consisting of all divisors in $\mathrm{Int}(D)$ of all powers of $f$, the *monadic submonoid generated by* $f$. That all monadic submonoids of $\mathrm{Int}(D)$ are Krull was shown by Reinhart [54] in the case where $D$ is a unique factorization domain, and, by a different method, by Frisch [33] in the case where $D$ is a Krull ring. Thus, our Theorem 2.4.1, concerning non-unique factorization in the Prüfer ring $\mathrm{Int}(D)$, also serves to show that quite wild factorization behavior is possible in Krull monoids.

Among Krull monoids, the best studied ones are multiplicative monoids of rings of algebraic integers. We should keep in mind, however, that the multiplicative monoids of rings of algebraic integers are very special, in that unique factorization of ideals always lurks in the background. In technical terms this means that there is a transfer homomorphism to a block monoid.

In Section 2.5, we show that there is no transfer homomorphism to a block monoid from the multiplicative monoid of $\mathrm{Int}(D)$. This is relevant for two reasons: Firstly, because the rings of whose multiplicative monoid it is known that it does not admit such a transfer homomorphism are few and far between, see [28, 37, 38]; and secondly, because most, if not all, results so far concerning arbitrary finite sets occurring as sets of lengths have been obtained using transfer homomorphisms to block monoids [44].

Our main results are in Sections 2.4 and 2.5; in Section 2.2 we introduce the necessary notation and Section 2.3 contains some useful lemmas.

## 2.2. Preliminaries

We start with a short review of some elementary facts on factorizations, Dedekind domains and integer-valued polynomials, and introduce some notation.

### Factorizations

We define here only the notions that we need throughout this paper, and refer to the monograph by Geroldinger and Halter-Koch [36] for a systematic introduction to non-unique factorizations.

Let $R$ be a commutative ring with identity and $r,\ s \in R$.

(i) If $r$ is a non-zero non-unit, we say $r$ is *irreducible* in $R$ if it cannot be written as the product of two non-units of $R$.

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

$$r = a_1 \cdots a_n \tag{2.2.1}$$

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

(iii) The number $n$ of irreducible factors is called the *length* of the factorization in (2.2.1).

(iv) The *set of lengths* of $r$ is the set of all natural numbers $n$ such that $r$ has a factorization of length $n$.

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

(vi) Two factorizations of the same element,

$$r = a_1 \cdots a_n = b_1 \cdots b_m, \tag{2.2.2}$$

are called *essentially the same* if $n = m$ and, after reindexing, $a_j \sim b_j$ for $1 \leq j \leq m$. If this is not the case, the factorizations in (2.2.2) are called *essentially different*.

## Dedekind domains

Recall that an integral domain $D$ is a *Dedekind domain* if and only if every non-zero ideal is a product of prime ideals. This is equivalent to every non-zero ideal being invertible. It is also equivalent to $D$ being a Noetherian domain such that the localization at every non-zero maximal ideal is a discrete valuation domain. And it is further equivalent to the following list of properties

(i) $D$ is Noetherian

(ii) $D$ is integrally closed

(iii) $\dim(D) \leq 1$

From now on, we only consider Dedekind domains that are not fields. For a Dedekind domain $D$ with quotient field $K$, let max-spec$(D)$ denote the set of maximal ideals of $D$. Every prime ideal $P \in$ max-spec$(D)$ defines a discrete valuation $\mathsf{v}_P$ by $\mathsf{v}_P(a) = \max\{n \in \mathbb{Z} \mid a \in P^n\}$ for $a \in K \setminus \{0\}$. $\mathsf{v}_P$ is called the *$P$-adic valuation* on $K$.

For a non-zero ideal $I$ of $D$, let $\mathsf{v}_P(I) = \min\{\mathsf{v}_P(a) \mid a \in I\}$. This is compatible with the definition of $\mathsf{v}_P(a)$ for $a \in K \setminus \{0\}$, in the sense that $\mathsf{v}_P(aD) = \mathsf{v}_P(a)$. With this notation, the factorization of $I$ into prime ideals is

$$I = \prod_{P \in \text{max-spec}(D)} P^{\mathsf{v}_P(I)} \tag{2.2.3}$$

Note that $\mathsf{v}_P(I) > 0$ is equivalent to $I \subseteq P$. There are only finitely many prime overideals of $I$ in $D$ and hence the product in Equation (2.2.3) is finite.

For two ideals $I$ and $J$ of $D$, $I \subseteq J$ is equivalent to $\mathsf{v}_P(J) \leq \mathsf{v}_P(I)$ for all $P \in$ max-spec($D$). Note that $I \subseteq J$ is equivalent to the fact that there exists an ideal $L$ of $D$ such that $JL = I$, in which case we say that $J$ divides $I$ and write $J \mid I$. This last equivalence is often summarized as "to contain is to divide."

For a thorough introduction to Dedekind domains, we refer to Bourbaki [15, Ch. VII, § 2].

## Dedekind domains with finite residue fields

Let $D$ be a Dedekind domain. For a maximal ideal $P$ with finite residue field we write $\|P\|$ for $|D/P|$ and call this number the *index of* $P$. In what follows we will only consider Dedekind rings with infinitely many maximal ideals, all of whose residue fields are finite. We will frequently use the fact that there are only finitely many maximal ideals of each individual finite index. This holds in every Noetherian domain, as Samuel [57] has shown; see also Gilmer [39].

We include a short proof by F. Halter-Koch for the special case of Dedekind domains.

**Proposition 2.2.1.** *[Samuel [57], Gilmer [39]] Let $D$ be a Dedekind domain. Then for each given $q \in \mathbb{N}$, there are at most finitely many maximal ideals $P$ of $D$ with $\|P\| = q$.*

**Proof (Halter-Koch, personal communication).** Suppose that for some $q \geq 2$ there exist infinitely many prime ideals of index $q$, and let $0 \neq a \in D$. Then there exist infinitely many prime ideals $P$ of $D$ such that $\|P\| = q$ and $a \notin P$. For each such prime ideal $P$ we obtain $a^{q-1} \equiv 1 \mod P$, hence $a^{q-1} - 1 \in P$ and thus $a^{q-1} = 1$. So, every non-zero element of $D$ is a $(q-1)$-st root of unity. Impossible! $\square$

## Integer-valued polynomials

If $D$ is a domain with quotient field $K$, the *ring of integer-valued polynomials* on $D$ is defined as

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

Every non-zero $f \in K[x]$ can be written as a quotient $f = \frac{g}{b}$ where $g \in D[x]$ and $b \in D \setminus \{0\}$. Clearly, $f = \frac{g}{b}$ is an element of $\mathrm{Int}(D)$ if and only if $b \mid g(a)$ for all $a \in D$.

**Definition 2.2.2.** Let $D$ be a domain and $g \in \mathrm{Int}(D)$. The *fixed divisor* of $g$ is the ideal $\mathsf{d}(g)$ of $D$ generated by the elements $g(a)$ with $a \in D$:

$$\mathsf{d}(g) = (g(a) \mid a \in D)$$

We say that $g$ is *image primitive* if $\mathsf{d}(g) = D$. By abuse of notation, this is also denoted $\mathsf{d}(g) = 1$.

**Remark 2.2.3.** Let $D$ be a domain and $K$ its quotient field.

(i) If $g \in D[x]$ and $b \in D \setminus \{0\}$, then $\frac{g}{b}$ is an element of $\mathrm{Int}(D)$ if and only if $\mathsf{d}(g) \subseteq bD$.

(ii) If $g \in D[x]$ and $P$ a prime ideal of $D$ such that $\mathsf{d}(g) \subseteq P$ then $g \in P[x]$ or $[D : P] \leq \deg(g)$.

(iii) If $f, g \in \mathrm{Int}(D)$, then $\mathsf{d}(fg) \subseteq \mathsf{d}(f)\mathsf{d}(g)$.

(iv) If $g \in D[x]$ is irreducible in $K[x]$, then every factorization of $g$ in $\mathrm{Int}(D)$ as a product of two (not necessarily irreducible) elements is of the form $c\frac{g}{c}$ with $c \in D$ and $\mathsf{d}(g) \subseteq cD$.

(v) If $g \in D[x]$ is irreducible in $K[x]$ and $\mathsf{d}(g) = D$, then $g$ is irreducible in $\mathrm{Int}(D)$.

For a general introduction to integer-valued polynomials we refer to the monograph by Cahen and Chabert [18] and to their more recent survey paper [19].

## 2.3. Auxiliary results

In this section we develop tools to construct, first, split polynomials in $D[x]$ with prescribed fixed divisor (Lemma 2.3.2), then, irreducible polynomials in $D[x]$ with prescribed fixed divisor (Lemma 2.3.3), and, finally, polynomials of a special form whose essentially different factorizations in $\mathrm{Int}(D)$ we have complete control over (Lemma 2.3.8).

**Remark 2.3.1.** In the following, we want to consider the multiplicity of roots of polynomials. For this purpose, we introduce some notation for multisets. Let $m_S(a)$ denote the multiplicity of an element $a$ in a multiset $S$ (with $m_S(a) = 0$ if $a \notin S$). For multisets $S$ and $T$, let $S \uplus T$ denote the collection of elements $a$ in the union of the sets underlying $S$ and $T$ with multiplicities $m_{S \uplus T}(a) = m_S(a) + m_T(a)$ (the disjoint union of $S$ and $T$). Note that $|S \uplus T| = |S| + |T|$.

**Lemma 2.3.2.** *Let $D$ be a domain, $\mathcal{T} \subseteq D$ a finite multiset and $f = \prod_{r\in\mathcal{T}}(x-r)$. If $Q$ is a non-zero prime ideal of $D$, then $\mathsf{d}(f) \subseteq Q$ if and only if $\mathcal{T}$ contains a complete system of residues modulo $Q$.*

*Furthermore, if $D$ is a Dedekind domain and $\mathcal{T} = \mathcal{T}_0 \uplus \biguplus_{i=1}^{e} \mathcal{T}_i$ such that:*

*(i) For all $1 \leq i \leq e$, $\mathcal{T}_i$ is a complete system of residues modulo $Q$ and the respective representatives of the same residue class in each $\mathcal{T}_i$ are congruent modulo $Q^2$,*

*(ii) There exists $z \in D$ such that for all $s \in \mathcal{T}_0$, $s \not\equiv z \mod Q$,*

*then $\mathsf{v}_Q(\mathsf{d}(f)) = e$.*

**Proof.** If $\mathcal{T}$ does not contain a complete system of residues modulo $Q$, then there exists an element $a \in D$ such that $a \not\equiv r \mod Q$ for all $r \in \mathcal{T}$. This implies $f(a) = \prod_{r\in\mathcal{T}}(a-r) \notin Q$, hence $\mathsf{d}(f) \nsubseteq Q$.

Conversely, if $\mathcal{T}$ contains a complete system of residues modulo $Q$ then, for all $a \in D$, there exists $r \in \mathcal{T}$ such that $a \equiv r \mod Q$. This implies $f(a) = \prod_{r\in\mathcal{T}}(a-r) \in Q$ for all $a \in D$ and hence $\mathsf{d}(f) \subseteq Q$.

Now assume that $D$ is a Dedekind domain and $\mathcal{T} = \biguplus_{i=1}^{e} \mathcal{T}_i \uplus \mathcal{T}_0$ such that (i) and (ii) hold. If $f_i = \prod_{r\in\mathcal{T}_i}(x-r)$ for $1 \leq i \leq e$ and $g = \prod_{s\in\mathcal{T}_0}(x-s)$, then $f = \left(\prod_{i=1}^{e} f_i\right) g$. Since $\mathcal{T}_i$ is a complete system of residues modulo $Q$, it follows that $\mathsf{v}_Q(f_i(a)) \geq 1$ for all $a \in D$. Therefore, for all $a \in D$,

$$\mathsf{v}_Q(f(a)) = \sum_{i=1}^{e} \mathsf{v}_Q(f_i(a)) + \mathsf{v}_Q(g(a)) \geq e \tag{2.3.1}$$

For $1 \leq i \leq e$, let $a_i \in \mathcal{T}_i$ with $a_i \equiv z \mod Q$. Since the elements $a_i$ are in the same residue class modulo $Q^2$, there exists $d \in D$ in the same residue class modulo $Q$ as $z$ and all the $a_i$, but in a different residue class modulo $Q^2$ from all the $a_i$.

For such a $d$, then $\mathsf{v}_Q(f_i(d)) = 1$ for all $1 \leq i \leq e$ and $\mathsf{v}_Q(g(d)) = 0$, since for all $s \in \mathcal{T}_0$, $s \not\equiv z \equiv d \mod Q$. Therefore

$$\mathsf{v}_Q(f(d)) = \sum_{i=1}^{e} \mathsf{v}_Q(f_i(d)) + \mathsf{v}_Q(g(d)) = e$$

which implies that $\mathsf{v}_Q(\mathsf{d}(f)) = e$. □

Next, we need to discuss how to replace split monic polynomials in $D[x]$ by monic polynomials in $D[x]$ which are irreducible in $K[x]$, without changing the fixed divisors.

**Lemma 2.3.3.** *Let $D$ be a Dedekind domain with infinitely many maximal ideals and $K$ its quotient field. Let $I \neq \emptyset$ be a finite set and $f_i \in D[x]$ be monic polynomials for $i \in I$.*

*Then, there exist monic polynomials $F_i \in D[x]$ for $i \in I$, such that*

*(i)* $\deg(F_i) = \deg(f_i)$ *for all $i \in I$,*

*(ii) the polynomials $F_i$ are irreducible in $K[x]$ and pairwise non-associated in $K[x]$ and*

*(iii) for all subsets $J \subseteq I$ and all partitions $J = J_1 \uplus J_2$,*

$$\mathsf{d}\left(\prod_{j\in J_1} f_j \prod_{j\in J_2} F_j\right) = \mathsf{d}\left(\prod_{j\in J} f_j\right).$$

**Proof.** Let $P_1, \ldots, P_n$ be all maximal ideals $P$ of $D$ with $\|P\| \leq \deg\left(\prod_{i\in I} f_i\right)$. Suppose the prime factorization of the fixed divisor of the product of the $f_i$ is

$$\mathsf{d}\left(\prod_{i\in I} f_i\right) = \prod_{j=1}^{n} P_j^{e_j}.$$

Let $Q \in \text{max-spec}(D) \setminus \{P_1, \ldots, P_n\}$. Using the Chinese Remainder Theorem, we add elements to the coefficients of the $f_i$ such that the resulting polynomials can be seen to be irreducible according to Eisenstein's irreducibility criterion with respect to $Q$, while retaining all relevant properties with respect to sufficiently high powers of the $P_i$.

Let $f_{ik}$ denote the coefficient of $x^k$ in $f_i$. For $i \in I$ and $0 \leq k < \deg(f_i)$, let $g_{ik} \in D$ such that

(i) $g_{ik} \in \prod_{j=1}^{n} P_j^{e_j+1}$ for all $0 \leq k < \deg(f_i)$.

(ii) $g_{ik} \equiv -f_{ik} \mod Q$ for all $0 \leq k < \deg(f_i)$ and

(iii) $g_{i0} \not\equiv -f_{i0} \mod Q^2$.

Since the $g_{ik}$ satisfying the above conditions are only determined modulo $Q^2 \prod_{i=1}^{n} P_i^{e_i+1}$, there are infinitely many choices for each $g_{ik}$. We use this flexibility to implement that $g_{i0} + f_{i0} \neq g_{j0} + f_{j0}$ for $i \neq j$. Then, for $i \in I$, we set

$$F_i = f_i + \sum_{k=0}^{\deg(f_i)-1} g_{ik} x^k.$$

As the resulting $F_i$ are monic and distinct, they are pairwise non-associated in $K[x]$.

According to Eisenstein's irreducibility criterion, the polynomials $F_i$ are irreducible in $D[x]$ for $i \in I$, cf. [46, §29, Lemma 1]. Since the $F_i$ are monic and $D$ is integrally closed, it follows that the $F_i$ are irreducible in $K[x]$ for all $i \in I$, cf. [15, Ch. 5, §1.3, Prop. 11].

By construction,

$$F_i \equiv f_i \mod \left(\prod_{j=1}^{n} P_j^{e_j+1}\right) D[x]$$

for all $i \in I$. Now, if $g(x)$ is the product of any selection of the polynomials $f_i$, and $G(x)$ the modified product in which some of the $f_i$ have been replaced by $F_i$, then $g(x)$ is congruent to $G(x)$ modulo $\left(\prod_{j=1}^{n} P_j^{e_j+1}\right) D[x]$.

Hence, for all $a \in D$, $g(a) \equiv G(a)$ modulo $\left(\prod_{j=1}^{n} P_j^{e_j+1}\right)$ and, therefore,

$$\min_{a\in D} \mathsf{v}_P(G(a)) = \min_{a\in D} \mathsf{v}_P(g(a))$$

for all $P$ that could conceivably divide the fixed divisor of $G(x)$ or $g(x)$ by Remark 2.2.3.(ii). This implies the last assertion of the Lemma, to the effect that substituting $F_i$ for some or all of the $f_i$ does not change the fixed divisor of a product. $\square$

Finally, the last two lemmas enable us to understand all essentially different factorizations of a certain type of polynomials in $\operatorname{Int}(D)$.

**Lemma 2.3.4.** *Let $D$ be a Dedekind domain with quotient field $K$ and $f \in \operatorname{Int}(D)$ of the following form:*

$$f = \frac{\prod_{i\in I} f_i}{c} \quad with \quad \mathsf{d}\left(\prod_{i\in I} f_i\right) = cD,$$

*where $c$ is a non-unit of $D$ and for each $i \in I$, $f_i \in D[x]$ is irreducible in $K[x]$.*

*Let $\mathcal{P} \subseteq \operatorname{max-spec}(D)$ be the finite set of prime ideal divisors of $cD$. If $f = g_1 \cdots g_m$ is a factorization of $f$ into (not necessarily irreducible) non-units in $\operatorname{Int}(D)$ then each $g_j$ is of the form*

$$g_j = a_j \prod_{i\in I_j} f_i,$$

*where $\emptyset \neq I_j \subseteq I$ and $a_j \in K$, such that $I_1 \uplus \ldots \uplus I_m = I$, $a_1 \cdots a_m = c^{-1}$ and*

(i) *$\mathsf{v}_P(a_j) \leq 0$ for all $P \in \operatorname{max-spec}(D)$ and all $1 \leq j \leq m$; and* *(ii)* $\mathsf{v}_P(a_j)=0$ *for all* $P\in\text{max-spec}(D)\setminus\mathcal{P}$ *and all* $1\leq j\leq m$.

**Proof.** Let $f = g_1\cdots g_m$ be a factorization of $f$ into (not necessarily irreducible) non-units in $\text{Int}(D)$. Since $\mathsf{d}(f)=1$, no $g_i$ is a constant, by Remark 2.2.3.(iv). Each factor $g_j$ is, therefore, of the form

$$g_j = a_j\prod_{i\in I_j} f_i \tag{2.3.2}$$

where $I_j$ is a non-empty subset of $I$ and $a_j\in K$, such that $I_1\uplus\ldots\uplus I_m = I$ and $a_1\cdots a_m = c^{-1}$. Note that for all $P\in\text{max-spec}(D)$

$$\sum_{j=1}^{m}\mathsf{v}_P(a_j)=-\mathsf{v}_P(c). \tag{2.3.3}$$

Suppose $\mathsf{v}_P(a_t) > 0$ for some maximal ideal $P$ and some $1\leq t\leq m$. Then $\sum_{j\neq t}\mathsf{v}_P(a_j)<-\mathsf{v}_P(c)$.

Remark 2.2.3.(iii) and the fact that $\mathsf{v}_P\left(\mathsf{d}\left(\prod_{i\in I}f_i\right)\right) = \mathsf{v}_P(c)$ imply $\mathsf{v}_P\left(\mathsf{d}\left(\prod_{j\neq t}\prod_{i\in I_j}f_i\right)\right)\leq\mathsf{v}_P(c)$. But now

$$\mathsf{v}_P\left(\mathsf{d}\left(\prod_{j\neq t}g_j\right)\right)=\mathsf{v}_P\left(\mathsf{d}\left(\prod_{j\neq t}\prod_{i\in I_j}f_i\right)\right)+\sum_{j\neq t}\mathsf{v}_P(a_j)<0,$$

which means that

$$\prod_{j\neq t}g_j\notin\text{Int}(D),$$

a contradiction. We have established that $\mathsf{v}_P(a_j)\leq 0$ for all $P\in\text{max-spec}(D)$ and all $1\leq j\leq m$. Now Equation (2.3.3) and the fact that $\mathsf{v}_P(c)=0$ for all $P\notin\mathcal{P}$ imply $\mathsf{v}_P(a_j)=0$ for all $P\notin\mathcal{P}$ and all $1\leq j\leq m$. □

**Definition 2.3.5.** Let $D$ be a Dedekind domain, $f_i\in D[x]$ with $i\in I$ for a finite set $I\neq\emptyset$ and $\mathcal{P}\subseteq\text{max-spec}(D)$ be the finite set of prime ideal divisors of $\mathsf{d}\left(\prod_{i\in I}f_i\right)$. If $P\in\mathcal{P}$, we say $f_k$ is *indispensable for* $P$ (among the polynomials $f_i$ with $i\in I$) if for all $J\subseteq I$

$$\mathsf{v}_P\left(\mathsf{d}\left(\prod_{i\in J}f_i\right)\right)>0\Longrightarrow k\in J.$$

**Remark 2.3.6.** Note that (with the notation of Definition 2.3.5) $f_k$ is indispensable for $P\in\mathcal{P}$ (among the polynomials $f_i$ with $i\in I$) if and only if there exists an element $z\in D$ such that $\mathsf{v}_P(f_k(z))>0$ and $\mathsf{v}_P(f_i(z))=0$ for all $i\neq k$.

**Remark 2.3.7.** For a finite set $I \neq \emptyset$, let $f_i$ and $F_i \in D[x]$ with $i \in I$ such that for all $J \subseteq I$ and all partitions $J = J_1 \uplus J_2$

$$\mathsf{d}\left(\prod_{j\in J_1} f_i \prod_{j\in J_2} F_j\right) = \mathsf{d}\left(\prod_{j\in J} f_i\right).$$

It follows that $\mathsf{d}\left(\prod_{i\in I} f_i\right) = \mathsf{d}\left(\prod_{i\in I} F_i\right)$ which implies that the fixed divisor of $\prod_{i\in I} f_i$ and $\prod_{i\in I} F_i$ have the same set $\mathcal{P}$ of prime ideal divisors. Moreover, for all $P \in \mathcal{P}$ and all $J \subseteq I$, it follows that $\mathsf{v}_P\left(\mathsf{d}\left(\prod_{i\in J} F_i\right)\right) = \mathsf{v}_P\left(\mathsf{d}\left(\prod_{i\in J} f_i\right)\right)$. Hence, for $P \in \mathcal{P}$, $f_k$ is indispensable for $P$ (among the polynomials $f_i$ with $i \in I$) if and only if $F_k$ is indispensable for $P$ (among the polynomials $F_i$ with $i \in I$). Note that this applies in particular in the setting of Lemma 2.3.3.

**Lemma 2.3.8.** *Let $D$ be a Dedekind domain with quotient field $K$ and $f \in \mathrm{Int}(D)$ of the following form:*

$$f = \frac{\prod_{i\in I} f_i}{c} \quad with \quad \mathsf{d}\left(\prod_{i\in I} f_i\right) = cD,$$

*where $c$ is a non-unit of $D$ and for each $i \in I$, $f_i \in D[x]$ is irreducible in $K[x]$. Let $\mathcal{P} \subseteq \text{max-spec}(D)$ be the finite set of prime ideal divisors of $cD$.*

*Suppose, for each $P \in \mathcal{P}$, $\Lambda_P$ is a subset of $I$ such that $f_i$ is indispensable for $P$ for each $i \in \Lambda_P$. Let $\Lambda = \bigcup_{P\in\mathcal{P}} \Lambda_P$.*

*If $\bigcap_{P\in\mathcal{P}} \Lambda_P \neq \emptyset$, then all essentially different factorizations of $f$ into irreducibles in* $\mathrm{Int}(D)$ *are given by:*

$$\frac{\left(\prod_{i\in\Lambda\cup J_1} f_i\right)}{c} \cdot \prod_{j\in J_2} f_j$$

*(each $f_j$ with $j \in J_2$ counted as an individual factor), where $I = \Lambda \uplus J_1 \uplus J_2$ such that $J_1$ is minimal with $\mathsf{d}\left(\prod_{i\in\Lambda\cup J_1} f_i\right) = cD$.*

**Proof.** Let $f = g_1 \cdots g_m$ be a factorization of $f$ into (not necessarily irreducible) non-units in $\mathrm{Int}(D)$. As in Lemma 2.3.4,

$$g_j = a_j \prod_{i\in I_j} f_i \tag{2.3.4}$$

where $I_j$ is a non-empty subset of $I$ and $a_j \in K$, such that $I_1 \uplus \ldots \uplus I_m = I$ and $a_1 \cdots a_m = c^{-1}$. Furthermore, $\mathsf{v}_P(a_j) \leq 0$ for all $P \in \text{max-spec}(D)$ and all $1 \leq j \leq m$ and $\mathsf{v}_P(a_j) = 0$ for all $P \notin \mathcal{P}$ and all $1 \leq j \leq m$.

We know there exists a polynomial $f_{i_0}$ that is indispensable for all $P \in \mathcal{P}$. We may assume that $i_0 \in I_1$. By the definition of indispensable polynomial, $\mathsf{v}_P\left(\mathsf{d}\left(\prod_{i\in I_j} f_i\right)\right) = 0$, for $2 \le j \le m$ and all $P \in \mathcal{P}$. From this and the fact that $g_j = a_j \prod_{i\in I_j} f_i$ is in $\text{Int}(D)$, we infer that $\mathsf{v}_P(a_j) = 0$ for all $2 \le j \le m$ and all $P \in \mathcal{P}$. We have shown that $a_2, \ldots, a_m$ are units of $D$.

Now $u = a_2 \cdots a_m$ is a unit of $D$ such that $a_1 u = c^{-1}$. Since $g_1 \in \text{Int}(D)$, we must have

$$\mathsf{v}_P\left(\mathsf{d}\left(\prod_{i\in I_1} f_i\right)\right) = \mathsf{v}_P(c) > 0$$

for all $P \in \mathcal{P}$ and, by Definition 2.3.5, $\Lambda \subseteq I_1$.

So far we have shown that every factorization $f = g_1 \cdots g_m$ of $f$ into (not necessarily irreducible) non-units of $\text{Int}(D)$ is – up to reordering of factors and multiplication of factors by units in $D$ – the same as one of the following:

$$\frac{\left(\prod_{i\in\Lambda\cup J_1} f_i\right)}{c} \cdot \left(\prod_{j\in I_2} f_j\right) \cdots \left(\prod_{j\in I_m} f_j\right), \tag{2.3.5}$$

where $I = I_1 \uplus \cdots \uplus I_m$ and $I_1 = \Lambda \uplus J_1$.

It remains to characterize, among the factorizations of the above form, those in which all factors are irreducible in $\text{Int}(D)$.

Since $\mathsf{d}(f) = D$, it is clear that $\mathsf{d}(g_j) = D$ for all $1 \le j \le m$, by Remark 2.2.3.(iii). By the same token, $\mathsf{d}(f_i) = D$ for all $i \in I_j$ with $j \ge 2$. Since the $f_i$ are irreducible in $K[x]$, those of them with fixed divisor $D$ are irreducible in $\text{Int}(D)$, by Remark 2.2.3.(v). The criterion for each factor $g_j = \prod_{i\in I_j} f_i$ with $j \ge 2$ to be irreducible is, therefore, $|I_j| = 1$ for all $j \ge 2$.

Now, concerning the irreducibility of $g_1$, the same arguments that lead to Equation (2.3.5), applied to $g_1 = c^{-1}\left(\prod_{i\in\Lambda\cup J_1} f_i\right)$ instead of $f$, show that $g_1$ is irreducible in $\text{Int}(D)$ if and only if we cannot split off any factors $f_i$ with $i \in J_1$. This is equivalent to $\mathsf{d}\left(\prod_{i\in\Lambda\cup J} f_i\right) \neq cD$ for every proper subset $J \subsetneq J_1$, in other words, to $J_1$ being minimal such that
$\mathsf{d}\left(\prod_{i\in\Lambda\cup J_1} f_i\right) = cD$. In this case we set $J_2 = \bigcup_{j=2}^{m} I_j$ and the assertion follows. □

**Remark 2.3.9.** When $|\mathcal{P}| > 1$, the hypothesis $\bigcap_{P\in\mathcal{P}} \Lambda_P \neq \emptyset$ in Lemma 2.3.8 can be replaced by a weaker condition:

Consider the prime ideals $P \in \mathcal{P}$ as vertices of an undirected graph $G$ and let $(P, Q)$ be an edge of $G$ if and only if there exists a polynomial $f_t$ which is indispensable for both $P$ and $Q$. If $G$ is a connected graph, then the conclusion of Lemma 2.3.8 holds. The proof of Lemma 2.3.8 generalizes readily.

## 2.4. Construction of polynomials with prescribed sets of lengths

We are now ready to prove the main result of this paper.

**Theorem 2.4.1.** *Let $D$ be a Dedekind domain with infinitely many maximal ideals, all of them of finite index. Let $1 \leq m_1 \leq m_2 \leq \cdots \leq m_n$ be natural numbers.*

*Then there exists a polynomial $H \in \mathrm{Int}(D)$ with exactly $n$ essentially different factorizations into irreducible polynomials in $\mathrm{Int}(D)$, the length of these factorizations being $m_1 + 1, \ldots, m_n + 1$.*

**Proof.** If $n = 1$, then $H(x) = x^{m_1+1} \in \mathrm{Int}(D)$ is a polynomial which has exactly one factorization, and this factorization has length $m_1+1$. From now on, assume $n \geq 2$.

First, we construct $H(x)$. Let $N = \left(\sum_{i=1}^{n} m_i\right)^2 - \sum_{i=1}^{n} m_i^2$ and $P$ a prime ideal of $D$ with $\|P\| > N+1$. Let $c \in D$ such that $\mathsf{v}_P(c) = 1$ and $c$ is not contained in any maximal ideal of index 2.

Say the prime factorization of $cD$ is $cD = PQ_1^{e_1} \cdots Q_t^{e_t}$. Let $\tau = (\|P\| - N)$ and $\sigma$ the maximum of the following numbers: $\tau$, and $e_i\|Q_i\|$ for $1 \leq i \leq t$.

We now choose two subsets of $D$: a set $\mathcal{R}$ of order $N$, and $\mathcal{S} = \{s_0, \ldots, s_{\sigma-1}\}$. Using the Chinese Remainder Theorem, we arrange that $\mathcal{R}$ and $\mathcal{S}$ have the following properties:

(i) $s_0 \equiv 0 \mod P$, and $\{s_0, \ldots, s_{\tau-1}\} \cup \mathcal{R}$ is a complete system of residues modulo $P$.

(ii) $s_i \equiv 0 \mod P$ for all $i \geq \tau$.

(iii) For each $Q_i$, $\mathcal{S}$ contains $e_i$ disjoint complete systems of residues, in which the respective representatives of the same residue class in different systems are congruent modulo $Q_i^2$.

(iv) For each $Q_i$, no more than $e_i$ elements of $\mathcal{S}$ are congruent to 1 modulo $Q_i$.

(v) For all $r \in \mathcal{R}$, $r \equiv 0 \mod \bigcap_{i=1}^{t} Q_i$.

(vi) $\mathcal{R} \cup \mathcal{S}$ does not contain a complete system of residues for any prime ideal $Q$ of $D$ other than $P$ and $Q_1, \ldots, Q_t$.

We now assign indices to the elements of $\mathcal{R}$ as follows

$$\mathcal{R} = \{r_{(k,i,h,j)} \mid 1 \le k, h \le n, k \ne h, 1 \le i \le m_k, 1 \le j \le m_h\}.$$

This allows us to visualize the elements of $\mathcal{R}$ as entries in a square matrix $B$ with $m = \sum_{i=1}^{n} m_i$ rows and columns, in which the positions in the blocks of a block-diagonal matrix with block sizes $m_1, \ldots, m_n$ are left empty, see Figure 2.1.

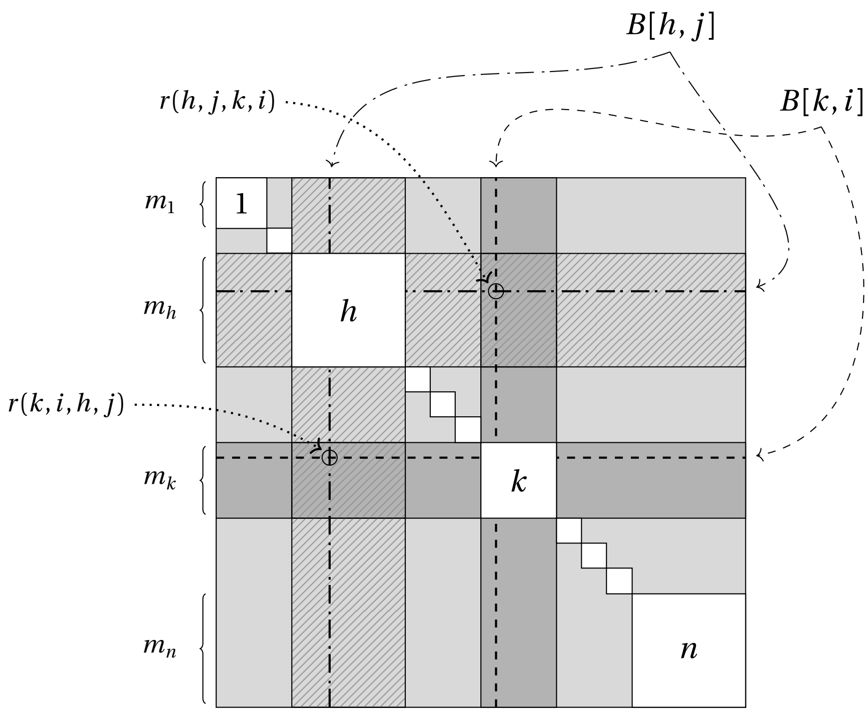


**Figure 2.1:** Say the $k$-th region of $B$ consists of the positions with either column index or row index in the $k$-th block. Then the union of the entries in any $n-1$ different regions covers $\mathcal{R}$. A union of different $B[u,v]$, from which $B[k,i]$ and $B[h,j]$ for two different blocks $k \ne h$ are missing, however, does not cover $\mathcal{R}$, because $r_{(k,i,h,j)}$ and $r_{(h,j,k,i)}$ are not included.

The rows and columns of $B$ are divided into $n$ blocks each, such that the $k$-th block of rows consists of $m_k$ rows, and similarly for columns. Now $r_{(k,i,h,j)}$ designates the entry in row $(k,i)$, that is, in the $i$-th row of the $k$-th block of rows, and in column $(h,j)$, that is, in the $j$-th column of the $h$-th block of columns. Since no element of $\mathcal{R}$ has row and column index in the same block, the positions of a block-diagonal matrix with blocks of sizes $m_1, \ldots, m_n$ are left empty.

For $1 \le k \le n$, let $I_k = \{(k,i) \mid 1 \le i \le m_k\}$ and set

$$I = \bigcup_{k=1}^{n} I_k.$$

Then

$$I = \{(k,i) \mid 1 \le k \le n, 1 \le i \le m_k\}$$

is the set of all possible row indices, or, equivalently, column indices.

For $(k,i) \in I_k$, let $B[k,i]$ be the set of all elements $r \in \mathcal{R}$ which are either in row or in column $(k,i)$ of $B$, that is,

$$B[k,i] = \{r_{(k,i,h,j)} \mid (h,j) \in I \setminus I_k\} \cup \{r_{(h,j,k,i)} \mid (h,j) \in I \setminus I_k\} \tag{2.4.1}$$

In order to construct $H \in \mathrm{Int}(D)$, we set $s(x) = \prod_{i=0}^{\sigma-1}(x - s_i)$ and, for $(k,i) \in I$,

$$f_i^{(k)}(x) = \prod_{r \in B[k,i]} (x - r).$$

Then, let $S(x) \in D[x]$, and, for each $(k,i) \in I$, $F_i^{(k)}(x) \in D[x]$ be monic polynomials such as we know to exist by Lemma 2.3.3: irreducible in $K[x]$, pairwise non-associated in $K[x]$, with $\deg(S) = \deg(s)$ and $\deg(F_i^{(k)}) = \deg(f_i^{(k)})$, and such that, for every selection of polynomials from among $s$ and $f_i^{(k)}$ for $(k,i) \in I$, the product of the polynomials has the same fixed divisor as the modified product in which $s$ has been replaced by $S$ and each $f_i^{(k)}$ by $F_i^{(k)}$. Now, let

$$G(x) = S(x) \prod_{(k,i) \in I} F_i^{(k)}(x) \quad \text{and} \quad H(x) = \frac{G(x)}{c}.$$

Second, we show that $\mathsf{d}(G(x)) = cD$, which implies $H(x) \in \mathrm{Int}(D)$ and $\mathsf{d}(H(x)) = 1$. Note that

$$\mathsf{d}(G(x)) = \mathsf{d}\left(S(x) \prod_{(k,i) \in I} F_i^{(k)}(x)\right) = \mathsf{d}\left(s(x) \prod_{(k,i) \in I} f_i^{(k)}\right) = \mathsf{d}\left(\prod_{i=0}^{\sigma-1}(x - s_i) \prod_{r \in \mathcal{R}} (x - r)^2\right). \tag{2.4.2}$$

By construction, the multiset $\mathcal{R} \uplus \mathcal{R} \uplus \mathcal{S}$ contains a complete system of residues modulo $P$, and the residue class modulo $P$ of $s_1 \in \mathcal{S}$ occurs only once among the elements of $\mathcal{R} \uplus \mathcal{R} \uplus \mathcal{S}$. Equation (2.4.2) and Lemma 2.3.2, applied to $Q = P$ and $\mathcal{T} = \mathcal{R} \uplus \mathcal{R} \uplus \mathcal{S}$, $e = 1$, and $z = s_1$, together imply that

$$\mathsf{v}_P\left(\mathsf{d}\left(S(x) \prod_{(k,i) \in I} F_i^{(k)}(x)\right)\right) = 1$$

One can argue similarly for $Q_i$, $1 \leq i \leq t$: The multiset $\mathcal{R} \uplus \mathcal{R} \uplus \mathcal{S}$ contains $e_i$ disjoint complete systems of residues modulo $Q_i$ in which the respective representatives of the same residue class in different systems are congruent modulo $Q_i^2$. No more than $e_i$ elements of $\mathcal{R} \uplus \mathcal{R} \uplus \mathcal{S}$ are congruent 1 modulo $Q_i$, and these $e_i$ elements are all in the same residue class modulo $Q_i^2$. By Lemma 2.3.2, applied to $Q = Q_i$, $\mathcal{T} = \mathcal{R} \uplus \mathcal{R} \uplus \mathcal{S}$, $e = e_i$ and $z = 1$, and Equation (2.4.2), it follows that

$$\mathsf{v}_{Q_i}\left(\mathsf{d}\left(S(x)\prod_{(k,i)\in I} F_i^{(k)}(x)\right)\right) = e_i \tag{2.4.3}$$

for $1 \leq i \leq t$. Since $\mathcal{R} \uplus \mathcal{R} \uplus \mathcal{S}$ does not contain a complete system of residues modulo any prime ideal other than $P$, $Q_1$, …, $Q_t$, we conclude (by Lemma 2.3.2) that

$$\mathsf{d}(G(x)) = \mathsf{d}\left(S(x)\prod_{(k,i)\in I} F_i^{(k)}(x)\right) = P Q_1^{e_1} \cdots Q_t^{e_t} = cD.$$

This shows $H(x) \in \operatorname{Int}(D)$ and $\mathsf{d}(H(x)) = 1$.

Third, we prove that the essentially different factorizations of $H(x)$ into irreducibles in $\operatorname{Int}(D)$ are given by:

$$H(x) = F_1^{(h)}(x) \cdots F_{m_h}^{(h)}(x) \cdot \frac{S(x)\prod_{(k,i)\in I\setminus I_h} F_i^{(k)}(x)}{c} \tag{2.4.4}$$

where $1 \leq h \leq n$.

It follows from the properties of $\mathcal{R}$ and $\mathcal{S}$ that the polynomial $s(x)$ is indispensable for the prime ideals $P$ and $Q_1$, …, $Q_t$ (among the polynomials $s(x)$ and $f_i^{(k)}$ for $(k,i) \in I$). This further implies that the polynomial $S(x)$ is indispensable for the prime ideals $P$ and $Q_1$, …, $Q_t$ (among the polynomials $S(x)$ and $F_i^{(k)}$ for $(k,i) \in I$), cf. Remark 2.3.7.

Thus, by Lemma 2.3.8, the essentially different factorizations of $H(x)$ into irreducibles in $\operatorname{Int}(D)$ are given by:

$$H(x) = \frac{S(x)\prod_{(k,i)\in J} F_i^{(k)}(x)}{c} \prod_{(h,j)\in I\setminus J} F_j^{(h)}(x) \tag{2.4.5}$$

where $J \subseteq I$ is minimal such that $\mathsf{d}\left(S(x)\prod_{(k,i)\in J} F_i^{(k)}(x)\right) = cD$.

Since $\mathsf{v}_{Q_i}(\mathsf{d}(S(x))) = e_i$ by Lemma 2.3.2, the possible choices for $J \subseteq I$ only depend on the prime ideal $P$. For a subset $J \subseteq I$, let $\mathcal{B}_J = \biguplus_{(k,i)\in J} B[k,i]$. Then

$$\mathsf{d}\left(S(x)\prod_{(k,i)\in J} F_i^{(k)}(x)\right) = \mathsf{d}\left(\prod_{r\in\mathcal{S}}(x-r)\prod_{r\in\mathcal{B}_J}(x-r)\right) \tag{2.4.6}$$

and it follows from Lemma 2.3.2 that the fixed divisor in Equation (2.4.6) is equal $cD$ if and only if $\mathcal{S} \uplus \mathcal{B}_J$ contains a complete set of residues modulo $P$ which is in turn equivalent to $\mathcal{R} \subseteq \mathcal{B}_J$. This is the case if and only if there exists $1 \leq h \leq n$ with $I \setminus I_h \subseteq J$.

Therefore, $J \subseteq I$ is minimal with $\mathsf{d}\big(S(x)\prod_{(k,i)\in J} F_i^{(k)}(x)\big) = cD$ if and only if $J = I \setminus I_h$ for some $1 \leq h \leq n$. Hence, the essentially different factorizations of $H(x)$, given by Equation (2.4.5), are precisely the $n$ essentially different factorizations stated in Equation (2.4.4), which are of lengths $m_1+1, \ldots, m_n+1$. □

**Corollary 2.4.1.** *Let $D$ be a Dedekind domain with infinitely many maximal ideals, all of them of finite index.*

*Then every finite subset of $\mathbb{N}\setminus\{1\}$ is the set of lengths of a polynomial in* $\mathrm{Int}(D)$.

**Remark 2.4.2.** Kainrath [44, Theorem 1] proved a similar result as Corollary 2.4.1 for Krull monoids $H$ with infinite class group in which every divisor class contains a prime divisor. In his proof, he uses transfer mechanisms.

Corollary 2.5.1 in the following section will show that this technique is not applicable to the proof of either Theorem 2.4.1 or Corollary 2.4.1.

## 2.5. Not a transfer Krull domain

In this section we show that if $D$ is a Dedekind domain with infinitely many maximal ideals, all of finite index, then there does not exist a transfer homomorphism from the multiplicative monoid $\mathrm{Int}(D)\setminus\{0\}$ to a block monoid. In the terminology introduced by Geroldinger [34], this means, $\mathrm{Int}(D)$ is not a *transfer Krull domain.*

We refer to [36, Definitions 2.5.5 & 3.2.1] for the definition of a block monoid and a transfer homomorphism, respectively. So far, there is only a small list of examples of naturally occurring rings $R$ for which it has been shown that there is no transfer homomorphism from $R\setminus\{0\}$ to a block monoid, see [28], [37], [38].

In a block monoid, the lengths of factorizations of elements of the form $c \cdot d$ with $c$, $d$ irreducible, $c$ fixed, are bounded by a constant depending only on $c$, cf. [36, Lemma 6.4.4]. More generally, every monoid admitting a transfer homomorphism to a block monoid has this property; see [36, Proposition 3.2.3].

We now demonstrate for the irreducible element $c = x$ in $\mathrm{Int}(D)$ that the lengths of factorizations of elements of the form $c \cdot d$ with $d$ irreducible in $\mathrm{Int}(D)$ are not bounded. We infer from this that there does not exist a transfer homomorphism from the multiplicative monoid $\mathrm{Int}(D)\setminus\{0\}$ to a block monoid.

**Theorem 2.5.1.** *Let $D$ be a Dedekind domain with infinitely many maximal ideals, all of them of finite index. Then for every $n \geq 1$ there exist irreducible elements $H, G_1, \ldots, G_{n+1}$ in $\mathrm{Int}(D)$ such that*

$$xH(x) = G_1(x) \cdots G_{n+1}(x).$$

**Proof.** Let $P_1, \ldots, P_n$ be distinct maximal ideals of $D$, none of them of index 2. By $\mathsf{v}_i$ we denote the discrete valuation associated to $P_i$. Let $c \in D$ such that $\mathsf{v}_i(c) = 1$ for $i = 1, \ldots, n$, and $c$ is not contained in any maximal ideal of $D$ of index 2.

Say the prime factorization of $cD$ is $cD = P_1 \cdot \ldots \cdot P_n \cdot Q_1^{e_1} \cdot \ldots \cdot Q_m^{e_m}$, and define

$$N = \max(\{\|P_i\| \mid 1 \leq i \leq n\} \cup \{e_i\|Q_i\| \mid 1 \leq i \leq m\}).$$

Let $\mathcal{P} = \{P_i \mid 1 \leq i \leq n\}$, $\mathcal{P}_1 = \{Q_i \mid 1 \leq i \leq m\}$, and

$$\mathcal{P}_2 = \{Q \in \text{max-spec}(D) \setminus (\mathcal{P} \cup \mathcal{P}_1) \mid \|Q\| \leq N + n\}.$$

Let $\mathcal{R}$ be a subset of $D$ of order $N$ with the following properties (which can be realized by the Chinese Remainder Theorem):

(i) $\mathcal{R}$ contains an element $r_0 \in \left(\bigcap_{i=1}^n P_i\right) \cap \left(\bigcap_{i=1}^m Q_i^2\right)$.

(ii) No element of $\mathcal{R}$ other than $r_0$ is in any $P_i \in \mathcal{P}$.

(iii) For each $P_i \in \mathcal{P}$, $\mathcal{R}$ contains a complete system of residues modulo $P_i$.

(iv) For each $Q_i \in \mathcal{P}_1$, $\mathcal{R}$ contains $e_i$ disjoint complete systems of residues, in which the respective representatives of the same residue class in different systems are congruent modulo $Q_i^2$;

(v) No more than $e_i$ elements of $\mathcal{R}$ are in $Q_i$.

(vi) For all $Q \in \mathcal{P}_2$, all elements of $\mathcal{R}$ are contained in $Q$.

We set $\mathcal{B} = \mathcal{R} \setminus \{r_0\}$.

Also, let $a_1, \ldots, a_n \in D$ with the following properties (which, again, can be realized by the Chinese Remainder Theorem):

(i) For all $i = 1, \ldots, n$, $a_i \equiv 0 \mod P_i$.

(ii) For all $i = 1, \ldots, n$, $a_i \equiv 1 \mod P_j$ for all $j \neq i$.

(iii) For all $Q \in \mathcal{P}_1$, $a_n \equiv 0 \mod Q^2$ and $a_i \equiv 1 \mod Q$ for all $1 \leq i < n$,

(iv) For all $Q \in \mathcal{P}_2$ and all $1 \leq i \leq n$, $a_i \equiv 0 \mod Q$.

Let $f(x) = \prod_{b \in \mathcal{B}}(x - b)$ and let $F(x) \in D[x]$ be monic and irreducible in $K[x]$ such that for every selection of polynomials from the set $\{x, f\} \cup \{(x - a_i) \mid 1 \leq i \leq n\}$ the product of the polynomials has the same fixed divisor as the modified product in which $f$ has been replaced by $F$, as in Lemma 2.3.3.

Lemmas 2.3.3 and 2.3.2, applied to $\mathcal{T} = \mathcal{B} \cup \{a_1, \ldots, a_n\}$ and each of the prime ideals in $\mathcal{P} \cup \mathcal{P}_1$, imply that

$$\mathsf{d}\left(F(x)\prod_{i=1}^{n}(x - a_i)\right) = \mathsf{d}\left(f(x)\prod_{i=1}^{n}(x - a_i)\right) = cD.$$

Similarly, Lemmas 2.3.3 and 2.3.2, applied to $\mathcal{T} = \mathcal{B} \cup \{0\}$ and each of the prime ideals in $\mathcal{P} \cup \mathcal{P}_1$, imply that

$$\mathsf{d}(xF(x)) = \mathsf{d}\big(xf(x)\big) = cD.$$

We set

$$H(x) = \frac{F(x)\prod_{j=1}^{n}(x - a_j)}{c} \quad \text{and} \quad G(x) = \frac{xF(x)}{c}.$$

Then $G(x)$ and $H(x)$ are elements of $\mathrm{Int}(D)$ with $\mathsf{d}(G(x)) = \mathsf{d}(H(x)) = 1$ such that

$$xH(x) = G(x)(x - a_1)\cdots(x - a_n).$$

It remains to show that $H(x)$ and $G(x)$ are irreducible in $\mathrm{Int}(D)$. Observe that, among the polynomials $x$ and $f(x)$, $x$ is indispensable for all $P \in \mathcal{P}$ and $f(x)$ is indispensable for all $P \in \mathcal{P}$ and all $Q \in \mathcal{P}_1$. It follows that, among the polynomials $x$ and $F(x)$, $x$ is indispensable for all $P \in \mathcal{P}$ and $F(x)$ is indispensable for all $P \in \mathcal{P}$ and all $Q \in \mathcal{P}_1$, cf. Remark 2.3.7. Hence $G(x)$ is irreducible in $\mathrm{Int}(D)$ by Lemma 2.3.8.

Finally, again by Lemma 2.3.8 and Remark 2.3.7, $H(x)$ is irreducible in $\mathrm{Int}(D)$, since

(i) $F(x)$ and $x - a_i$ are indispensable for $P_i$ $(1 \leq i \leq n)$

(ii) $F(x)$ is indispensable for $Q_i$ $(1 \leq i \leq m)$

among the polynomials $F(x)$ and $x - a_j$ with $1 \le j \le n$. $\square$

As discussed at the beginning of this section, we may conclude:

**Corollary 2.5.1.** *Let $D$ be a Dedekind domain with infinitely many maximal ideals, all of them of finite index.*

*Then there does not exist a transfer homomorphism from the multiplicative monoid* $\mathrm{Int}(D) \setminus \{0\}$ *to a block monoid; in other words:* $\mathrm{Int}(D)$ *is not a transfer Krull domain.*

# 3. Non-absolutely irreducible elements in the ring of integer-valued polynomials

This chapter consists of article [47] titled, "Non-absolutely irreducible elements in the ring of integer-valued polynomials". The article appeared in *Communications in Algebra* in January 2020.


## Abstract

Let $R$ be a commutative ring with identity. An element $r \in R$ is said to be absolutely irreducible in $R$ if for all natural numbers $n > 1$, $r^n$ has essentially only one factorization namely $r^n = r \cdots r$. If $r \in R$ is irreducible in $R$ but for some $n > 1$, $r^n$ has other factorizations distinct from $r^n = r \cdots r$, then $r$ is called non-absolutely irreducible. In this paper, we construct non-absolutely irreducible elements in the ring $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$ of integer-valued polynomials. We also give generalizations of these constructions.



**Keywords:** Irreducible elements, absolutely irreducible elements, non-absolutely irreducible elements, integer-valued polynomials

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


## 3.1. Introduction

The ring $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$ of integer-valued polynomials is known not to be a unique factorization domain. To fully understand the factorization behaviour of $\mathrm{Int}(\mathbb{Z})$, several researchers have investigated the irreducible elements of $\mathrm{Int}(\mathbb{Z})$, see for example [12], [17], [25] and [52].

In [36, Chapter 7], Geroldinger and Halter-Koch defined a type of irreducible elements called absolutely irreducible. They called an irreducible element $r$ absolutely irreducible if for all natural numbers $n > 1$, each power $r^n$ of $r$ has essentially only one factorization namely $r^n = r \cdots r$. Such irreducible elements have also been called strong atoms in [24] and completely irreducible in [43].

Of much interest are the non-absolutely irreducible elements. We call an irreducible element $r$ non-absolutely irreducible if there exists a natural number $n > 1$ such that $r^n$ has other factorizations essentially distinct from $r \cdots r$. In [24], Chapman and Krause proved that the ring of integers of a number field always has non-absolutely irreducible elements unless it is a unique factorization domain. Similarly, $\mathrm{Int}(\mathbb{Z})$ is a non-unique factorization domain with non-absolutely irreducible elements. For instance, the polynomial $f = \frac{x(x^2+3)}{2}$ is not absolutely irreducible in $\mathrm{Int}(\mathbb{Z})$ since

$$f^2 = f \cdot f = \frac{x^2(x^2+3)}{4} \cdot (x^2+3).$$

In this paper, we construct non-absolutely irreducible elements in $\mathrm{Int}(\mathbb{Z})$, a first step to characterizing them. The constructions we give serve as a cornerstone for studying patterns of factorizations in $\mathrm{Int}(\mathbb{Z})$.

The researchers who have studied factorizations in $\mathrm{Int}(\mathbb{Z})$ have mostly been considering square-free factorizations. For instance, in [29], Frisch showed that $\mathrm{Int}(\mathbb{Z})$ has wild factorization behavior but the factorizations she used to realize her main result (Theorem 9 in [29]) were all square-free. It is not known whether $\mathrm{Int}(\mathbb{Z})$ exhibits similar behavior for non-square-free factorizations. The study of the non-absolutely irreducible elements of $\mathrm{Int}(\mathbb{Z})$ will be helpful in answering such questions.

We first give some necessary definitions and facts in Section 3.2. In Sections 3.3 and 3.4, we construct non-absolutely irreducible elements in $\mathrm{Int}(\mathbb{Z})$. We then give a construction for patterns of factorizations in Section 3.5 and finally in Section 3.6, we give generalizations of the examples in Sections 3.3 and 3.4.

## 3.2. Preliminaries

This section contains necessary definitions and facts on factorizations and irreducible elements of $\mathrm{Int}(\mathbb{Z})$.

### Factorization terms

We only define the factorization terms we need in this paper and refer to [36] for a deeper study of factorization theory. Let $R$ be a commutative ring with identity and $r, s \in R$ be non-zero non-units.

(i) We say $r$ is *irreducible* in $R$ if it cannot be written as the product of two non-units of $R$.

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

$$r = a_1 \cdots a_n \qquad (3.2.1)$$

where $a_i$ is irreducible in $R$ for $1 \le i \le n$.

(iii) The *length* of the factorization in (3.2.1) is the number $n$ of irreducible factors.

(iv) We say $r$ and $s$ are *associated* in $R$ if there exists a unit $u \in R$ such that $r = us$.

(v) Two factorizations

$$r = a_1 \cdots a_n = b_1 \cdots b_m \qquad (3.2.2)$$

are called *essentially the same* if $n = m$ and after some possible reordering, $a_j$ is associated to $b_j$ for $1 \le j \le m$. Otherwise, the factorizations in (3.2.2) are called *essentially different*.

(vi) An element $r \in R$ is said to be *absolutely irreducible* if it is irreducible in $R$ and for all natural numbers $n > 1$, every factorization of $r^n$ is essentially the same as $r^n = r \cdots r$. Equivalently, $r \in R$ is called *absolutely irreducible* if $r^n$ has exactly one factorization up to associates.

If $r$ is irreducible but there exists a natural number $n > 1$ such that $r^n$ has other factorizations essentially different from $r^n = r \cdots r$, then $r$ is called *non-absolutely irreducible*.

## Irreducible elements of Int($\mathbb{Z}$)

We begin with some preliminary definitions and facts, and later state a characterization of irreducible elements of Int($\mathbb{Z}$) which we shall use in this paper.

**Definition 3.2.1.** The ring $\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$ is called the *ring of integer-valued polynomials.*

We refer to [18] for a deeper study of integer-valued polynomials.

**Definition 3.2.2.** (i) Let $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. The *content* of $f$ is the ideal

$$\mathsf{c}(f) = (gcd[a_0, a_1, \ldots, a_n])$$

of $\mathbb{Z}$ generated by the coefficients of $f$. The polynomial $f$ is said to be *primitive* if $\mathsf{c}(f) = (1) = \mathbb{Z}$.

(ii) Let $f \in \mathrm{Int}(\mathbb{Z})$. The *fixed divisor* of $f$ is the ideal

$$\mathsf{d}(f) = (gcd[f(a) \mid a \in \mathbb{Z}])$$

of $\mathbb{Z}$ generated by the elements $f(a)$ with $a \in \mathbb{Z}$. Note that it is sufficient to consider $0 \le a \le deg(f)$, that is,

$$\mathsf{d}(f) = (gcd[f(a) \mid 0 \le a \le deg(f)]),$$

cf. [11, Lemma 2.7]. The polynomial $f$ is said to be *image primitive* if $\mathsf{d}(f) = (1) = \mathbb{Z}$.

**Note 3.2.3.** (i) A polynomial $\frac{g}{b}$ with $g \in \mathbb{Z}[x]$ and $b \in \mathbb{N}$, is in $\mathrm{Int}(\mathbb{Z})$ if and only if $b$ divides the fixed divisor $\mathsf{d}(g)$ of $g$.

(ii) Let $f \in \mathbb{Z}[x]$ be primitive with degree $n$ and $p \in \mathbb{Z}$ be prime. If $p$ divides the fixed divisor of $f$, then $p \le n$, cf. for instance [29, Remark 3].

**Remark 3.2.4.** In analogy to the well known fact that $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is primitive and irreducible in $\mathbb{Q}[x]$, Chapman and McClain [25] showed that $f \in \mathbb{Z}[x]$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ if and only if it is image primitive and irreducible in $\mathbb{Q}[x]$. This follows as a special case from Remark 3.2.6.

**Note 3.2.5.** Every non-zero polynomial $f \in \mathbb{Q}[x]$ can be written in a unique way up to the sign of $a$ and the signs and indexing of the $g_i$ as

$$f(x) = \frac{a}{b} \prod_{i \in I} g_i(x)$$

with $a \in \mathbb{Z}, b \in \mathbb{N}$ with $\gcd(a, b) = 1$, $I$ a non-empty finite set and for $i \in I$, $g_i$ primitive and irreducible in $\mathbb{Z}[x]$.

**Remark 3.2.6.** [29] A non-constant polynomial $f \in \mathrm{Int}(\mathbb{Z})$ written as in Note 3.2.5 is irreducible in $\mathrm{Int}(\mathbb{Z})$ if and only if:

(i) $a = \pm 1$,

(ii) $(b) = \mathsf{d}\left(\prod_{i \in I} g_i\right)$ and

(iii) there does not exist a partition of $I$ into non-empty subsets $I = I_1 \uplus I_2$ and $b_1, b_2 \in \mathbb{N}$ with $b_1 b_2 = b$ and $(b_1) = \mathsf{d}\left(\prod_{i \in I_1} g_i\right), (b_2) = \mathsf{d}\left(\prod_{i \in I_2} g_i\right)$.

## 3.3. Non-absolutely irreducibles: different factorizations of the same length

In this section we construct non-absolutely irreducible elements $r$ such that for all $n > 1$, the factorizations of $r^n$ are all of the same length.

Consider the irreducible polynomial

$$f = \frac{x(x-4)(x^2+3)}{4} \in \mathrm{Int}(\mathbb{Z}).$$

It can be checked easily that

$$\mathsf{d}(x(x-4)(x^2+3)) = (4) = \mathsf{d}(x^2(x^2+3)) = \mathsf{d}((x-4)^2(x^2+3)).$$

Furthermore, the polynomials $\frac{x^2(x^2+3)}{4}$ and $\frac{(x-4)^2(x^2+3)}{4}$ are irreducible in $\mathrm{Int}(\mathbb{Z})$ by Remark 3.2.6. Thus

$$f^2 = \frac{x^2(x^2+3)}{4} \cdot \frac{(x-4)^2(x^2+3)}{4}$$

is a factorization of $f^2$ and it is essentially different from $f \cdot f$. Therefore

$$f = \frac{x(x-4)(x^2+3)}{4}$$

is not absolutely irreducible in $\mathrm{Int}(\mathbb{Z})$.

More generally, we have the following construction.

**Example 3.3.1.** Let $p$ be an odd prime and $n > 1$ a natural number. Let

$$h(x) = x^{p^{n-1}(p-1)} - q$$

where $q$ is a prime congruent to 1 mod $p^{n+1}$ and $q > p^{n-1}(p-1) + n$. Then $h$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's irreducibility criterion.

Furthermore, $\mathsf{v}_p(h(u)) \geq n$ for all integers $u$ not divisible by $p$ since the group of units of $\mathbb{Z}/p^n\mathbb{Z}$ is cyclic of order $p^{n-1}(p-1)$. Moreover, if $r$ is a generator of the group of units of $\mathbb{Z}/p^{n+1}\mathbb{Z}$, then, since $h(r)$ is not zero modulo $p^{n+1}$, it follows that $\mathsf{v}_p(h(r)) = n$. Therefore the minimum $\mathsf{v}_p(h(u))$ for $u$ an integer not divisible by $p$ is exactly $n$.

Now let $a_1, \ldots, a_n$ be integers divisible by $p$, not representing all residue classes of $p^2$ that are divisible by $p$ and such that no $a_i$ (for $1 \leq i \leq n$) is congruent to 0 modulo any prime $l \leq p^{n-1}(p-1) + n$, $l \neq p$.

We set
$$f(x)=\frac{h(x)\prod_{i=1}^{n}(x-a_i)}{p^n}.$$
By the choice of the integers $a_1,\dots,a_n$, the minimum $\mathsf{v}_p\left(\prod_{i=1}^{n}(w-a_i)\right)$ for $w\in p\mathbb{Z}$ is exactly $n$. Moreover, for each prime $l\le p^{n-1}(p-1)+n$, $l\neq p$, $l$ does not divide the fixed divisor of the numerator $h(x)\prod_{i=1}^{n}(x-a_i)$ of $f(x)$. Because of these facts and by Remark 3.2.6, $f(x)$ is in Int($\mathbb{Z}$) and it is irreducible in Int($\mathbb{Z}$).

Now suppose $a_1,\dots,a_n$ contains at least two different elements. Then for $k>1$, $f^k$ has factorizations essentially different from $f\cdots f$. All of these factorizations have length $k$.

For example, without loss of generality, let $a_1$ and $a_2$ be different. Then
$$f^k=\frac{h(x)(x-a_1)^2\prod_{i=3}^{n}(x-a_i)}{p^n}\cdot\frac{h(x)(x-a_2)^2\prod_{i=3}^{n}(x-a_i)}{p^n}\cdot\underbrace{f\cdots f}_{k-2\text{ copies}}$$
is a factorization of $f^k$ essentially different from $f\cdots f$.

**Remark 3.3.2.** In Example 3.3.1, we could use a different polynomial $h(x)$, namely:
$$h(x)=c(x)d(x)$$
where
$$\begin{aligned} c(x) &= x^{\frac{p^{n-1}(p-1)}{2}}-q\\ d(x) &= x^{\frac{p^{n-1}(p-1)}{2}}-r \end{aligned}$$
with $q$ and $r$ primes congruent to 1 and $-1$ respectively, mod $p^{n+1}$ and both $q,r$ greater than $p^{n-1}(p-1)+n$. Similarly, both $c(x)$ and $d(x)$ are irreducible in $\mathbb{Q}[x]$ by Eisenstein's irreducibility criterion.

Furthermore, if $u$ is a unit mod $p^n$, then $\mathsf{v}_p(c(u))\ge n$ iff $u$ is a square mod $p^n$ and $\mathsf{v}_p(d(u))\ge n$ iff $u$ is a non-square mod $p^n$. Also, if $r$ is a generator of the group of units of $\mathbb{Z}/p^{n+1}\mathbb{Z}$, then $\mathsf{v}_p(d(r))=n$ and $\mathsf{v}_p(c(r))=0$. Therefore the minimum $\mathsf{v}_p(c(u)d(u))$ for $u$ an integer not divisible by $p$ is exactly $n$.

The construction involving two polynomials $c(x)$ and $d(x)$ can be used to exhibit factorizations of different lengths of a power of an irreducible polynomial, cf. Example 3.4.1.

**Note 3.3.3.** In Example 3.3.1, we have one prime in the denominator but this can be extended to several primes. For instance, if we allow some $a_i$ to be congruent to 0 modulo other primes $l < p^{n-1}(p-1)+n$, then the roots of the numerator of $f$ can contain a complete set of residues modulo some $l$. More specifically, we have the following example.

**Example 3.3.4.** Let $p, q$ be distinct odd primes, and let $n \geq 2q$ be a natural number. Let

$$h(x) = x^{p^{n-1}(p-1)} - r$$

where $r$ is a prime congruent to 1 mod $p^{n+1}$ and $r > p^{n-1}(p-1)+n$. Then $h$ is irreducible in $\mathbb{Q}[x]$ and the minimum $\mathsf{v}_p(h(u))$ for $u$ an integer not divisible by $p$ is $n$.

Let $a_1, \ldots, a_n$ be integers divisible by $p$, not representing all residue classes of $p^2$ that are divisible by $p$, and such that:

(i) $a_1, \ldots, a_q$ is a complete system of residues mod $q$, and the remaining $a_i$ with $i > q$ are all congruent to 1 mod $q$.

(ii) For $1 \leq i \leq n$, $a_i \not\equiv 0 \pmod{l}$ for all primes $l < p^{n-1}(p-1)+n$, $l \neq p, q$.

Set

$$f(x) = \frac{h(x)\prod_{i=1}^{n}(x-a_i)}{qp^n}.$$

Then $f$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ by Remark 3.2.6 and $f^2$ has a factorization essentially different from $f \cdot f$, namely;

$$f^2 = \frac{h(x)\prod_{i=1}^{q}(x-a_i)^2\prod_{i=2q+1}^{n}(x-a_i)}{q^2p^n} \cdot \frac{h(x)\prod_{i=q+1}^{2q}(x-a_i)^2\prod_{i=2q+1}^{n}(x-a_i)}{p^n}.$$

Also in the spirit of Example 3.3.1, we have the following example involving two primes.

**Example 3.3.5.** Let $q < p$ be odd primes, and let $1 < m \leq n$ be natural numbers. Let

$$t = lcm(q^{m-1}(q-1), p^{n-1}(p-1)).$$

We set

$$h(x) = x^t - r$$

where $r$ is a prime congruent to 1 mod $p^{n+1}q^{m+1}$ and $r > t+n$. Then $h$ is irreducible in $\mathbb{Q}[x]$ and $\mathsf{v}_p(h(u)) \geq n$ for all integers $u$ not divisible by $p$, and $\mathsf{v}_q(h(w)) \geq m$ for all integers $w$ not divisible by $q$.

Now let $a_1,\dots,a_n$ be integers divisible by $p$ but not representing all residue classes of $p^2$ that are divisible by $p$, and such that:

(i) $a_1,\dots,a_m$ are divisible by $q$ but not representing all residue classes of $q^2$ that are divisible by $q$, and the remaining $a_i$ with $i > m$ are all congruent to 1 mod $q$.

(ii) For $1 \le i \le n$, $a_i \not\equiv 0 \pmod{l}$ for all primes $l < t+n$, $l \ne p,q$.

We set

$$f(x) = \frac{h(x)\prod_{i=1}^{n}(x-a_i)}{p^n q^m}.$$

Then $f$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ by Remark 3.2.6 and if $a_1,\dots,a_m$ or $a_{m+1},\dots,a_n$ contains at least two different elements, then for some $k>1$, $f^k$ has a factorization essentially different from $f\cdots f$.

For instance, without loss of generality let $a_1$ and $a_2$ be different. Then

$$f^2 = \frac{h(x)(x-a_1)^2\prod_{i=3}^{n}(x-a_i)}{p^n q^m}\cdot\frac{h(x)(x-a_2)^2\prod_{i=3}^{n}(x-a_i)}{p^n q^m}$$

is a factorization of $f^2$ essentially different from $f\cdot f$. Similarly, if $a_{m+1}$ and $a_{m+2}$ are different, then

$$f^2 = \frac{h(x)g(x)(x-a_{m+1})^2}{p^n q^m}\cdot\frac{h(x)g(x)(x-a_{m+2})^2}{p^n q^m}$$

where $g(x)=\prod_{i=1}^{m}(x-a_i)\prod_{i=m+3}^{n}(x-a_i)$, is a factorization of $f^2$ essentially different from $f\cdot f$.

## 3.4. Non-absolutely irreducibles: factorizations of different lengths

Here we construct non-absolutely irreducible elements $r$ such that for some $n>1$, some factorizations of $r^n$ have different lengths.

Consider the irreducible polynomial

$$f = \frac{(x-3)(x^3-17)(x^3-19)}{3} \in \mathrm{Int}(\mathbb{Z}).$$

Then

$$f^2 = \frac{(x-3)^2(x^3-17)(x^3-19)}{9}\cdot(x^3-17)(x^3-19)$$

is a factorization of $f^2$ essentially different from $f \cdot f$. This results from

$$gcd(a^3 - 17 \mid a \in \{2 + 3\mathbb{Z}\}) = gcd(a^3 - 19 \mid a \in \{1 + 3\mathbb{Z}\}) = 9$$

such that for all $a \not\equiv 0 \pmod 3$, $(a^3 - 17)(a^3 - 19)$ is divisible by 9.

This behaviour motivates the next example and more generally Lemma 3.6.7.

**Example 3.4.1.** Let $p$ be an odd prime and $n > m$ be natural numbers. We set

$$\begin{aligned} c(x) &= x^{\frac{p^{n-1}(p-1)}{2}} - q \\ d(x) &= x^{\frac{p^{n-1}(p-1)}{2}} - r \end{aligned}$$

where $q$ and $r$ are primes congruent to 1 and $-1$ respectively, mod $p^{n+1}$ and both $q, r$ are greater than $p^{n-1}(p-1) + m$. Then both $c(x)$ and $d(x)$ are irreducible in $\mathbb{Q}[x]$ by Eisenstein's irreducibility criterion.

Furthermore, if $u$ is a unit mod $p^n$, then $\mathsf{v}_p(c(u)) \geq n$ iff $u$ is a square mod $p^n$ and $\mathsf{v}_p(d(u)) \geq n$ iff $u$ is a non-square mod $p^n$. Note that both $c(x)$ and $d(x)$ are irreducible in Int($\mathbb{Z}$) by Remark 3.2.4 because, being primitive, they are irreducible in $\mathbb{Z}[x]$ and $\mathsf{d}(c(x)) = \mathsf{d}(d(x)) = (1)$. Furthermore, $\mathsf{d}(c(x)d(x)) = (1)$.

Now let $a_1, \ldots, a_m$ be integers divisible by $p$, not representing all residue classes of $p^2$ that are divisible by $p$ and such that no $a_i$ (for $1 \leq i \leq m$) is congruent to 0 modulo any prime $l \leq p^{n-1}(p-1) + m$, $l \neq p$.

Set

$$f(x) = \frac{c(x)d(x)\prod_{i=1}^{m}(x - a_i)}{p^m}.$$

Then $f$ is irreducible in Int($\mathbb{Z}$) by Remark 3.2.6. Now irrespective of all $a_1, \ldots, a_m$ being the same or different,

$$f^n = \prod_{i=1}^{m} \frac{c(x)d(x)(x - a_i)^n}{p^n} \cdot c(x)^{n-m} d(x)^{n-m}$$

is a factorization of $f^n$ essentially different from $\underbrace{f \cdots f}_{n \text{ copies}}$.

Note that $f^k$ can have factorizations essentially different from $f \cdots f$ also for $k < n$, see for example the proof of Lemma 3.6.7.

For our next general example, we begin with the following motivation.

**Example 3.4.2.** Consider the irreducible polynomial

$$f = \frac{(x^4 + x^3 + 8)(x - 3)}{4} \in \text{Int}(\mathbb{Z}).$$

It can easily be checked that

$$gcd(a^4+a^3+8 \mid a \in \{0+2\mathbb{Z}\}) = 8$$

and

$$gcd(a^4+a^3+8 \mid a \in \{1+2\mathbb{Z}\}) = 2.$$

Thus 0 and 1 are both roots mod 2 of $x^4+x^3+8$ and for all $a \in \{0+2\mathbb{Z}\}$, $a^4+a^3+8$ is divisible by 8.

Therefore

$$f^2 = \frac{(x^4+x^3+8)(x-3)^2}{8} \cdot \frac{(x^4+x^3+8)}{2}$$

is a factorization of $f^2$ essentially different from $f \cdot f$.

We need the following lemma for our general example.

**Lemma 3.4.3.** *[29, Lemma 6], [32, Lemma 3.3] Let $I \neq \emptyset$ be a finite set and $f_i \in \mathbb{Z}[x]$ be monic polynomials for $i \in I$. Then there exist monic polynomials $F_i \in \mathbb{Z}[x]$ for $i \in I$, such that*

*(i)* $\deg(F_i) = \deg(f_i)$ *for all $i \in I$,*

*(ii) the polynomials $F_i$ are irreducible in $\mathbb{Q}[x]$ and pairwise non-associated in $\mathbb{Q}[x]$ and*

*(iii) for all subsets $J \subseteq I$ and all partitions $J = J_1 \uplus J_2$,*

$$\mathsf{d}\left(\prod_{j\in J_1} f_j \prod_{j\in J_2} F_j\right) = \mathsf{d}\left(\prod_{j\in J} f_j\right).$$

**Example 3.4.4.** Let $p > 3$ be a prime number and let $a_1, \ldots, a_p$ be a complete set of residues mod $p$ that does not contain a complete set of residues mod any prime $q < p$. Let

$$g_1 = (x-a_2)^2(x-a_3)^2\prod_{i=4}^{p}(x-a_i)$$

$$g_2 = (x-a_1)^2(x-a_3)^2\prod_{i=4}^{p}(x-a_i)$$

$$g_3 = (x-a_1)^2(x-a_2)^2\prod_{i=4}^{p}(x-a_i).$$

By Lemma 3.4.3, we find polynomials $G_1, G_2, G_3$, of the same degree as $g_1, g_2, g_3$ respectively, irreducible in $\mathbb{Q}[x]$ and pairwise non-associated in $\mathbb{Q}[x]$ such that for any product $P$ of polynomials from among the $g_i$ and any product $Q$ that differs from $P$ in that some of the $g_i$ have been replaced by their respective $G_i$, we have $\mathsf{d}(P) = \mathsf{d}(Q)$.

Let $e_p(g) = \mathsf{v}_p(\mathsf{d}(g))$ denote the exponent of $p$ in the fixed divisor of $g$. Now note that for each index $i$, $e_p(G_i) = 0$ and for any two different indices $i, j$, $e_p(G_i G_j) = 2$, and, finally, $e_p(G_1 G_2 G_3) = 3$.

This shows that
$$f = \frac{G_1 G_2 G_3}{p^3}$$
is in $\mathrm{Int}(\mathbb{Z})$ and is irreducible in $\mathrm{Int}(\mathbb{Z})$, and that $f^2$ factors as
$$f^2 = \frac{G_1 G_2}{p^2} \cdot \frac{G_2 G_3}{p^2} \cdot \frac{G_3 G_1}{p^2}, \tag{3.4.1}$$
which factorization is essentially different from $f \cdot f$. Thus $f$ is not absolutely irreducible.

Note that in the above example, $p$ divides the fixed divisor of $G_i G_j$ for $i \neq j$ and
$$\mathsf{v}_p\left(gcd\left(G_i(a)G_j(a) \,\middle|\, a \equiv a_k \pmod{p}, k \neq i, j\right)\right) = 4 > \mathsf{v}_p(\mathsf{d}(f)).$$
This behaviour is similar to the one in example 3.4.2 and more generally in Lemma 3.6.8.

**Remark 3.4.5.** (i) Like Example 3.3.1, the constructions in this section can be extended to several primes in the denominator of $f$.

(ii) In Example 3.4.1, if we employ the usual
$$h(x) = x^{p^{n-1}(p-1)} - q$$
where $q$ is a prime congruent to 1 mod $p^{n+1}$ and $q > p^{n-1}(p-1) + n$, instead of $c(x)d(x)$, $f$ remains non-absolutely irreducible but the factorizations of $f^k$ all have the same length $k$.

(iii) In the examples we have given in this section, the factorizations of $f^k$ have length greater than or equal to $k$ but we can also have non-absolutely irreducibles $f$ in $\mathrm{Int}(\mathbb{Z})$ such that for some $k > 2$, some factorizations of $f^k$ have length less than $k$. For instance, consider the polynomial
$$f = \frac{(x^2+4)(x^4+7)}{4} \in \mathrm{Int}(\mathbb{Z}).$$

It is clearly irreducible and

$$f^3 = \frac{(x^2+4)^3(x^4+7)^2}{64} \cdot (x^4+7)$$

is a factorization of $f^3$ essentially different from $f \cdot f \cdot f$ and it is of length 2.

## 3.5. Patterns of factorizations

The researchers who have studied factorizations in Int($\mathbb{Z}$) have mostly been considering square-free factorizations. For instance, in [29], Frisch showed that Int($\mathbb{Z}$) has wild factorization behavior but the factorizations she used to realize her main result (Theorem 9 in [29]) were all square-free. It is not known whether Int($\mathbb{Z}$) exhibits similar behavior for non-square-free factorizations. The study of non-absolutely irreducible elements lays a foundation for studying patterns of factorizations.

As a first step to understanding patterns of factorizations in Int($\mathbb{Z}$), we give a construction using the examples in Sections 3.3 and 3.4. We begin with a motivation.

**Definition 3.5.1.** Let $R$ be a commutative ring with identity and $r \in R$ be a nonzero non-unit.

(i) A sequence of natural numbers $\lambda = (k_1, \dots, k_s)$ is called a *partition of a natural number $n$* if $k_1 + \dots + k_s = n$ with $k_1 \geq k_2 \geq \dots \geq k_s > 0$. The natural numbers $k_1, \dots, k_s$ are called *blocks*.

(ii) If $\lambda = (k_1, \dots, k_s)$ is a partition, we say a factorization of $r$ is of *type* $\lambda$ if $r = a_1^{k_1} \cdots a_s^{k_s}$ for pairwise non-associated irreducible elements $a_1, \dots, a_s \in R$.

**Example 3.5.2.** Consider the different partitions of 4:

$$\{(4), (3,1), (2,2), (2,1,1), (1,1,1,1)\}.$$

The polynomial

$$f = \frac{(x^8-17)^4(x-4)^2(x-8)^2}{2^4} \in \mathrm{Int}(\mathbb{Z})$$

gives us factorizations of type $\lambda$ for partitions $\lambda$ of 4 other than (4):

$$\begin{aligned} f &= (x^8-17)^3\cdot\frac{(x^8-17)(x-4)^2(x-8)^2}{2^4}\\ &= (x^8-17)^2\cdot\left(\frac{(x^8-17)(x-4)(x-8)}{2^2}\right)^2\\ &= (x^8-17)^2\cdot\frac{(x^8-17)(x-4)^2}{2^2}\cdot\frac{(x^8-17)(x-8)^2}{2^2}\\ &= \frac{(x^8-17)(x-4)}{2}\cdot\frac{(x^8-17)(x-8)}{2}\cdot\frac{(x^8-17)(x-4)(x-8)}{2^2}\cdot(x^8-17). \end{aligned}$$

Note, however, that $f$ has factorizations other than those above. For example,

$$f=(x^8-17)^2\cdot\frac{(x^8-17)(x-4)^2(x-8)}{2^3}\cdot\frac{(x^8-17)(x-8)}{2}$$

is another factorization of $f$ essentially different from the above.

More generally, we have the following construction for patterns of factorizations in $\mathrm{Int}(\mathbb{Z})$. We first give a remark.

**Remark 3.5.3.** In the following example, we use partition of sets; if a set $S$ is the disjoint union of $m$ non-empty subsets $B_1,\dots,B_m$, then, we call $B=\{B_1,\dots,B_m\}$ a partition of $S$. This should not be confused with the concept of partition of a number as defined in Definition 3.5.1

**Example 3.5.4.** Let $p\in\mathbb{Z}$ be an odd prime and $n,s,t>1$ natural numbers. Set

$$\begin{aligned} c_i(x) &= x^{\frac{p^{n-1}(p-1)}{2}}-q_i\\ d_i(x) &= x^{\frac{p^{n-1}(p-1)}{2}}-r_i \end{aligned}$$

where $q_1,\dots,q_s$ are primes congruent to 1 modulo $p^{n+1}$, $r_1,\dots,r_t$ are primes congruent to $-1$ modulo $p^{n+1}$ and for all $1\le i\le s$ and $1\le j\le t$, $q_i,r_j>p^{n-1}(p-1)+n$.

Now let $a_1,\dots,a_n$ be integers divisible by $p$, not representing all residue classes of $p^2$ that are divisible by $p$ and such that no $a_j$ (for $1\le j\le n$) is congruent to 0 modulo any prime $l\le p^{n-1}(p-1)+n$, $l\ne p$. Set

$$G(x)=\frac{\prod_{i=1}^{s}c_i(x)\prod_{i=1}^{t}d_i(x)\prod_{j=1}^{n}(x-a_j)}{p^n}.$$

Then every factorization of $G$ in $\mathrm{Int}(\mathbb{Z})$ corresponds to a triple $(B,\theta,\sigma)$ where:

(i) $B$ is a partition of the set $\{1,\dots,n\}$ into $m_B$ blocks $B_1,\dots,B_{m_B}$,

(ii) $\theta$ is an injective function $\theta : \{1, \dots, m_B\} \to \{1, \dots, s\}$ and

(iii) $\sigma$ is an injective function $\sigma : \{1, \dots, m_B\} \to \{1, \dots, t\}$.

Given such a triple, for $1 \leq i \leq m_B$, we construct a polynomial $g_i$ corresponding to the $i$-th block. Suppose the $i$-th block consists of $w_i$ elements. We set

$$g_i = \frac{c_{\theta(i)}(x) d_{\sigma(i)}(x) \prod_{j \in B_i} (x - a_j)}{p^{w_i}}.$$

Then $g_i$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ by Remark 3.2.6.

Furthermore, each factorization of $G$ is of the form

$$G = \prod_{i=1}^{m_B} g_i \cdot \prod_{j \notin \operatorname{Im} \theta} c_j(x) \cdot \prod_{k \notin \operatorname{Im} \sigma} d_k(x). \tag{3.5.1}$$

Note that the length of the factorization in (3.5.1) is $s + t - m_B$.

## 3.6. Generalizations

In this section we give lemmas generalizing the examples in Sections 3.3 and 3.4. We begin with a generalization of Example 3.3.1.

**Definition 3.6.1.** (i) Let $I \neq \emptyset$ be a finite set and for $i \in I$, let $g_i \in \mathbb{Z}[x]$ be primitive and irreducible in $\mathbb{Z}[x]$. Let

$$f(x) = \frac{\prod_{i \in I} g_i(x)}{b} \in \mathrm{Int}(\mathbb{Z})$$

be irreducible in $\mathrm{Int}(\mathbb{Z})$ where $b > 1$ is a natural number. We call non-empty subsets $J_1, J_2 \subsetneqq I$ *interchangeable* if $J_1 \cap J_2 = \emptyset$ and

$$\mathsf{d}\left(\prod_{i \in J_1} g_i(x) \cdot \prod_{i \in I \setminus J_2} g_i(x)\right) = \mathsf{d}\left(\prod_{i \in J_2} g_i(x) \cdot \prod_{i \in I \setminus J_1} g_i(x)\right) = (b).$$

(ii) We call two non-empty disjoint index sets $J_1, J_2 \subsetneqq I$ *element-disjoint* if

$$\{g_i \mid i \in J_1\} \cap \{g_j \mid j \in J_2\} = \emptyset.$$

**Example 3.6.2.** Consider the irreducible polynomial

$$f = \frac{(x-1)(x-3)(x^2+4)}{4} \in \mathrm{Int}(\mathbb{Z}).$$

A quick check shows that

$$\mathsf{d}((x-1)^2(x^2+4)) = \mathsf{d}((x-3)^2(x^2+4)) = (4).$$

Thus setting $g_1 = x-1, g_2 = x-3$ and $g_3 = x^2+4$, we see that the subsets $J_1 = \{1\}$ and $J_2 = \{2\}$ of $I = \{1,2,3\}$ are interchangeable. Furthermore, $J_1$ and $J_2$ are element-disjoint since they contain different elements.

**Lemma 3.6.3.** *Let $f(x) = \frac{\prod_{i\in I} g_i(x)}{b} \in \mathrm{Int}(\mathbb{Z})$ be irreducible in $\mathrm{Int}(\mathbb{Z})$, where $b > 1$ is a natural number, $I \neq \emptyset$ is a finite set and for $i \in I$, $g_i \in \mathbb{Z}[x]$ is primitive and irreducible in $\mathbb{Z}[x]$.*

*If there exist two element-disjoint interchangeable subsets $J_1, J_2 \subsetneq I$, then $f$ is not absolutely irreducible.*

**Proof.** Suppose $J_1, J_2 \subsetneq I$ are element-disjoint and interchangeable. Then for $k \geq 2$,

$$f^k = \frac{\prod_{i\in J_1} g_i(x) \prod_{i\in I\setminus J_2} g_i(x)}{b} \frac{\prod_{i\in J_2} g_i(x) \prod_{i\in I\setminus J_1} g_i(x)}{b} \underbrace{\frac{\prod_{i\in I} g_i(x)}{b} \cdots \frac{\prod_{i\in I} g_i(x)}{b}}_{k-2 \text{ copies}}$$

implies the existence of a factorization of $f^k$ essentially different from $\underbrace{f \cdots f}_{k \text{ copies}}$. □

The next lemma tells us that we cannot have interchangeable subsets in the case when the fixed divisor $b$ of the numerator of $f$ is a prime $p$. We begin with a supporting definition.

**Definition 3.6.4.** Let $I \neq \emptyset$ be a finite set and for $i \in I$, let $f_i \in \mathbb{Z}[x]$ be primitive and irreducible in $\mathbb{Z}[x]$. Let $p$ be a prime dividing $\mathsf{d}\left(\prod_{i\in I} f_i\right)$. We say $f_k$ is *indispensable for $p$* (among the polynomials $f_i$ with $i \in I$) if there exists an integer $z$ such that $\mathsf{v}_p(f_k(z)) > 0$ and $\mathsf{v}_p(f_i(z)) = 0$ for all $i \neq k$. We call such a $z$ a *witness* for $f_k$ being indispensable for $p$.

**Example 3.6.5.** Consider the polynomials $f_1 = x, f_2 = x-1$ and $f_3 = x-2$ in $\mathbb{Z}[x]$. It is easy to check that $\mathsf{d}(x(x-1)(x-2)) = 6$. Now note that $f_2 = x-1$ is indispensable for 2 since for all odd numbers $a$,

$$\mathsf{v}_2(f_2(a)) = \mathsf{v}_2(a-1) > 0 \text{ and } \mathsf{v}_2(f_1(a)) = \mathsf{v}_2(f_3(a)) = 0.$$

In this case any odd number is a witness for $x-1$ being indispensable for 2. On the other hand, $x$ and $x-2$ are not indispensable for 2 since for any even number $b$,

$$\mathsf{v}_2(f_1(b)) = \mathsf{v}_2(b) > 0 \text{ and } \mathsf{v}_2(f_3(b)) = \mathsf{v}_2(b-2) > 0.$$

**Lemma 3.6.6.** *Let $I \neq \emptyset$ be a finite set and for $i \in I$, let $g_i \in \mathbb{Z}[x]$ be primitive and irreducible in $\mathbb{Z}[x]$. Let*

$$f(x) = \frac{\prod_{i \in I} g_i(x)}{p} \in \mathrm{Int}(\mathbb{Z})$$

*be irreducible in* $\mathrm{Int}(\mathbb{Z})$. *Then there do not exist interchangeable subsets of $I$.*

**Proof.** Suppose $J_1, J_2 \subsetneq I$ are disjoint. Now since $f$ is irreducible, every $g_i$ for $i \in I$ is indispensable for $p$ and this implies that $g_i \neq g_j$ for $i \neq j$. Thus $J_1$ and $J_2$ being disjoint, are element-disjoint. Furthermore, if $r_i$ is a witness for $g_i$ being indispensable for $p$, then

$$\mathsf{v}_p\left(\prod_{j \in I \setminus \{i\}} g_j(r_i)\right) = 0.$$

Now suppose $g_k$ for $k \in J_1$ is indispensable for $p$ with witness $r_k$. Then, since $J_1$ and $J_2$ are element-disjoint, it follows that

$$\mathsf{v}_p\left(\prod_{j \in (I \setminus J_1)} g_j(r_k) \cdot \prod_{j \in J_2} g_j(r_k)\right) = 0.$$

Thus $\mathsf{d}\left(\prod_{j \in (I \setminus J_1)} g_j(x) \cdot \prod_{j \in J_2} g_j(x)\right)$ is not divisible by $p$. This shows that $J_1, J_2$ are not interchangeable because if they were, we would have

$$\mathsf{d}\left(\prod_{j \in (I \setminus J_1)} g_j(x) \cdot \prod_{j \in J_2} g_j(x)\right) = (p).$$

$\square$

The next lemma generalizes Example 3.4.1. In Example 3.4.1, setting $g_0 = c(x)$, $g_1 = d(x)$ and $g_i = x - a_{i-1}$ for $i = 2, \ldots, m+1$, we can choose $\{0,1\}$ for the index set $J$ in Lemma 3.6.7.

**Lemma 3.6.7.** *Let $I \neq \emptyset$ be a finite set and for $i \in I$, let $g_i \in \mathbb{Z}[x]$ be primitive and irreducible in $\mathbb{Z}[x]$. Suppose*

$$f = \frac{\prod_{i \in I} g_i(x)}{b} \in \mathrm{Int}(\mathbb{Z})$$

*is irreducible in* $\mathrm{Int}(\mathbb{Z})$, *where $b > 1$. Let $\mathbb{P}$ be the set of prime divisors of $b$ and $b = \prod_{p \in \mathbb{P}} p^{e_p}$ be the prime factorization of $b$ with $e_p \in \mathbb{N}$. If there exists a subset $\emptyset \neq J \subsetneq I$ such that for all $p \in \mathbb{P}$, for every integer $s$ that is a root mod $p$ of $\prod_{j \in J} g_j$, we have*

$$\mathsf{v}_p\left(\prod_{j \in J} g_j(s)\right) > e_p, \tag{3.6.1}$$

*then $f$ is not absolutely irreducible.*

**Proof.** Suppose there exists $\emptyset \neq J \subsetneq I$ such that for all $p \in \mathbb{P}$, inequality 3.6.1 is satisfied. Let $n = \max\{e_p \mid p \in \mathbb{P}\}$. We claim that $f^{n+1}$ has a factorization essentially different from $f \cdots f$. The existence of such a factorization follows from 3.6.2 below.

$$f^{n+1} = \frac{\left(\prod_{j\in J} g_j(x)\right)^n \left(\prod_{i\in I\setminus J} g_i(x)\right)^{n+1}}{b^{n+1}} \cdot \prod_{j\in J} g_j(x). \tag{3.6.2}$$

To see that the factor on the left is integer-valued, let $p \in \mathbb{P}$ and $s \in \mathbb{Z}$. If $s$ is a root mod $p$ of $\prod_{j\in J} g_j$, then

$$\mathsf{v}_p\left(\left(\prod_{j\in J} g_j(s)\right)^n\right) \geq n(e_p+1) = ne_p + n \geq (n+1)e_p = \mathsf{v}_p(b^{n+1})$$

On the other hand, if $s$ is not a root mod $p$ of $\prod_{j\in J} g_j$, then

$$\mathsf{v}_p\left(\left(\prod_{j\in J} g_j(s)\right)^n \left(\prod_{i\in I\setminus J} g_i(s)\right)^{n+1}\right) = \mathsf{v}_p\left(\left(\prod_{i\in I} g_i(s)\right)^{n+1}\right) \geq \mathsf{v}_p(b^{n+1}).$$

Finally, that the factorization 3.6.2 can be refined to a factorization into irreducibles (necessarily essentially different from $f \cdots f$) follows from the fact that $\mathrm{Int}(\mathbb{Z})$ is atomic. $\square$

We generalize Examples 3.4.2 and 3.4.4 in the next lemma. In Example 3.4.2, setting $g_0 = x^4 + x^3 + 8$ and $g_1 = x - 3$, the index set $J$ in Lemma 3.6.8 was $\{0\}$.

**Lemma 3.6.8.** *Let $I \neq \emptyset$ be a finite set and for $i \in I$, let $g_i \in \mathbb{Z}[x]$ be primitive and irreducible in $\mathbb{Z}[x]$. Suppose*

$$f(x) = \frac{\prod_{i\in I} g_i(x)}{p^n} \in \mathrm{Int}(\mathbb{Z})$$

*is irreducible in $\mathrm{Int}(\mathbb{Z})$, where $p$ is a prime and $n > 1$.*

*If there exists $J \subsetneq I$ such that the following holds:*

*(i) $\mathbb{Z} = S \uplus T$ where $S$ and $T$ are each a union of residue classes mod $p$ and such that*

$$\mathsf{v}_p\left(gcd\left(\prod_{i\in J} g_i(a) \,\middle|\, a \in S\right)\right) > n \text{ and } \forall\ t \in T,\ \mathsf{v}_p\left(gcd\left(\prod_{i\in J} g_i(b) \,\middle|\, b \in t + p\mathbb{Z}\right)\right) = e,$$

*with* $1 \leq e < n$*, and for all* $t \in T$

$$\mathsf{v}_p\left(gcd\left(\prod_{i\in J} g_i(b) \,\middle|\, b \in t + p\mathbb{Z}\right)\right) + \mathsf{v}_p\left(gcd\left(\prod_{i\in I\setminus J} g_i(b) \,\middle|\, b \in t + p\mathbb{Z}\right)\right) \geq n. \tag{3.6.3}$$

*Then* $f$ *is not absolutely irreducible.*

**Proof.** Suppose there exists a subset $J \subsetneq I$ such that (i) holds.

It follows from inequality (3.6.3) and $f$ being irreducible that

$$\min_{t\in T}\left\{\mathsf{v}_p\left(gcd\left(\prod_{i\in I\setminus J} g_i(b) \,\middle|\, b \in t + p\mathbb{Z}\right)\right)\right\} = n - e.$$

Now let

$$m = \mathsf{v}_p\left(gcd\left(\prod_{i\in J} g_i(a) \,\middle|\, a \in S\right)\right) > n.$$

We set $k = m - e$ and claim that $f^k$ has a factorization essentially different from $f \cdots f$. This factorization follows from

$$f^k = \frac{\left(\prod_{i\in J} g_i\right)^{n-e}\left(\prod_{i\in I\setminus J} g_i\right)^k}{p^{(n-e)m}} \cdot \left(\frac{\prod_{i\in J} g_i}{p^e}\right)^{m-n}.$$

In fact, for each $t \in T$, let

$$l = \mathsf{v}_p\left(gcd\left(\prod_{i\in J} g_i(b) \,\middle|\, b \in t + p\mathbb{Z}\right)^{n-e}\right) + \mathsf{v}_p\left(gcd\left(\prod_{i\in I\setminus J} g_i(b) \,\middle|\, b \in t + p\mathbb{Z}\right)^k\right).$$

Then $l = e(n-e) + k(n-e) = e(n-e) + (m-e)(n-e) = (n-e)m$.

Furthermore

$$\mathsf{v}_p\left(gcd\left(\prod_{i\in J} g_i(a) \,\middle|\, a \in S\right)^{n-e}\right) = (n-e)m.$$

Moreover, $k - (n-e) = m - n$ and $(n-e)m + (m-n)e = (m-e)n = kn$. □

# 4. A graph-theoretic criterion for absolute irreducibility of integer-valued polynomials with square-free denominator

This chapter consists of article [31] titled, "A graph-theoretic criterion for absolute irreducibility of integer-valued polynomials with square-free denominator". The article appeared in *Communications in Algebra* in April 2020 and it is joint work with Sophie Frisch.


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



**Keywords:** Factorization, non-unique factorization, irreducible elements, absolutely irreducible elements, atom, atomic domain, integer-valued polynomials, simple graphs, connected graphs.

**2010 Mathematics Subject Classification:** 13A05, 13B25, 13F20, 11R09, 11C08, 13P05


## 4.1. 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 [13, 36, 43, 47, 56].

For rings of integers in number fields, their existence actually characterizes non-unique factorization, as Chapman and Krause [24] 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 $K$ its quotient field.

In an earlier paper [32, 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 4.2.1. This 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 4.2.2, 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 4.3.1.

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

$$r = a_1 \cdots a_n \tag{4.1.1}$$

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 $r \sim s$.

(iv) Two factorizations into irreducibles of the same element,

$$r = a_1 \cdots a_n = b_1 \cdots b_m, \tag{4.1.2}$$

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 (4.1.2) are called *essentially different*.

**Definition 4.1.1.** Let $R$ be a commutative ring with identity. An irreducible element $c \in R$ is called *absolutely irreducible* (or, a *strong atom*), if for all natural numbers $n$, every factorization of $c^n$ is essentially the same as $c^n = c \cdots c$.

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 4.1.2.** 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 4.1.3.** 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 4.1.4.** Let $D$ be a principal ideal domain with quotient field $K$, and $f \in K[x]$ written in standard form as in Definition 4.1.2. Then $f$ is in $\mathrm{Int}(D)$ if and only if $b$ divides $\mathsf{d}\left(\prod_{i\in I} g_i\right)$.

**Remark 4.1.5.** 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 4.1.2) is an image-primitive element of $\mathrm{Int}(D)$ if and only if (up to multiplication by units) $a = 1$ and $b = \mathsf{d}\left(\prod_{i\in I} g_i\right)$.

**Definition 4.1.6.** Let $D$ be a principal ideal domain. For $f \in \mathrm{Int}(D)$, and $p$ a prime element in $D$, we let

$$\mathsf{d}_p(f) = \mathsf{v}_p\left(\mathsf{d}(f)\right)$$

**Remark 4.1.7.** By the above definition,

$$\mathsf{d}(f) = \prod_{p \in \mathbb{P}} p^{\mathsf{d}_p(f)} \quad \text{and} \quad \mathsf{d}_p(f) = \min_{c \in D} \mathsf{v}_p(f(c))$$

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 $n \in \mathbb{N}$.

## 4.2. Graph-theoretic irreducibility criteria

We refer to, for instance, [14] for the graph theory terms we use in this section.

**Definition 4.2.1.** 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 $p \in D$ a 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 $\mathsf{v}_p\left(g_i(w)\right) > 0$ and $\mathsf{v}_p\left(g_j(w)\right) = 0$ 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 $\mathsf{v}_p\left(g_i(w)\right) = \mathsf{v}_p\left(\mathsf{d}(g)\right)$ and $\mathsf{v}_p\left(g_j(w)\right) = 0$ 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 4.2.2.** 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 4.2.3.** Let $D$ be a principal ideal domain, $I \neq \emptyset$ 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 $p$ among the $g_k$ with $k \in I$.

(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 $p$ among the $g_k$ with $k \in I$.

**Example 4.2.4.** Let $I = \{1,2,3,4\}$ and for $i \in I$, $g_i \in \mathbb{Z}[x]$ as follows:
$g_1 = x^3 - 19$, $g_2 = x^2 + 9$, $g_3 = x^2 + 1$, $g_4 = x - 5$, and set

$$g = (x^3 - 19)(x^2 + 9)(x^2 + 1)(x - 5).$$

A quick check shows that the fixed divisor of $g$ is 15.

(i) Taking $w = 1,2,0$ respectively, as witnesses, we see that $g_2, g_3, g_4$ are quintessential for 5. The polynomial $g_1$ is not essential for 5 because $\mathsf{v}_5(g_1(a)) > 0$ only if $a \in 4 + 5\mathbb{Z}$ and for such $a$, also $\mathsf{v}_5(g_2(a)) > 0$.

(ii) Taking $w = 1,0,2$ respectively, as witnesses, we see that $g_1, g_2, g_4$ are essential for 3. Only $g_4$ is quintessential for 3. The polynomial $g_3$ is not essential for 3.

Figure 4.1 shows the essential and quintessential graphs of $(g_1, g_2, g_3, g_4)$.


**Figure 4.1:** Graphs for Example 4.2.4

**Lemma 4.2.5.** *Let $D$ be a principal ideal domain and $f \in \text{Int}(D)$ a non-constant image-primitive integer-valued polynomial, written in standard form according to Definition 4.1.2 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 $h \in \text{Int}(D)$ 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 4.1.7). So, $f^n$ is image-primitive, and, therefore, all polynomials in $\text{Int}(D)$ dividing $f^n$ are image-primitive. Let $f^n = hk$ with $h, k \in \text{Int}(D)$. When $h$ is written in standard form as in Definition 4.1.2, 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 4.1.5.

Now let $q \in D$ be prime and $j \in I$ such that $g_j$ is quintessential for $q$. Note that, by Remark 4.2.2 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 the following equalities and inequalities of the exponents:

(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 4.2.2.

To see (iii), consider a witness $w$ for $g_j$ being quintessential for $q$. Since $f$ is image-primitive, $e_q = \mathsf{v}_q(\mathsf{d}(\prod_{i\in I} g_i))$, by Remark 4.1.5. From Definition 4.2.1 and Remark 4.1.4 we deduce

$$e_q\gamma_j(h) = \mathsf{v}_q\left(g_j(w)\right)\gamma_j(h) = \mathsf{v}_q\left(g_j^{\gamma_j(h)}(w)\right) = \mathsf{v}_q\left(\prod_{i\in I} g_i(w)^{\gamma_i(h)}\right) \geq \beta_q(h)$$

(and similarly for $k$ instead of $h$).

Finally, (i) - (iii) together imply $e_q\gamma_j(h) = \beta_q(h)$ and $e_q\gamma_j(k) = \beta_q(k)$. □

**Theorem 4.2.1.** *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 $p_0$ in $D$ dividing $b$, $g_{i_0}$ and $g_{i_1}$ are both essential for $p_0$. As $g_i$ is essential for $p_0$, $p_0$ cannot divide any $b_k$ with $k \neq 1$ and, hence, $p_0$ divides $b_1$. For any $g_k$ essential for $p_0$ it follows that $k \in I_1$, and, in particular, $i_1 \in I_1$. The same argument with reference to a prime $p_k$ for which both $g_{i_k}$ and $g_{i_{k+1}}$ are essential, 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 4.2.2.** *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 $0 \leq m_l(i) \leq n$, $0 \leq k_l(p) \leq n e_p$ and for all $i$, $\sum_{l=1}^{s} m_l(i) = n$ and for all $p$, $\sum_{l=1}^{s} k_l(p) = n e_p$.

Fix $t$ with $1 \leq t \leq s$. 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 4.2.5, $g_{i_h}$ 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 4.1.5) and, hence, $f_t$ is a power of $f$. Since $f_t$ is irreducible, $f_t = f$. □

**Example 4.2.6.** 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 $\mathrm{Int}(\mathbb{Z})$, by Theorem 4.2.2.

The converse of Theorem 4.2.2 does not hold in general. For instance, the polynomial

$$f = \frac{x^2(x^2+3)}{4} \in \mathrm{Int}(\mathbb{Z})$$

is absolutely irreducible in $\mathrm{Int}(\mathbb{Z})$ but the quintessential graph of $(x, x, x^2+3)$ is not connected.

There is, however, a converse to Theorem 4.2.2 in the special case where the denominator of $f$ is square-free, as we now proceed to show, cf. Theorem 4.3.1.

## 4.3. Absolutely irreducible polynomials with square-free denominator

Let $D$ be a principal ideal domain with quotient field $K$. When we talk of the denominator of a polynomial in $K[x]$, this refers to the standard form of a polynomial introduced in Definition 4.1.2.

**Remark 4.3.1.** Let $D$ be a principal ideal domain. Suppose the denominator of $f \in \mathrm{Int}(D)$, written in standard form as in Definition 4.1.2, is square-free:

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

Then, if $f$ is irreducible in $\mathrm{Int}(D)$, it follows that each $g_i$ is essential for some $p \in T$. Otherwise, we can split off $g_i$. This further implies $g_i \not\sim g_j$ in $D[x]$ for $i \neq j$, whenever $f \in \mathrm{Int}(D)$ with square-free denominator is irreducible. A criterion for irreducibility of an integer-valued polynomial with square-free denominator has been given by Peruginelli [52].

**Theorem 4.3.1.** *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 $D[x]$.*

*Let $G$ be the quintessential graph of $(g_i \mid i \in I)$ as in Definition 4.2.3.*

*Then $f$ is absolutely irreducible if and only if $G$ is connected.*

**Proof.** In view of Theorem 4.2.2, we only need to show necessity. If $|I| = 1$, then $G$ is connected. Now assume $|I| > 1$, and suppose $G$ is not connected. We show that $f$ is not absolutely irreducible. If $f$ is not even irreducible, we are done. So suppose $f$ is irreducible. This implies $g_i \not\sim g_j$ in $D[x]$ for $i \neq j$, by Remark 4.3.1. Since $G$ is not connected, $I$ is a 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 $j \in J_2$.

We express $T$ as a disjoint union of $T_1$ and $T_2$ by assigning every $p \in T$ for which some $g_i$ with $i \in J_1$ is quintessential to $T_1$, every $p \in T$ for which some $g_i$ with $i \in J_2$ is quintessential to $T_2$, and assigning each $p \in T$ for which no $g_i$ is quintessential to $T_1$ or $T_2$ arbitrarily. (It may happen that $T_1 = \emptyset$ and $T_2 = T$ or vice versa).

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. [17]), each of the two factors above can further be factored into irreducibles. Since $J_1$ and $J_2$ are both non-empty and $g_i \not\sim g_j$ in $D[x]$ (and hence, $g_i \not\sim g_j$ in $K[x]$) for $i \neq j$, it is clear that the resulting factorization of $f^3$ into irreducibles is essentially different from $f \cdot f \cdot f$. □

**Remark 4.3.2.** Let $D$ be a principal ideal domain. The proof of Theorem 4.3.1 shows that any non-absolutely irreducible element $f \in \mathrm{Int}(D)$ with square-free denominator exhibits non-unique factorization of $f^n$ already for $n = 3$.

If $f(x) = \prod_{i\in I} g_i(x)/p$, where $D$ is a principal ideal domain, $p$ a prime of $D$ and each $g_i \in D[x]$ primitive and irreducible in $D[x]$, then it is easy to see that $f$ is an irreducible element of $\mathrm{Int}(D)$ if and only if

(i) $\mathsf{d}\left(\prod_{i\in I} g_i(x)\right) = p$ and

(ii) each $g_i$ is essential for $p$, that is, for each $i \in I$ there exists $w_i \in D$ such that $\mathsf{v}_p\left(g_i(w_i)\right) > 0$ and $\mathsf{v}_p\left(g_j(w_i)\right) = 0$ for all $j \in I \setminus \{i\}$.

An analogous statement relates absolutely irreducible integer-valued polynomials with prime denominator to quintessential irreducible factors of the numerator:

**Corollary 4.3.3.** *Let $D$ be a principal ideal domain, $p \in D$ a prime, 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*

*(i) $\mathsf{d}\left(\prod_{i\in I} g_i(x)\right) = p$ and*

*(ii) each $g_i$ is quintessential for $p$ among the $g_i$ with $i \in I$, that is, for each $i \in I$ there exists $w_i \in D$ such that $\mathsf{v}_p\left(g_i(w_i)\right) = 1$ and $\mathsf{v}_p\left(g_j(w_i)\right) = 0$ for all $j \in I \setminus \{i\}$.*

**Proof.** If $\mathsf{d}\left(\prod_{i\in I} g_i(x)\right) = p$, then $f \in \mathrm{Int}(D)$ with $\mathsf{d}(f) = 1$, and Theorem 4.3.1 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 4.3.1 applies. Now the statement follows from the fact that, whenever $\mathsf{d}\left(\prod_{i\in I} g_i(x)\right) = p$ is prime, the quintessential graph of $(g_i \mid i \in I)$ is connected if and only if every $g_i$ is quintessential for $p$. □

We conclude by an example of how to apply Theorem 4.3.1:

**Example 4.3.4.** The following polynomial $f \in \operatorname{Int}(\mathbb{Z})$ is irreducible, by Theorem 4.2.1; but not absolutely irreducible, by Theorem 4.3.1:

$$f = \frac{(x^3-19)(x^2+9)(x^2+1)(x-5)}{15}$$

This is so because the essential graph of $(x^3-19, x^2+9, x^2+1, x-5)$ is connected, but the quintessential graph is not connected, see Example 4.2.4 and Figure 4.1.

# A. Appendix

This appendix consists of factorization terms and results from [36] that we refer to in Section 2.5. We only state the items we need in this thesis and refer to [36] for the full results and their proofs.

**Definition A.0.1.** Let $H, B$ be monoids. A map $\varphi : H \longrightarrow B$ is called a monoid homomorphism if:

(i) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in H$.

(ii) $\varphi(1_H) = 1_B$.

**Definition A.0.2.** [36, Definition 3.2.1] A monoid homomorphism $\theta : H \longrightarrow B$ is called a *transfer homomorphism* if it satisfies the following properties:

(i) $B = \theta(H)B^\times$ and $\theta^{-1}(B^\times) = H^\times$.

(ii) If $u \in H, b, c \in B$ and $\theta(u) = bc$, then there exist $v, w \in H$ such that $u = vw, \theta(v) \sim b$ and $\theta(w) \sim c$,

where $B^\times$ and $H^\times$ are the units of $B$ and $H$ respectively.

In the next proposition, we state parts of [36, Proposition 3.2.3] that we need in this thesis. First recall that the *set of lengths* of a non-zero non-unit $a \in H$ is the set $L(a)$ of all natural numbers $n$ such that $a$ has a factorization of length $n$.

**Proposition A.0.3.** *Let $\theta : H \longrightarrow B$ be a transfer homomorphism and $a \in H$. Then the following hold:*

*(i) $a$ is an atom of $H$ if and only if $\theta(a)$ is an atom $B$.*

*(ii) $H$ is atomic if and only if $B$ is atomic.*

*(iii) If $H$ is atomic, then $L(a) = L(\theta(a))$, $H$ and $B$ have the same elasticity, and $H$ is a BF-monoid if and only if $B$ is a BF-monoid.*

**Definition A.0.4.** (i) Let $G$ be an additively written abelian group and $G_0 \subseteq G$ a nonempty subset. Let $\mathcal{F}(G_0)$ denote the free abelian monoid with basis $G_0$.

(ii) The elements of $\mathcal{F}(G_0)$ are called *sequences* over $G_0$ and are of the form

$$S = \prod_{g \in G_0} g^{n_g}$$

where $n_g = v_g(S) \in \mathbb{N} \cup \{0\}$, $n_g = 0$ for almost all $g \in G_0$.

(iii) The *length* of a sequence $S$ is

$$|S| = \sum_{g \in G_0} v_g(S) \quad \in \ \mathbb{N} \cup \{0\}$$

and the *sum* of $S$ is

$$\sigma(S) = \sum_{g \in G_0} v_g(S) g \quad \in \ G$$

(iv) The monoid

$$\mathcal{B}(G_0) = \left\{ S \in \mathcal{F}(G_0) \;\middle|\; \sigma(S) = 0 \right\}$$

is called the *block monoid* over $G_0$ or the *monoid of zero-sum sequences.*

**Lemma A.0.5.** *[36, Lemma 6.4.4.] Let $G$ be an additively written abelian group and $G^\bullet = G \setminus \{0\}$. Let $U, V$ be atoms of $\mathcal{B}(G^\bullet)$.*

*(i) $maxL(UV) \leq min\{|U|, |V|\}$.*

*(ii) $maxL(UV) = max\{|U|, |V|\}$ if and only if $V = -U$.*

*(iii) $|U| = max\{maxL(UU') \mid U'$ is an atom of $\mathcal{B}(G)\}$.*

**Definition A.0.6.** A commutative monoid $H$ is said to be a *transfer Krull monoid* (over $G_0$) if there exists a transfer homomorphism $\theta : H \longrightarrow \mathcal{B}(G_0)$ for a subset $G_0$ of an abelian group $G$.

# Bibliography


[1] Ahmet G. Ağargün, D. D. Anderson, and Silvia Valdes-Leon. "Factorization in commutative rings with zero divisors. III". *Rocky Mountain J. Math.* 31.1 (2001), pp. 1–21. ISSN: 0035-7596. DOI: 10.1216/rmjm/1008959664.

[2] D. D. Anderson, ed. *Factorization in integral domains.* Vol. 189. Lecture Notes in Pure and Applied Mathematics. Marcel Dekker, Inc., New York, 1997, pp. x–432. ISBN: 0-8247-0032-5.

[3] D. D. Anderson, David F. Anderson, and Muhammad Zafrullah. "Factorization in integral domains". *J. Pure Appl. Algebra* 69.1 (1990), pp. 1–19. ISSN: 0022-4049. DOI: 10.1016/0022-4049(90)90074-R.

[4] D. D. Anderson, David F. Anderson, and Muhammad Zafrullah. "Factorization in integral domains. II". *J. Algebra* 152.1 (1992), pp. 78–93. ISSN: 0021-8693. DOI: 10.1016/0021-8693(92)90089-5.

[5] D. D. Anderson, David F. Anderson, and Muhammad Zafrullah. "Rings between $D[X]$ and $K[X]$". *Houston J. Math.* 17.1 (1991), pp. 109–129. ISSN: 0362-1588.

[6] D. D. Anderson and Silvia Valdes-Leon. "Factorization in commutative rings with zero divisors". *Rocky Mountain J. Math.* 26.2 (1996), pp. 439–480. ISSN: 0035-7596. DOI: 10.1216/rmjm/1181072068.

[7] D. D. Anderson and Silvia Valdes-Leon. "Factorization in commutative rings with zero divisors. II". *Factorization in integral domains (Iowa City, IA, 1996).* Vol. 189. Lecture Notes in Pure and Appl. Math. Dekker, New York, 1997, pp. 197–219.

[8] David F. Anderson. "Elasticity of factorizations in integral domains: a survey". *Factorization in integral domains (Iowa City, IA, 1996).* Vol. 189. Lecture Notes in Pure and Appl. Math. Dekker, New York, 1997, pp. 1–29.

[9] David F. Anderson and David Dobbs. *Zero-dimensional commutative rings.* Vol. 171. CRC Press, 1995.

[10] David F. Anderson and Driss Nour El Abidine. "Factorization in integral domains. III". *J. Pure Appl. Algebra* 135.2 (1999), pp. 107–127. ISSN: 0022-4049. DOI: 10.1016/S0022-4049(97)00147-3.

[11] David F. Anderson et al. "Some factorization properties of the ring of integer-valued polynomials". *Zero-dimensional commutative rings (Knoxville, TN, 1994)*. Vol. 171. Lecture Notes in Pure and Appl. Math. Dekker, New York, 1995, pp. 125–142.

[12] Austin Antoniou, Sarah Nakato, and Roswitha Rissner. "Irreducible polynomials in Int($\mathbb{Z}$)". *ITM Web Conf.* 20:01004 (2018). DOI: 10.1051/itmconf/20182001004.

[13] Paul Baginski and Ross Kravitz. "A new characterization of half-factorial Krull monoids". *J. Algebra Appl.* 9.5 (2010), pp. 825–837. ISSN: 0219-4988. DOI: 10.1142/S0219498810004269.

[14] J. A. Bondy and U. S. R. Murty. *Graph theory*. Vol. 244. Graduate Texts in Mathematics. Springer, New York, 2008, pp. xii–651. ISBN: 978-1-84628-969-9. DOI: 10.1007/978-1-84628-970-5. URL: https://doi.org/10.1007/978-1-84628-970-5.

[15] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Translated from French, Reprint of the 1989 English translation. Springer-Verlag, Berlin, 1998, pp. xxiv–625. ISBN: 3-540-64239-0.

[16] Paul-Jean Cahen. "Integer-valued polynomials on a subset". *Proc. Amer. Math. Soc.* 117.4 (1993), pp. 919–929. ISSN: 0002-9939. DOI: 10.2307/2159516.

[17] Paul-Jean Cahen and Jean-Luc Chabert. "Elasticity for integral-valued polynomials". *J. Pure Appl. Algebra* 103.3 (1995), pp. 303–311. ISSN: 0022-4049. DOI: 10.1016/0022-4049(94)00108-U.

[18] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*. Vol. 48. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 1997, pp. xx–322. ISBN: 0-8218-0388-3.

[19] Paul-Jean Cahen and Jean-Luc Chabert. "What you should know about integer-valued polynomials". *Amer. Math. Monthly* 123.4 (2016), pp. 311–337. ISSN: 0002-9890. DOI: 10.4169/amer.math.monthly.123.4.311.

[20] Paul-Jean Cahen and Jean-Luc Chabert. "What's new about integer-valued polynomials on a subset?" *Non-Noetherian commutative ring theory*. Vol. 520. Math. Appl. Kluwer Acad. Publ., Dordrecht, 2000, pp. 75–96.

[21] Paul-Jean Cahen, Jean-Luc Chabert, and Sophie Frisch. "Interpolation domains". *J. Algebra* 225.2 (2000), pp. 794–803. ISSN: 0021-8693. DOI: 10.1006/jabr.1999.8151.

[22] Leonard Carlitz. "A characterization of algebraic number fields with class number two". *Proc. Amer. Math. Soc.* 11 (1960), pp. 391–392. ISSN: 0002-9939. DOI: 10.2307/2034782.

[23] Scott T. Chapman and Jim Coykendall. "Half-factorial domains, a survey". *Non-Noetherian commutative ring theory*. Vol. 520. Math. Appl. Kluwer Acad. Publ., Dordrecht, 2000, pp. 97–115.

[24] Scott T. Chapman and Ulrich Krause. "A closer look at non-unique factorization via atomic decay and strong atoms". *Progress in commutative algebra 2*. Walter de Gruyter, Berlin, 2012, pp. 301–315.

[25] Scott T. Chapman and Barbara A. McClain. "Irreducible polynomials and full elasticity in rings of integer-valued polynomials". *J. Algebra* 293.2 (2005), pp. 595–610. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2005.01.026.

[26] Scott T. Chapman and William W. Smith. "Factorization in Dedekind domains with finite class group". *Israel J. Math.* 71.1 (1990), pp. 65–95. ISSN: 0021-2172. DOI: 10.1007/BF02807251.

[27] David Dobbs. *Advances in Commutative Ring Theory*. CRC Press, 1999.

[28] Yushuang Fan and Salvatore Tringali. "Power monoids: a bridge between factorization theory and arithmetic combinatorics". *J. Algebra* 512 (2018), pp. 252–294. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2018.07.010.

[29] Sophie Frisch. "A construction of integer-valued polynomials with prescribed sets of lengths of factorizations". *Monatsh. Math.* 171.3-4 (2013), pp. 341–350. ISSN: 0026-9255. DOI: 10.1007/s00605-013-0508-z.

[30] Sophie Frisch. "Integer-valued polynomials on algebras: a survey". *Actes des rencontres du CIRM* 2.2 (2010), pp. 27–32. DOI: 10.5802/acirm.30.

[31] Sophie Frisch and Sarah Nakato. "A graph-theoretic criterion for absolute irreducibility of integer-valued polynomials with square-free denominator". *Communications in Algebra* 0.0 (2020), pp. 1–8. DOI: 10.1080/00927872.2020.1744618.

[32] 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), pp. 231–249. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2019.02.040.

[33] Sophie Frisch. "Relative polynomial closure and monadically Krull monoids of integer-valued polynomials". *Multiplicative ideal theory and factorization theory*. Vol. 170. Springer Proc. Math. Stat. Springer, [Cham], 2016, pp. 145–157. DOI: 10.1007/978-3-319-38855-7_6.

[34] Alfred Geroldinger. "Sets of lengths". *Amer. Math. Monthly* 123.10 (2016), pp. 960–988. ISSN: 0002-9890. DOI: 10.4169/amer.math.monthly.123.10.960.

[35] Alfred Geroldinger and Franz Halter-Koch. "Arithmetical theory of monoid homomorphisms". *Semigroup Forum* 48.3 (1994), pp. 333–362. ISSN: 0037-1912. DOI: 10.1007/BF02573682.

[36] Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations*. Vol. 278. Pure and Applied Mathematics (Boca Raton). Algebraic, combinatorial and analytic theory. Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xxii–700. ISBN: 978-1-58488-576-4; 1-58488-576-9. DOI: 10.1201/9781420003208.

[37] Alfred Geroldinger, Wolfgang A. Schmid, and Qinghai Zhong. "Systems of sets of lengths: transfer Krull monoids versus weakly Krull monoids". *Rings, polynomials, and modules*. Springer, Cham, 2017, pp. 191–235.

[38] Alfred Geroldinger and Emil D. Schwab. "Sets of lengths in atomic unit-cancellative finitely presented monoids". *Colloq. Math.* 151.2 (2018), pp. 171–187. ISSN: 0010-1354. DOI: 10.4064/cm7242-6-2017.

[39] Robert Gilmer. "Zero-dimensionality and products of commutative rings". *Zero-dimensional commutative rings (Knoxville, TN, 1994)*. Vol. 171. Lecture Notes in Pure and Appl. Math. Dekker, New York, 1995, pp. 15–25.

[40] Franz Halter-Koch. "Finitely generated monoids, finitely primary monoids, and factorization properties of integral domains". *Factorization in integral domains (Iowa City, IA, 1996)*. Vol. 189. Lecture Notes in Pure and Appl. Math. Dekker, New York, 1997, pp. 31–72.

[41] Franz Halter-Koch. "Finiteness theorems for factorizations". *Semigroup Forum* 44.1 (1992), pp. 112–117. ISSN: 0037-1912. DOI: 10.1007/BF02574329.

[42] Franz Halter-Koch. "Non-unique factorizations of algebraic integers". *Funct. Approx. Comment. Math.* 39.part 1 (2008), pp. 49–60. ISSN: 0208-6573. DOI: 10.7169/facm/1229696553.

[43] J Kaczorowski. "A pure arithmetical characterization for certain fields with a given class group". *Colloq. Math.* 45.2 (1981), pp. 327–330. ISSN: 0010-1354. DOI: 10.4064/cm-45-2-327-330.

[44] Florian Kainrath. "Factorization in Krull monoids with infinite class group". *Colloq. Math.* 80.1 (1999), pp. 23–30. ISSN: 0010-1354.

[45] K. Alan Loper. "A classification of all $D$ such that $\mathrm{Int}(D)$ is a Prüfer domain". *Proc. Amer. Math. Soc.* 126.3 (1998), pp. 657–660. ISSN: 0002-9939. DOI: 10.1090/S0002-9939-98-04459-1.

[46] Hideyuki Matsumura. *Commutative ring theory*. Second. Vol. 8. Cambridge Studies in Advanced Mathematics. Translated from the Japanese by M. Reid. Cambridge University Press, Cambridge, 1989, pp. xiv–320. ISBN: 0-521-36764-6.

[47] Sarah Nakato. "Non-absolutely irreducible elements in the ring of integer-valued polynomials". *Communications in Algebra* 48.4 (2020), pp. 1789–1802. DOI: 10.1080/00927872.2019.1705474.

[48] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Third. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004, pp. xii–708. ISBN: 3-540-21902-1. DOI: 10.1007/978-3-662-07001-7.

[49] Władysław Narkiewicz. "Some unsolved problems". *Colloque de Théorie des Nombres (Univ. Bordeaux, Bordeaux, 1969)*. 1971, 159–164. Bull. Soc. Math. France, Mém. No. 25. DOI: 10.24033/msmf.48.

[50] Władysław Narkiewicz. *The story of algebraic numbers in the first half of the 20th century*. Springer Monographs in Mathematics. From Hilbert to Tate. Springer, Cham, 2018, pp. xi–443. ISBN: 978-3-030-03753-6; 978-3-030-03754-3.

[51] Alexander Ostrowski. "Über ganzwertige Polynome in algebraischen Zahlkörpern". *J. Reine Angew. Math.* 149 (1919), pp. 117–124. ISSN: 0075-4102. DOI: 10.1515/crll.1919.149.117.

[52] Giulio Peruginelli. "Factorization of integer-valued polynomials with square-free denominator". *Comm. Algebra* 43.1 (2015), pp. 197–211. ISSN: 0092-7872. DOI: 10.1080/00927872.2014.897563.

[53] Georg Pólya. "Über ganzwertige Polynome in algebraischen Zahlkörpern". *J. Reine Angew. Math.* 149 (1919), pp. 97–116. ISSN: 0075-4102. DOI: 10.1515/crll.1919.149.97.

[54] Andreas Reinhart. "On monoids and domains whose monadic submonoids are Krull". *Commutative algebra*. Springer, New York, 2014, pp. 307–330.

[55] Moshe Roitman. "Polynomial extensions of atomic domains". *J. Pure Appl. Algebra* 87.2 (1993), pp. 187–199. ISSN: 0022-4049. DOI: 10.1016/0022-4049(93)90122-A.

[56] David E. Rush. "An arithmetic characterization of algebraic number fields with a given class group". *Math. Proc. Cambridge Philos. Soc.* 94.1 (1983), pp. 23–28. ISSN: 0305-0041. DOI: 10.1017/S0305004100060886.

[57] Pierre Samuel. "About Euclidean rings". *J. Algebra* 19 (1971), pp. 282–301. ISSN: 0021-8693. URL: https://doi.org/10.1016/0021-8693(71)90110-4.

[58] Daniel Smertnig. "Factorizations of elements in noncommutative rings: a survey". *Multiplicative ideal theory and factorization theory*. Vol. 170. Springer Proc. Math. Stat. Springer, [Cham], 2016, pp. 353–402. DOI: 10.1007/978-3-319-38855-7_15.

[59] Nicholas J. Werner. "Integer-valued polynomials on algebras: a survey of recent results and open questions". *Rings, polynomials, and modules*. Springer, Cham, 2017, pp. 353–375.

[60] Abraham Zaks. "Half factorial domains". *Bull. Amer. Math. Soc.* 82.5 (1976), pp. 721–723. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1976-14130-4.

[61] Abraham Zaks. "Half-factorial-domains". *Israel J. Math.* 37.4 (1980), pp. 281–302. ISSN: 0021-2172. DOI: 10.1007/BF02788927.