Springer Proceedings in Mathematics & Statistics

Alberto Facchini
Marco Fontana
Alfred Geroldinger
Bruce Olberding *Editors*

# Advances in Rings, Modules and Factorizations

Graz, Austria, February 19–23, 2018

Springer

# Springer Proceedings in Mathematics & Statistics

Volume 321

**Springer Proceedings in Mathematics & Statistics**

This book series features volumes composed of selected contributions from workshops and conferences in all areas of current research in mathematics and statistics, including operation research and optimization. In addition to an overall evaluation of the interest, scientific quality, and timeliness of each proposal at the hands of the publisher, individual contributions are all refereed to the high quality standards of leading journals in the field. Thus, this series provides the research community with well-edited, authoritative reports on developments in the most exciting areas of mathematical and statistical research today.

More information about this series at http://www.springer.com/series/10533

Alberto Facchini · Marco Fontana ·
Alfred Geroldinger · Bruce Olberding
Editors

# Advances in Rings, Modules and Factorizations

Graz, Austria, February 19–23, 2018

Springer

*Editors*
Alberto Facchini
Dipartimento di Matematica
"Tullio Levi-Civita"
Università degli Studi di Padova
Padua, Italy

Alfred Geroldinger
Institut für Mathematik und
Wissenschaftliches Rechnen
Universität Graz
Graz, Austria

Marco Fontana
Dipartimento di Matematica e Fisica
Università degli Studi Roma Tre
Rome, Italy

Bruce Olberding
Department of Mathematical Sciences
New Mexico State University
Las Cruces, NM, USA

ISSN 2194-1009 ISSN 2194-1017 (electronic)
Springer Proceedings in Mathematics & Statistics
ISBN 978-3-030-43415-1 ISBN 978-3-030-43416-8 (eBook)
https://doi.org/10.1007/978-3-030-43416-8

Mathematics Subject Classification (2010): 13A15, 13A50, 13B21, 13F15, 13G05, 13H99, 14H99, 16D25, 20M25



This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

This volume is occasioned by the conference *Rings and Factorizations* that took place at the University of Graz (Austria), February 19–23, 2018. The meeting featured five days of lectures on a range of topics that reflected new research trends in areas such as ideal theory (especially Prüfer, Krull, and Mori rings); topological methods in ring theory; rings of integer-valued polynomials; module theory and direct-sum decompositions; and factorization and divisibility theory in rings and semigroups. The conference continues a long tradition of international conferences in commutative ring theory, module theory and factorization theory that have been held in Austria, France, Italy, South Korea, Morocco and the United States.

The volume consists of invited, refereed research and expository articles from leading researchers in the fields represented at the conference. Most of the contributors to the volume were speakers at the conference. The diverse list of topics in the volume, like that of the lectures at the conference, represents areas of research that are expanding and transcending traditional boundaries between fields of study.

The conference *Rings and Factorizations* was organized by Alfred Geroldinger, Jun Seok Oh, Salvatore Tringali, and Qinghai Zhong. It was supported by the University of Graz, Institute for Mathematics and Scientific Computing, NAWI Graz, Federal State of Styria, and by the Austrian Science Fund FWF (Project Numbers P28864-N35 and W1230 Doctoral Program Discrete Mathematics). We thank all our sponsors. Without their assistance and support, the conference would not have been possible.

Finally, we thank the authors for their contributions, the referees for their work, and the editorial staff at Springer for their guidance and patience in directing this volume to its publication.

Padua, Italy — Alberto Facchini
Rome, Italy — Marco Fontana
Graz, Austria — Alfred Geroldinger
Las Cruces, NM, USA — Bruce Olberding
September 2019

# Contents

# Commutative Rings Whose Principal Ideals Have Unique Generators

**P. N. Ánh, Keith A. Kearnes, and Ágnes Szendrei**

**Abstract** We investigate the class of commutative unital rings in which principal ideals have unique generators. We prove that this class forms a finitely axiomatizable, relatively ideal distributive quasivariety, and also that it equals the quasivariety generated by the class of integral domains with trivial unit group.

**Keywords** Divisibility · Relatively distributive quasivariety

**2010 Mathematics Subject Classification** 13A05 · 13A15 · 08C15

## 1 Introduction

What can be said about the class of commutative rings in which, if $a$ differs from $b$, the set of elements divisible by $a$ differs from the set of elements divisible by $b$? Equivalently, what can be said about the class of rings where $a \neq b$ implies $(a) \neq (b)$? In this paper we show that this class is a relatively ideal distributive quasivariety, and we give a set of axioms for the quasivariety. Along the way we learn that this quasivariety is exactly the quasivariety of commutative rings generated by the class of integral domains with trivial unit group.

P. N. Ánh (✉)
Rényi Institute of Mathematics, Hungarian Academy of Sciences,
Pf. 127, 1364 Budapest, Hungary
e-mail: anh.pham.ngoc@renyi.mta.hu

K. A. Kearnes · Á. Szendrei
Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, USA
e-mail: Kearnes@Colorado.EDU

Á. Szendrei
e-mail: Szendrei@Colorado.EDU



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_1

## 2 The Quasivariety of Rings Whose Principal Ideals have Unique Generators

Our goal in this section is to describe the class of commutative rings whose principal ideals have unique generators. The main result is that this class is a relatively ideal distributive quasivariety, so let us explain now what that means. (For more details about relatively congruence distributive/modular quasivarieties, we refer to [1–3].)

A *quasi-identity* in the language of commutative rings is a universally quantified implication of the form

$$(s_1 = t_1) \wedge \cdots \wedge (s_n = t_n) \to (s_0 = t_0)$$

where $s_i$ and $t_i$ are ring terms (= "words", or "polynomials"). We allow $n = 0$, in which case the quasi-identity reduces to an identity: $s_0 = t_0$ (universally quantified). To emphasize this last point: identities are special quasi-identities.

A *variety* is a class axiomatized by identities. A *quasivariety* is a class axiomatized by quasi-identities. For an example of the former, the class of commutative rings is a variety. For an example of the latter, the class of rings axiomatized by the identities defining commutative rings together with the quasi-identity $(x^2 = 0) \to (x = 0)$ is the quasivariety of reduced commutative rings (rings with no nonzero nilpotent elements).

If $\mathcal{Q}$ is a quasivariety of commutative rings, $R \in \mathcal{Q}$, and $I \lhd R$ is an ideal of $R$, then $I$ is a *$\mathcal{Q}$-ideal* (or a *relative* ideal) if $R/I \in \mathcal{Q}$. For example, if $\mathcal{Q}$ is the quasivariety of commutative reduced rings and $R \in \mathcal{Q}$, then $I$ is a relative ideal of $R$ exactly when $I$ is a semiprime ideal of $R$.

The collection of $\mathcal{Q}$-ideals of some $R \in \mathcal{Q}$, when ordered by inclusion, forms an algebraic lattice. It is not a sublattice of the ordinary ideal lattice, but it is a sub<u>set</u> of the ordinary ideal lattice that is closed under arbitrary meet.

A quasivariety $\mathcal{Q}$ of commutative rings is *relatively ideal distributive* if the $\mathcal{Q}$-ideal lattice of any member of $\mathcal{Q}$ satisfies the distributive law:

$$I \wedge (J \vee K) = (I \wedge J) \vee (I \wedge K).$$

Here, the meet operation is just intersection ($I \wedge J = I \cap J$) while the join operation depends on $\mathcal{Q}$; all that can be said is that $I \vee J$ is the least $\mathcal{Q}$-ideal that contains $I \cup J$ (or, equivalently, contains $I + J$).

It is interesting to find that some particular quasivariety of rings is relatively ideal distributive. Any distributive algebraic lattice is isomorphic to the lattice of open sets of a topology defined on the set of meet irreducible lattice elements. Therefore, if $\mathcal{Q}$ is relatively ideal distributive, then to each member of $\mathcal{Q}$ there is a naturally associated topological space, its $\mathcal{Q}$-spectrum. It is possible to treat a member $R \in \mathcal{Q}$ as a ring of functions defined over its $\mathcal{Q}$-spectrum. It turns out that the quasivariety of commutative reduced rings, mentioned earlier as an example, is relatively ideal distributive, and for this $\mathcal{Q}$ the $\mathcal{Q}$-spectrum of any $R \in \mathcal{Q}$ is just the ordinary prime spectrum of $R$.

The main result of this section is that the class of commutative rings whose principal ideals have unique generators is a relatively ideal distributive quasivariety, and for which we provide an axiomatization.

**Theorem 1.** *Let $\mathcal{Q}$ be the class of all commutative rings (with* 1*) having the property that each principal ideal has a unique generator. Let $\mathcal{D}$ be the class of domains in $\mathcal{Q}$.*

(1) *$\mathcal{Q}$ is a quasivariety. It is exactly the class of rings axiomatized by the quasi-identity $(xyz = z) \to (yz = z)$ along with the identities defining the variety of all commutative rings. All rings in $\mathcal{Q}$ have trivial unit group and are reduced. Such rings are $\mathbb{F}_2$-algebras.*
(2) *$\mathcal{D}$ is exactly the class of domains with trivial unit group.*
(3) *$\mathcal{Q}$ consist of the subrings of products of members of $\mathcal{D}$ (we write $\mathcal{Q} = \mathsf{SP}(\mathcal{D})$).*
(4) *$\mathcal{Q}$ is a relatively ideal distributive quasivariety.*
(5) *The class of locally finite algebras in $\mathcal{Q}$ is the class of Boolean rings. This class is the largest subvariety of $\mathcal{Q}$.*

*Proof.* We argue the first two claims of Item (1) together. Namely, we show that $R \in \mathcal{Q}$ if and only if $R$ belongs to the quasivariety of commutative rings satisfying $(xyz = z) \to (yz = z)$.

For the "if" part, let $R$ be a commutative ring satisfying $(xyz = z) \to (yz = z)$. Choose $r \in R$ and assume that $(r) = (s)$ for some $s$. Then $s = qr$ and $r = ps$ for some $p, q \in R$. Since $pqr = r$, the quasi-identity yields $qr = r$, or $s = r$. Thus, $(r) = (s)$ implies $r = s$, showing that $R$ satisfies the unique generator property for principal ideals. Conversely, for "only if", suppose that $R$ does not satisfy $(xyz = z) \to (yz = z)$. $R$ must have elements $p, q, r$ such that $pqr = r$ and $qr \neq r$, Then $(r) = (qr)$ and $qr \neq r$, so $R$ does not have the unique generator property.

For the second to last statement of Item (1), suppose that $R \in \mathcal{Q}$ and that $u$ is a unit in $R$. Then $(u) = R = (1)$, so by the unique generator property $u = 1$. Also, to see that $R$ is reduced, assume that $n \in R$ satisfies $n^2 = 0$. Then $1 + n$ is a unit (with inverse $1 - n$), so $1 + n = 1$, so $n = 0$.

For the final statement of Item (1), the fact that any $R \in \mathcal{Q}$ is an $\mathbb{F}_2$-algebra follows from the fact that $-1$ is a unit, so $1 = -1$. Then the prime subring of $R$ is isomorphic to $\mathbb{F}_2$, which is enough to establish that $R$ is an $\mathbb{F}_2$-algebra.

For Item (2), if $D \in \mathcal{D}$, then $D$ is a domain by definition, and it has trivial unit group by Item (1). Conversely, suppose that $D$ is a domain with trivial unit group. If $(a) = (b)$ in $D$, then $a$ and $b$ must differ by a unit, hence $a = b$, showing that $D$ has the unique generator property, so $D$ is a domain in $\mathcal{Q}$, yielding $D \in \mathcal{D}$.

In order to establish Item (3) we first prove a claim.

**Claim 2.** *If $R \in \mathcal{Q}$ and $S \subseteq R$ is a subset, then the annihilator $A = ann(S)$ is a $\mathcal{Q}$-ideal (meaning that $R/A \in \mathcal{Q}$).*

*Proof of claim.* For this we must verify that $R/A$ satisfies the quasi-identity $(xyz = z) \to (yz = z)$. Equivalently, we must show that if $x, y, z \in R$ and $xyz \equiv z \pmod{A}$, then $yz \equiv z \pmod{A}$. We begin: If $xyz \equiv z \pmod{A}$, then $(xyz - z) \in A$, so $(xyz - z)s = 0$ for any $s \in S$. This means that $xy(zs) = (zs)$ for any $s \in S$. Applying the quasi-identity from Item (1) with $zs$ in place of $z$ we derive that $yzs = zs$, or $(yz - z)s = 0$ for any $r \in I$. Hence $yz \equiv z \pmod{A}$, as desired.

Next we argue that if $R \in \mathcal{Q}$ is not a domain, then $R$ has disjoint nonzero $\mathcal{Q}$-ideals $I$ and $J$. If $R$ is not a domain, then there exist nonzero $r$ and $s$ such that $rs = 0$. Take $I = \text{ann}(r)$ and $J = \text{ann}(I)$. $I$ is nonzero since it contains $s$, and $J$ is nonzero since it contains $r$. Both $I$ and $J$ are $\mathcal{Q}$-ideals by Claim 2. If $t \in I \cap J$, then $t^2 \in IJ = \{0\}$, so $t$ is nilpotent. According to Item (1), any $R \in \mathcal{Q}$ is reduced, so $t = 0$. Thus $I$ and $J$ are indeed disjoint nonzero $\mathcal{Q}$-ideals.

The argument for Item (3) is completed by noting that any quasivariety $\mathcal{Q}$ is expressible as $\mathsf{SP}(\mathcal{K})$ where $\mathcal{K}$ is the subclass of relatively subdirectly irreducible members of $\mathcal{Q}$. This is a version of Birkhoff's subdirect representation theorem, stated for quasivarieties, and it holds for quasivarieties because relative ideal/congruence lattices are algebraic. The previous paragraph shows that the only members of $\mathcal{Q}$ that could possibly be relatively subdirectly irreducible are the domains. (That is, $R$ not a domain $\Rightarrow$ $R$ has disjoint nonzero $\mathcal{Q}$-ideals $\Rightarrow$ $R$ is not relatively subdirectly irreducible.)

To prove Item (4), we refer to general criteria from [3] for proving that a quasivariety is relatively congruence distributive. Specifically, we will use Theorems 4.1 and 4.3 of that paper, along with some of the remarks between those theorems.

Here is a summary of what we are citing. From Theorem 4.1 of [3], a quasivariety is relatively congruence modular if and only if it satisfies the "extension principle" and the "relative shifting lemma". From remarks following the proof of Theorem 4.1, the "extension principle" can be replaced by the "weak extension principle". From Theorem 2.1 of that paper, the "relative shifting lemma" can be replaced by the "existence of quasi-Day terms". Finally, from Theorem 4.3 of that paper, a quasivariety is relatively congruence distributive if and only if it is relatively congruence modular and no member has a nonzero abelian congruence.

What this reduces to in our setting is this: to prove that our quasivariety $\mathcal{Q}$ is relatively ideal distributive (Item (4)) it suffices to show that $\mathcal{Q}$

(i) has "quasi-Day terms",
(ii) satisfies the "weak extension principle", and
(iii) has no member with a nontrivial abelian congruence (i.e., with a nonzero ideal $A$ satisfying $A^2 = 0$).

Condition (i) holds since $\mathcal{Q}$ has ordinary Day terms, in fact a Maltsev term. (More explicitly, the singleton set $\Sigma_s := \{(p(w, x, y, z), q(w, x, y, z)\}$ where $p(w, x, y, z) := w - x + y$ and $q(w, x, y, z) := z$ meets the defining conditions from Theorem 2.1(2) of [3] for "quasi-Day terms".)

Condition (iii) holds since if $A \lhd R \in \mathcal{Q}$ and $A^2 = 0$, then the elements of $A$ are nilpotent. As argued in the proof of Item (1), the only nilpotent element in $R$ is 0, hence $A = 0$.

Condition (ii) means that if $R \in \mathcal{Q}$ has disjoint ideals $I$ and $J$, then $I$ and $J$ can be extended to $\mathcal{Q}$-ideals $\overline{I} \supseteq I$ and $\overline{J} \supseteq J$ that are also disjoint. To prove that Condition (ii) holds we modify an argument from above: If $R$ has ideals $I$ and $J$ such that $I \cap J = 0$, then $IJ = 0$. The $\mathcal{Q}$-ideal $\overline{J} = \mathrm{ann}(I)$ contains $J$, the $\mathcal{Q}$-ideal $\overline{I} = \mathrm{ann}(\overline{J})$ contains $I$, both are $\mathcal{Q}$-ideals, and $\overline{I} \cap \overline{J} = 0$ (since the elements in this intersection square to zero and $R$ is reduced). This shows that disjoint ideals $I$ and $J$ may be extended to disjoint $\mathcal{Q}$-ideals.

For Item (5), to show that a locally finite ring in $\mathcal{Q}$ is a Boolean ring it suffices to show that any finite ring $F \in \mathcal{Q}$ is Boolean. (The reason this reduction is permitted is that the property of being a Boolean ring is expressible by the identity $x^2 = x$, and a locally finite structure satisfies a universal sentence if and only if its finite substructures satisfy the sentence.)

So choose a finite $F \in \mathcal{Q}$. As $F$ has trivial unit group, and $1 + \mathrm{rad}(F) \subseteq U(F)$, we get that $F$ must be semiprimitive. Since $F$ is finite it must be a product of fields. Since $F$ has only trivial units, each factor field must have size 2, so $F$ is Boolean.

Conversely, if $B$ is any Boolean ring, then multiplication is a semilattice operation, so $xyz \leq yz \leq z$ in the semilattice order for any $x, y, z \in B$. If, in $B$, we have first = last ($xyz = z$), then we must have middle = last ($yz = z$). Hence $B \in \mathcal{Q}$.

To complete the proof of Item (5) we must show that if $\mathcal{V}$ is a variety and $\mathcal{V} \subseteq \mathcal{Q}$, then $\mathcal{V}$ consists of Boolean rings. For this it suffices to show that if $R \in \mathcal{Q}$ is not Boolean (i.e., $R$ has an element $r$ satisfying $r \neq r^2$), then $R \notin \mathcal{V}$. This holds because $\langle r^2 \rangle \subsetneq \langle r \rangle$ by the unique generator property, so $r/\langle r^2 \rangle$ is a nonzero nilpotent element of $R/\langle r^2 \rangle$, establishing that some homomorphic image of $R$ is not in $\mathcal{Q}$. □

By substituting $z = 1$ in the quasi-identity $(xyz = z) \to (yz = z)$ we obtain the consequence $(xy = 1) \to (y = 1)$, which expresses that the unit group is trivial. Since a consequence can be no stronger than the original statement, this is enough to deduce that the quasivariety of commutative rings with trivial unit group contains the quasivariety of commutative rings whose principal ideals have unique generators. This containment is proper, and the following example describes a commutative ring satisfying $(xy = 1) \to (y = 1)$ but not $(xyz = z) \to (yz = z)$.

**Example 3.** Let $R$ be the commutative $\mathbb{F}_2$-algebra presented by

$$\langle X, Y, Z \mid XYZ = Z \rangle.$$

That is, $R$ is the quotient of the polynomial ring $\mathbb{F}_2[X, Y, Z]$ by the ideal $(XYZ - Z)$.

We may view the relation $XYZ - Z = 0$ as a reduction rule $XYZ \to Z$ to produce a normal form for elements of $R$. This single rule is applied as follows: choose a monomial of the form $XYZW$ ($W$ is a product of variables) of an element in a coset of $(XYZ - Z) \subseteq \mathbb{F}_2[X, Y, Z]$ and replace $XYZW$ by $ZW$. That is, if each of $X, Y, Z$ appear in a monomial, we delete one instance of $X$ and one instance of $Y$ from that monomial.

The Diamond Lemma applies to show that there is a normal form for elements of $R$, and the elements in normal form are exactly the polynomials over $\mathbb{F}_2$ in the generators $X, Y, Z$ where no monomial is divisible by each of $X$, $Y$, and $Z$.

Note that each application of the reduction rule reduces the $X$-degree and the $Y$-degree of some monomial, but does not alter the $Z$-degree of any monomial. This is enough to prove that the unit group of $R$ is trivial. For if $R$ had a unit $u$ with inverse $v$, then the $Z$-degree of the product $uv = 1$ is zero, but it is also the sum of the $Z$-degrees of $u$ and $v$. Hence the normal form of a unit must be $Z$-free. But then $u$ and $v$ would then be inverse units in the subring $\mathbb{F}_2[X, Y]$, where all elements are in normal form. Now one can argue in this subring, using $X$-degree and $Y$-degree, to conclude that none of $X, Y, Z$ appear in the normal form of a unit. We are left with $u = v = 1$ as the only possibility.

Notice also that $YZ - Z$ is in normal form, so $YZ - Z \neq 0$ in $R$. This shows that $R$ fails to satisfy $(xyz = z) \to (yz = z)$, but does satisfy $(xy = 1) \to (y = 1)$. In particular, the fact that $XYZ = Z$ while $YZ \neq Z$ means that $(YZ) = (Z)$, while $YZ \neq Z$, so the principal ideal $(Z)$ does not have a unique generator.

## 3 Some Related Quasivarieties

We saw in the previous section that the class of commutative rings whose principal ideals have unique generators is the quasivariety generated by the class of domains with trivial unit group. We also saw that this quasivariety is relatively ideal distributive, and that it is axiomatized by the quasi-identity $(xyz = z) \to (yz = z)$.

In this section we will show that the quasivariety $\mathcal{Q}_{|n}$ generated by those domains $D$ whose unit group $U(D)$ is cyclic of order dividing $n$ is also relatively ideal distributive, and we shall provide an axiomatization for $\mathcal{Q}_{|n}$.

Write $\mathcal{D}_{|n}$ for the class of domains whose unit group is cyclic of order dividing $n$.

**Theorem 4.** *By definition, we have that $\mathcal{Q}_{|n}$ is the quasivariety generated by $\mathcal{D}_{|n}$.*

(1) $\mathcal{Q}_{|n}$ *is axiomatized* by

  (a) *the identities defining commutative rings,*
  (b) *the quasi-identity* $(x^2 = 0) \to (x = 0)$, *which expresses that the only nilpotent element is* $0$, *and*
  (c) *the quasi-identity* $(xyz = z) \to (y^n z = z)$.

(2) $\mathcal{Q}_{|n}$ *is a relatively ideal distributive quasivariety.*

*Proof.* To prove Item (1), let $\mathcal{K}$ be the quasivariety axiomatized by the sentences in (a), (b), and (c). It is easy to see that $\mathcal{D}_{|n}$ satisfies the quasi-identities in (a), (b), and (c), so $\mathcal{D}_{|n} \subseteq \mathcal{K}$, and therefore $\mathcal{Q}_{|n} \subseteq \mathcal{K}$.

Conversely, we must show that $\mathcal{K} \subseteq \mathcal{Q}_{|n}$ For this, we need the analogue of Claim 2 for $\mathcal{K}$:

**Claim 5.** *If $R \in \mathcal{K}$ and $S \subseteq R$ is a subset, then the annihilator $A = ann(S)$ is a $\mathcal{K}$-ideal.*

*Proof of claim.* Our goal is to prove that $R/A \in \mathcal{K}$, so we must prove that $R/A$ is a commutative ring satisfying $(x^2 = 0) \to (x = 0)$ and $(xyz = z) \to (y^n z = z)$. It is clear that $R/A$ is a commutative ring (identities are preserved under quotients), so we only need to verify that $R/A$ satisfies $(x^2 = 0) \to (x = 0)$ and $(xyz = z) \to (y^n z = z)$. For the second of these, the proof is exactly like the proof of Claim 2, while for the first there is an extra idea. We prove the first only.

To prove that $R/A$ satisfies $(x^2 = 0) \to (x = 0)$, we must show that $R$ satisfies $x^2 \equiv 0 \pmod{A}$ implies $x \equiv 0 \pmod{A}$. If $x^2 \equiv 0 \pmod{A}$, or $x^2 \in A$, then $x^2 s = 0$ for all $s \in S$. This implies $(xs)^2 = (x^2 s)s = 0$ for all $s \in S$. (This is the "extra idea".) But $R$ satisfies $(x^2 = 0) \to (x = 0)$, so from $(xs)^2 = 0$ we deduce $xs = 0$ for all $s \in S$. This proves that $x \in A$ or $x \equiv 0 \pmod{A}$.

We will use Claim 5 the same way we used Claim 2 in the proof of Theorem 1. If $R \in \mathcal{K}$ is not a domain, then there exist nonzero $r$ and $s$ such that $rs = 0$. Take $I = \text{ann}(r)$ and $J = \text{ann}(I)$. $I$ is nonzero since it contains $s$, and $J$ is nonzero since it contains $r$. By Claim 5, $I$ and $J$ are $\mathcal{K}$-ideals. Any element in $I \cap J$ must square to zero, so since $\mathcal{K}$ satisfies axiom (b) we get $I \cap J = \{0\}$. Thus, if $R$ is not a domain, then it has a pair of nonzero, disjoint, $\mathcal{K}$-ideals. This is enough to guarantee that $R$ is not subdirectly irreducible relative to $\mathcal{K}$.

In the contrapositive form, we have shown that any relatively subdirectly irreducible member of $\mathcal{K}$ is a domain. Hence $\mathcal{K}$ is generated by its subclass of domains.

But if $D \in \mathcal{K}$ is a domain, then by substituting $z = 1$ in the quasi-identity (1)(c) we obtain that $D$ satisfies $(xy = 1) \to (y^n = 1)$. This implies that the unit group $U(D)$ of $D$ is a cyclic group of order dividing $n$. The reason for this is that $U(D)$ is an abelian group satisfying $x^n = 1$, hence $U(D)$ is a locally finite abelian group. If $U(D)$ is not cyclic, then it contains a finite noncyclic subgroup $G \subseteq U(D)$. But now $G$ is a finite noncyclic subgroup of the field of fractions of $D$, and we all know that the multiplicative group of a field contains no finite noncyclic subgroup. This shows that the domains in $\mathcal{K}$ lie in $\mathcal{D}_{|n}$, so $\mathcal{K}$ is contained in the quasivariety generated by $\mathcal{D}_{|n}$, which is $\mathcal{Q}_{|n}$.

Item (2) of this theorem is proved exactly like Item (4) of Theorem 1. □

**Observations 6.** A quick test to rule out that some nonzero ring $R$ belongs to some quasivariety $\mathcal{Q}_{|n}$ is to show that the prime subring of $R$ does not belong to $\mathcal{Q}_{|n}$. Since the prime subring of $R$ is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}_k$ for some $k > 1$, and since the units of $\mathbb{Z}$ and $\mathbb{Z}_k$ are easy to determine, it is not hard to derive some consequences.

Namely, $\mathbb{Z}_k$ satisfies the quasi-identity in Theorem 4(1)(b) if and only if $k$ is square-free, and hence $k = p_1 \dots p_m$ and $\mathbb{Z}_k \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_m}$ for distinct primes $p_1, \dots, p_m$. Now, for such a $k$, $\mathbb{Z}_k$ satisfies the quasi-identity in Theorem 4(1)(c) if and only if $p_i - 1$ divides $n$ for each $i$. Therefore, these conditions on $k$ are necessary for $R$ to belong to $\mathcal{Q}_{|n}$ whenever the prime subring of $R$ is isomorphic to $\mathbb{Z}_k$. Similarly, $\mathbb{Z}$ satisfies the quasi-identity in Theorem 4(1)(c) if and only if $n$ is even. Hence, if the prime subring of $R$ is isomorphic to $\mathbb{Z}$, then for $R$ to belong to $\mathcal{Q}_{|n}$ the number $n$ must be even.

These considerations imply, in particular, that if $n$ is odd, then $\mathbb{Z}_k \notin \mathcal{Q}_{|n}$ unless $k = 2$, and $\mathbb{Z} \notin \mathcal{Q}_{|n}$. Hence, each ring in $\mathcal{Q}_{|n}$ may be thought of as an $\mathbb{F}_2$-algebra.

Notice also that, when $n$ is odd, the axiom $(x^2 = 0) \to (x = 0)$ from Theorem 4(1)(b) is a consequence of the axiom $(xyz = z) \to (y^n z = z)$ from Theorem 4(1)(c). For if $R$ satisfies $(xyz = z) \to (y^n z = z)$ for some odd $n$, and some $r \in R$ satisfies $r^2 = 0$, then as observed in the previous paragraph the characteristic of $R$ must be 2, so $(1 + r)^2 = 1$. This implies that $1 + r$ is a unit of order dividing 2 (and also $n$), so necessarily $1 + r = 1$, which implies that $r = 0$.

We can use Observation 6 to show that not all the quasivarieties $\mathcal{Q}_{|n}$ are distinct, in particular

**Theorem 7.** *If $p$ is an odd prime, then $\mathcal{Q}_{|p} = \mathcal{Q}_{|1}$ unless $p$ is a Mersenne prime.*

*Proof.* To prove that $\mathcal{Q}_{|p} = \mathcal{Q}_{|1}$ when $p$ is an odd non-Mersenne prime, it will suffice to show that these quasivarieties contain the same domains. We always have $\mathcal{Q}_{|m} \subseteq \mathcal{Q}_{|n}$ when $m \mid n$, from the definition of these quasivarieties, so we must show that any domain $D \in \mathcal{Q}_{|p}$ is contained in $\mathcal{Q}_{|1}$ (i.e., has a trivial unit group).

Choose $D \in \mathcal{Q}_{|p}$. From Observation 6, we know (since $p$ is odd) that $D$ is an $\mathbb{F}_2$-algebra. Suppose that $\theta \in D$ is a nontrivial unit. Since $\theta$ has finite multiplicative order, and the prime subring of $D$ is finite, the subring $S \subseteq D$ generated by $\theta$ is finite. $S$ is a subring of a domain itself, hence it is a field, and $U(S) = S^\times$. $S$ belongs to $\mathcal{Q}_{|p}$, so $S^\times$ has order dividing $p$, and it must therefore be that $|S^\times| = p$. This shows that $S$ is a finite field of characteristic 2 and of cardinality $|S| = p + 1$. We derive that $p + 1 = 2^s$ for some $s$, or $p = 2^s - 1$. This completes the proof that $\mathcal{Q}_{|p} = \mathcal{Q}_{|1}$ unless $p$ is a Mersenne prime.

The primality of $p$ did not play a big role in the proof. The same argument shows that if $n$ is any odd number, then $\mathcal{Q}_{|n} = \mathcal{Q}_{|1}$ unless $n$ is divisible by some number $x > 1$ of the form $x = 2^s - 1$. So, for example, $\mathcal{Q}_{|55} = \mathcal{Q}_{|25} = \mathcal{Q}_{|1}$. But if $n$ is divisible by some number $x > 1$ of the form $x = 2^s - 1$, then $\mathcal{Q}_{|n}$ will contain some finite fields that are not in $\mathcal{Q}_{|1}$.

**Acknowledgements** This material is based upon work supported by the National Research, Development and Innovation Office NKFIH K119934, the Vietnam Institute for Advanced Study in Mathematics (VIASM), the Vietnamese Institute of Mathematics, the National Science Foundation grant no. DMS 1500254, the Hungarian National Foundation for Scientific Research (OTKA) grant no. K115518, and the National Research, Development and Innovation Fund of Hungary (NKFI) grant no. K128042.

## References

1. Kearnes, K.A.: Relatively congruence distributive subquasivarieties of a congruence modular variety. Bull. Austral. Math. Soc. **41**(1), 87–96 (1990). https://doi.org/10.1017/S0004972700017871
2. Kearnes K.A.: Relatively congruence modular quasivarieties of modules. In: Czelakowski, J. (eds.) Don Pigozzi on Abstract Algebraic Logic, Universal Algebra, and Computer Science. Outstanding Contributions to Logic, vol. 16, pp. 221–232. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-74772-9_8
3. Kearnes, K., McKenzie, R.: Commutator theory for relatively modular quasivarieties. Trans. Amer. Math. Soc. **331**(2), 465–502 (1992). https://doi.org/10.2307/2154123

# On Monoids of Ideals of Orders in Quadratic Number Fields

**Johannes Brantner, Alfred Geroldinger, and Andreas Reinhart**

**Abstract** We determine the set of catenary degrees, the set of distances, and the unions of sets of lengths of the monoid of nonzero ideals and of the monoid of invertible ideals of orders in quadratic number fields.

**Keywords** Orders · Quadratic number fields · Sets of lengths · Sets of distances · Catenary degree

**2010 Mathematics Subject Classification** 11R11 · 11R27 · 13A15 · 13F15 · 20M12 · 20M13

## 1 Introduction

Factorization theory for Mori domains and their semigroups of ideals splits into two cases. The first and best understood case is that of Krull domains (i.e., of completely integrally closed Mori domains). The arithmetic of a Krull domain depends only on the class group and on the distribution of prime divisors in the classes, and it can be studied—at least to a large extent—with methods from additive combinatorics. The link to additive combinatorics is most powerful when the Krull domain has a finite class group and when each class contains at least one prime divisor (this holds true,

J. Brantner · A. Geroldinger (✉)
Institut Für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, NAWI Graz, Heinrichstraße 36, 8010 Graz, Austria
e-mail: alfred.geroldinger@uni-graz.at
URL: https://imsc.uni-graz.at/geroldinger

J. Brantner
e-mail: j.brantner@gmx.at

A. Reinhart
Department of Mathematical Sciences, New Mexico State University, Las Cruces, NM 88003, USA
e-mail: andreas.reinhart@uni-graz.at



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*, Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_2

among others, for rings of integers in number fields). Then sets of lengths, sets of distances, and of catenary degrees of the domain can be studied in terms of zero-sum problems over the class group. Moreover, we obtain a variety of explicit results for arithmetical invariants in terms of classical combinatorial invariants (such as the Davenport constant of the class group) or even in terms of the group invariants of the class group. We refer to [15] for a description of the link to additive combinatorics and to the recent survey [32] discussing explicit results for arithmetical invariants.

Let us consider Mori domains that are not completely integrally closed but have a nonzero conductor toward their complete integral closure. The best investigated classes of such domains are weakly Krull Mori domains with finite $v$-class group and C-domains. For them there is a variety of abstract arithmetical finiteness results but in general there are no precise results. For example, it is well-known that sets of distances and of catenary degrees are finite but there are no reasonable bounds for their size. The simplest not completely integrally closed Mori domains are orders in number fields. They are one-dimensional noetherian with nonzero conductor, finite Picard group, and all factor rings modulo nonzero ideals are finite. Thus they are weakly Krull domains and C-domains. Although there is recent progress for seminormal orders, for general orders in number fields there is no characterization of half-factoriality (for progress in the local case see [26]) and there is no information on the structure of their sets of distances or catenary degrees (neither for orders nor for their monoids of ideals).

In the present paper, we focus on monoids of ideals of orders in quadratic number fields and establish precise results for their set of distances $\Delta(\cdot)$ and their set of catenary degrees $\mathrm{Ca}(\cdot)$. Orders in quadratic number fields are intimately related to quadratic irrationals, continued fractions, and binary quadratic forms and all these areas provide a wealth of number theoretic tools for the investigation of orders. We refer to [25] for a modern presentation of these connections and to [9, 29] for recent progress on the arithmetic and ideal theoretic structure of quadratic orders.

Let $\mathcal{O}$ be an order in a quadratic number field, $\mathcal{I}^*(\mathcal{O})$ be the monoid of invertible ideals, and $\mathcal{I}(\mathcal{O})$ be the monoid of nonzero ideals (note that $\mathcal{I}(\mathcal{O})$ is not cancellative if $\mathcal{O}$ is not maximal). Since $\mathcal{I}^*(\mathcal{O})$ is a divisor-closed submonoid of $\mathcal{I}(\mathcal{O})$, the set of catenary degrees and the set of distances of $\mathcal{I}^*(\mathcal{O})$ are contained in the respective sets of $\mathcal{I}(\mathcal{O})$. We formulate a main result of this paper and then we compare it with related results in the literature.

**Theorem 1.1.** *Let $\mathcal{O}$ be an order in a quadratic number field $K$ with discriminant $d_K$ and conductor $\mathfrak{f} = f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$.*

1. *The following statements are equivalent:*
   (a) *$\mathcal{I}(\mathcal{O})$ is half-factorial.*
   (b) $\mathsf{c}\big(\mathcal{I}(\mathcal{O})\big) = 2$.
   (c) $\mathsf{c}\big(\mathcal{I}^*(\mathcal{O})\big) = 2$.
   (d) *$\mathcal{I}^*(\mathcal{O})$ is half-factorial.*
   (e) *$f$ is squarefree and all prime divisors of $f$ are inert.*

2. *Suppose that $\mathcal{I}^*(\mathcal{O})$ is not half-factorial.*
   (a) *If $f$ is squarefree, then* $\mathsf{Ca}\big(\mathcal{I}(\mathcal{O})\big) = [1, 3]$, $\mathsf{Ca}\big(\mathcal{I}^*(\mathcal{O})\big) = [2, 3]$, $\Delta\big(\mathcal{I}(\mathcal{O})\big) = \Delta\big(\mathcal{I}^*(\mathcal{O})\big) = \{1\}$.
   (b) *Suppose that $f$ is not squarefree.*
      (i) *If* $\mathsf{v}_2(f) \notin \{2, 3\}$ *or* $d_K \not\equiv 1 \mod 8$, *then* $\mathsf{Ca}\big(\mathcal{I}(\mathcal{O})\big) = [1, 4]$, $\mathsf{Ca}\big(\mathcal{I}^*(\mathcal{O})\big) = [2, 4]$, *and* $\Delta\big(\mathcal{I}(\mathcal{O})\big) = \Delta\big(\mathcal{I}^*(\mathcal{O})\big) = [1, 2]$.
      (ii) *If* $\mathsf{v}_2(f) \in \{2, 3\}$ *and* $d_K \equiv 1 \mod 8$, *then* $\mathsf{Ca}\big(\mathcal{I}(\mathcal{O})\big) = [1, 5]$, $\mathsf{Ca}\big(\mathcal{I}^*(\mathcal{O})\big) = [2, 5]$, *and* $\Delta\big(\mathcal{I}(\mathcal{O})\big) = \Delta\big(\mathcal{I}^*(\mathcal{O})\big) = [1, 3]$.

We say that a cancellative monoid $H$ is *weakly Krull* if $\bigcap_{P \in \mathfrak{X}(H)} H_P = H$ and $\{P \in \mathfrak{X}(H) \mid a \in P\}$ is finite for each $a \in H$ (where $\mathfrak{X}(H)$ denotes the set of height-one prime ideals of $H$). Moreover, a cancellative monoid $H$ is called *weakly factorial* if every nonunit of $H$ is a finite product of primary elements of $H$. Let all notation be as in Theorem 1.1, and recall that $\mathcal{I}^*(\mathcal{O})$ is a weakly factorial C-monoid, and that for every atomic monoid $H$ with $\Delta(H) \neq \emptyset$ we have $\min \Delta(H) = \gcd \Delta(H)$.

There is a characterization (due to Halter-Koch) when the order $\mathcal{O}$ is half-factorial [16, Theorem 3.7.15]. This characterization and Theorem 1.1 or [30, Corollary 4.6] show that the half-factoriality of $\mathcal{O}$ implies the half-factoriality of $\mathcal{I}^*(\mathcal{O})$. Consider the case of seminormal orders whence suppose that $\mathcal{O}$ is seminormal. Then $f$ is squarefree (this follows from an explicit characterization of seminormal orders given by Dobbs and Fontana in [10, Corollary 4.5]). Moreover, $\mathcal{I}^*(\mathcal{O})$ is seminormal and if $\mathcal{I}^*(\mathcal{O})$ is not half-factorial, then its catenary degree equals three by [18, Theorems 5.5 and 5.8]. Clearly, this coincides with 2.(a) of the above theorem. Among others, Theorem 1.1 shows that the sets of distances and of catenary degrees are intervals and that the minimum of the set of distances equals 1. We discuss some analogous results and some results which are in sharp contrast to this. If $H$ is a Krull monoid with finite class group, then $H$ is a weakly Krull C-monoid and if there are prime divisors in all classes, then the sets $\mathsf{Ca}(H)$ and $\Delta(H)$ are intervals [23, Theorem 4.1]. On the other hand, for every finite set $S \subset \mathbb{N}$ with $\min S = \gcd S$ (resp. every finite set $S \subset \mathbb{N}_{\geq 2}$) there is a finitely generated Krull monoid $H$ such that $\Delta(H) = S$ (resp. $\mathsf{Ca}(H) = S$) [21] resp. [11, Proposition 3.2]. Just as the monoids of ideals under discussion, every numerical monoid is a weakly factorial C-monoid. However, in contrast to them, the set of distances need not be an interval [8], its minimum need not be 1 [5, Proposition 2.9], and a recent result of O'Neill and Pelayo [28] shows that for every finite set $S \subset \mathbb{N}_{\geq 2}$ there is a numerical monoid $H$ such that $\mathsf{Ca}(H) = S$.

We proceed as follows. In Section 2 we summarize the required background on the arithmetic of monoids. In Section 3 we do the same for orders in quadratic number fields and we provide an explicit description of (invertible) irreducible ideals in orders of quadratic number fields (Theorem 3.6). In Section 4 we give the proof of Theorem 1.1. Based on this result we establish a characterization of those orders $\mathcal{O}$ with $\min \Delta(\mathcal{O}) > 1$ (Theorem 4.14) which allows us to give the first explicit examples of orders $\mathcal{O}$ with $\min \Delta(\mathcal{O}) > 1$. Our third main result (given in Theorem 5.2) states that unions of sets of lengths of $\mathcal{I}(\mathcal{O})$ and of $\mathcal{I}^*(\mathcal{O})$ are intervals.

# 2 Preliminaries on the Arithmetic of Monoids

Let $\mathbb{N}$ be the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers, and for every $m \in \mathbb{N}$, we denote by

$$\varphi(m) = \left|(\mathbb{Z}/m\mathbb{Z})^\times\right| \quad Euler's\,\varphi\text{-}function.$$

For $a, b \in \mathbb{Q} \cup \{-\infty, \infty\}$, $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$ denotes the discrete interval between $a$ and $b$. Let $L, L' \subset \mathbb{Z}$. We denote by $L + L' = \{a + b \mid a \in L,\ b \in L'\}$ their *sumset*. A positive integer $d \in \mathbb{N}$ is called a *distance* of $L$ if there exists a $k \in L$ such that $L \cap [k, k + d] = \{k, k + d\}$, and we denote by $\Delta(L)$ the *set of distances* of $L$. If $\emptyset \ne L \subset \mathbb{N}$, we denote by $\rho(L) = \sup L / \min L \in \mathbb{Q}_{\ge 1} \cup \{\infty\}$ the *elasticity* of $L$. We set $\rho(\{0\}) = 1$ and $\max \emptyset = \min \emptyset = \sup \emptyset = 0$. All rings and semigroups are commutative and have an identity element.

## 2.1 *Monoids*

Let $H$ be a multiplicatively written commutative semigroup. We denote by $H^\times$ the group of invertible elements of $H$. We say that $H$ is reduced if $H^\times = \{1\}$ and we denote by $H_{\text{red}} = \{aH^\times \mid a \in H\}$ the associated reduced semigroup of $H$. An element $u \in H$ is said to be cancellative if $au = bu$ implies that $a = b$ for all $a, b \in H$. The semigroup $H$ is said to be

- *cancellative* if every element of $H$ is cancellative.
- *unit-cancellative* if $a, u \in H$ and $a = au$ implies that $u \in H^\times$.

By definition, every cancellative semigroup is unit-cancellative. All semigroups of ideals, that are studied in this paper, are unit-cancellative but not necessarily cancellative.

*Throughout this paper, a monoid means a*
*commutative unit-cancellative semigroup with identity element.*

Let $H$ be a monoid. A submonoid $S \subset H$ is said to be *divisor-closed* if $a \in S$ and $b \in H$ with $b \mid a$ implies that $b \in S$. An element $u \in H$ is said to be

- *prime* if $u \notin H^\times$ and, for all $a, b \in H$, $u \mid ab$ and $u \nmid a$ implies $u \mid b$.
- *primary* if $u \notin H^\times$ and, for all $a, b \in H$, $u \mid ab$ and $u \nmid a$ implies $u \mid b^n$ for some $n \in \mathbb{N}$.
- *irreducible* (or an *atom*) if $u \notin H^\times$ and, for all $a, b \in H$, $u = ab$ implies that $a \in H^\times$ or $b \in H^\times$.

The monoid $H$ is said to be *atomic* if every $a \in H \setminus H^\times$ is a product of finitely many atoms. If $H$ satisfies the ascending chain condition (ACC) on principal ideals, then $H$ is atomic [12, Lemma 3.1].

### 2.2 Sets of Lengths

For a set $P$, we denote by $\mathcal{F}(P)$ the free abelian monoid with basis $P$. Every $a \in \mathcal{F}(P)$ is written in the form

$$a = \prod_{p \in P} p^{\mathsf{v}_p(a)} \text{ with } \mathsf{v}_p(a) \in \mathbb{N}_0 \quad \text{and} \quad \mathsf{v}_p(a) = 0 \text{ for almost all } p \in P.$$

We call $|a| = \sum_{p \in P} \mathsf{v}_p(a)$ the length of $a$ and $\operatorname{supp}(a) = \{p \in P \mid \mathsf{v}_p(a) > 0\} \subset P$ the support of $a$. Let $H$ be an atomic monoid. The free abelian monoid $\mathsf{Z}(H) = \mathcal{F}(\mathcal{A}(H_{\text{red}}))$ denotes the *factorization monoid* of $H$ and

$$\pi \colon \mathsf{Z}(H) \to H_{\text{red}} \quad \text{satisfying} \quad \pi(u) = u \text{ for all } u \in \mathcal{A}(H_{\text{red}})$$

denotes the *factorization homomorphism* of $H$. For every $a \in H$,

$$\mathsf{Z}_H(a) = \mathsf{Z}(a) = \pi^{-1}(aH^\times) \quad \text{is the } \textit{set of factorizations} \text{ of } a \text{ and}$$
$$\mathsf{L}_H(a) = \mathsf{L}(a) = \{|z| \mid z \in \mathsf{Z}(a)\} \quad \text{is the } \textit{set of lengths} \text{ of } a.$$

For a divisor-closed submonoid $S \subset H$ and an element $a \in S$, we have $\mathsf{Z}(S) \subset \mathsf{Z}(H)$ whence $\mathsf{Z}_S(a) = \mathsf{Z}_H(a)$, and $\mathsf{L}_S(a) = \mathsf{L}_H(a)$. We denote by

- $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ the *system of sets of lengths* of $H$ and by
- $\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L) \subset \mathbb{N}$ the *set of distances* of $H$.

The monoid $H$ is said to be *half-factorial* if $\Delta(H) = \emptyset$ and if $H$ is not half-factorial, then $\min \Delta(H) = \gcd \Delta(H)$.

### 2.3 Distances and Chains of Factorizations

Let two factorizations $z, z' \in \mathsf{Z}(H)$ be given, say

$$z = u_1 \cdot \ldots \cdot u_\ell v_1 \cdot \ldots \cdot v_m \quad \text{and} \quad z' = u_1 \cdot \ldots \cdot u_\ell w_1 \cdot \ldots \cdot w_n ,$$

where $\ell, m, n \in \mathbb{N}_0$ and all $u_i, v_j, w_k \in \mathcal{A}(H_{\text{red}})$ such that $v_j \ne w_k$ for all $j \in [1, m]$ and all $k \in [1, n]$. Then $\mathsf{d}(z, z') = \max\{m, n\}$ is the *distance* between $z$ and $z'$. If $\pi(z) = \pi(z')$ and $z \ne z'$, then

$$1 + \big||z| - |z'|\big| \le \mathsf{d}(z, z') \text{ resp. } 2 + \big||z| - |z'|\big| \le \mathsf{d}(z, z') \text{ if } H \text{ is cancellative} \tag{2.1}$$

(see [12, Proposition 3.2] and [16, Lemma 1.6.2]). Let $a \in H$ and $N \in \mathbb{N}_0$. A finite sequence $z_0, \ldots, z_k \in \mathsf{Z}(a)$ is called an $N$-chain of factorizations (concatenating $z_0$ and $z_k$) if $\mathsf{d}(z_{i-1}, z_i) \le N$ for all $i \in [1, k]$. For $z, z' \in \mathsf{Z}(H)$ with $\pi(z) = \pi(z')$, we set $\mathsf{c}(z, z') = \min\{N \in \mathbb{N}_0 \mid z$ and $z'$ can be concatenated by an $N$-chain of factorizations from $\mathsf{Z}\big(\pi(z)\big)\}$. Then, for every $a \in H$,

$$\mathsf{c}(a) = \sup\{\mathsf{c}(z, z') \mid z, z' \in \mathsf{Z}(a)\} \in \mathbb{N}_0 \cup \{\infty\} \quad \text{is the } \textit{catenary degree} \text{ of } a.$$

Clearly, $a$ has unique factorization (i.e., $|\mathsf{Z}(a)| = 1$) if and only if $\mathsf{c}(a) = 0$. We denote by

$$\mathrm{Ca}(H) = \{\mathsf{c}(a) \mid a \in H, \mathsf{c}(a) > 0\} \subset \mathbb{N} \quad \text{the } \textit{set of catenary degrees} \text{ of } H,$$

and then

$$\mathsf{c}(H) = \sup \mathrm{Ca}(H) \in \mathbb{N}_0 \cup \{\infty\} \quad \text{is the catenary degree of } H.$$

We use the convention that $\sup \emptyset = 0$ whence $H$ is factorial if and only if $\mathsf{c}(H) = 0$. Note that $\mathsf{c}(a) = 0$ for all atoms $a \in H$. The restriction to positive catenary degrees in the definition of $\mathrm{Ca}(H)$ simplifies the statement of some results whence it is usual to restrict to elements with positive catenary degrees. If $H$ is cancellative, then Equation (2.1) implies that $\min \mathrm{Ca}(H) \ge 2$ and

$$2 + \sup \Delta(H) \le \mathsf{c}(H) \quad \text{if } H \text{ is not factorial.}$$

If $H = \coprod_{i \in I} H_i$, then a straightforward argument shows that

$$\mathrm{Ca}(H) = \bigcup_{i \in I} \mathrm{Ca}(H_i) \quad \text{whence} \quad \mathsf{c}(H) = \sup\{\mathsf{c}(H_i) \mid i \in I\}. \tag{2.2}$$

## 2.4 Semigroups of Ideals

Let $R$ be a domain. We denote by $\mathsf{q}(R)$ its quotient field, by $\mathfrak{X}(R)$ the set of minimal nonzero prime ideals of $R$, and by $\overline{R}$ its integral closure. Then $R \setminus \{0\}$ is a cancellative monoid,

- $\mathcal{I}(R)$ is the semigroup of nonzero ideals of $R$ (with usual ideal multiplication),
- $\mathcal{I}^*(R)$ is the subsemigroup of invertible ideals of $R$, and
- $\mathrm{Pic}(R)$ is the Picard group of $R$.

For every $I \in \mathcal{I}(R)$, we denote by $\sqrt{I}$ its radical and by $\mathcal{N}(I) = (R\colon I) = |R/I| \in \mathbb{N} \cup \{\infty\}$ its norm.

Let $S$ be a Dedekind domain and $R \subset S$ a subring. Then $R$ is called an *order* in $S$ if one of the following two equivalent conditions hold:

- $\mathsf{q}(R) = \mathsf{q}(S)$ and $S$ is a finitely generated $R$-module.
- $R$ is one-dimensional noetherian and $\overline{R} = S$ is a finitely generated $R$-module.

Let $R$ be an order in a Dedekind domain $S = \overline{R}$. We analyze the structure of $\mathcal{I}^*(R)$ and of $\mathcal{I}(R)$.

Since $R$ is noetherian, Krull's intersection theorem holds for $R$ whence $\mathcal{I}(R)$ is unit-cancellative [20, Lemma 4.1]. Thus $\mathcal{I}(R)$ is a reduced atomic monoid with identity $R$ and $\mathcal{I}^*(R)$ is a reduced cancellative atomic divisor-closed submonoid. For the sake of clarity, we will say that an ideal of $R$ is an ideal atom if it is an atom of the monoid $\mathcal{I}(R)$. If $I, J \in \mathcal{I}^*(R)$, then $I \mid J$ if and only if $J \subset I$. The prime elements of $\mathcal{I}^*(R)$ are precisely the invertible prime ideals of $R$. Every ideal is a product of primary ideals belonging to distinct prime ideals (in particular, $\mathcal{I}^*(R)$ is a weakly factorial monoid). Thus every ideal atom (i.e., every $I \in \mathcal{A}(\mathcal{I}(R))$ is primary, and if $\sqrt{I} = \mathfrak{p} \in \mathfrak{X}(R)$, then $I$ is $\mathfrak{p}$-primary. Since $\overline{R}$ is a finitely generated $R$-module, the conductor $\mathfrak{f} = (R : \overline{R})$ is nonzero, and we set

$$\mathcal{P} = \{\mathfrak{p} \in \mathfrak{X}(R) \mid \mathfrak{p} \not\supset \mathfrak{f}\} \quad \text{and} \quad \mathcal{P}^* = \mathfrak{X}(R) \setminus \mathcal{P}.$$

Let $\mathfrak{p} \in \mathfrak{X}(R)$. We denote by

$$\mathcal{I}_{\mathfrak{p}}^*(R) = \{I \in \mathcal{I}^*(R) \mid \sqrt{I} \supset \mathfrak{p}\} \quad \text{and} \quad \mathcal{I}_{\mathfrak{p}}(R) = \{I \in \mathcal{I}(R) \mid \sqrt{I} \supset \mathfrak{p}\}$$

the set of invertible $\mathfrak{p}$-primary ideals of $R$ and the set of $\mathfrak{p}$-primary ideals of $R$. Clearly, these are monoids and, moreover,

$$\mathcal{I}_{\mathfrak{p}}(R) \subset \mathcal{I}(R), \quad \mathcal{I}_{\mathfrak{p}}^*(R) \subset \mathcal{I}_{\mathfrak{p}}(R), \quad \text{and} \quad \mathcal{I}_{\mathfrak{p}}^*(R) \subset \mathcal{I}^*(R)$$

are divisor-closed submonoids. Thus $\mathcal{I}_{\mathfrak{p}}^*(R)$ is a reduced cancellative atomic monoid, $\mathcal{I}_{\mathfrak{p}}(R)$ is a reduced atomic monoid, and if $\mathfrak{p} \in \mathcal{P}$, then $\mathcal{I}_{\mathfrak{p}}^*(R) = \mathcal{I}_{\mathfrak{p}}(R)$ is free abelian. Since $R$ is noetherian and one-dimensional,

$$\alpha : \mathcal{I}(R) \to \coprod_{\mathfrak{p} \in \mathfrak{X}(R)} \mathcal{I}_{\mathfrak{p}}(R), \quad \text{defined by} \quad \alpha(I) = (I_{\mathfrak{p}} \cap R)_{\mathfrak{p} \in \mathfrak{X}(R)} \tag{2.3}$$

is a monoid isomorphism which induces a monoid isomorphism

$$\alpha_{|\mathcal{I}^*(R)} : \mathcal{I}^*(R) \to \coprod_{\mathfrak{p} \in \mathfrak{X}(R)} \mathcal{I}_{\mathfrak{p}}^*(R). \tag{2.4}$$

## 3 Orders in Quadratic Number Fields

The goal of this section is to prove Theorem 3.6 which provides an explicit description of (invertible) ideal atoms of an order in a quadratic number field. These results are essentially due to Butts and Pall (see [6] where they are given in a different style), and they were summarized without proof by Geroldinger and Lettl in [19].

Unfortunately, that presentation is misleading in one case (namely, in case $p = 2$ and $d_K \equiv 5 \mod 8$). Thus we restate the results and provide a full proof.

First we put together some facts on orders in quadratic number fields and fix our notation which remains valid throughout the rest of this paper. For proofs, details, and any undefined notions, we refer to [25]. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be squarefree, $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field,

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2, 3 \mod 4; \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \mod 4. \end{cases} \quad \text{and} \quad d_K = \begin{cases} 4d, & \text{if } d \equiv 2, 3 \mod 4; \\ d, & \text{if } d \equiv 1 \mod 4. \end{cases}$$

Then $\mathcal{O}_K = \mathbb{Z}[\omega]$ is the ring of integers and $d_K$ is the discriminant of $K$. For every $f \in \mathbb{N}$, we define

$$\varepsilon \in \{0, 1\} \text{ with } \varepsilon \equiv f d_K \mod 2\,, \quad \eta = \frac{\varepsilon - f^2 d_K}{4}\,, \quad \text{and} \quad \tau = \frac{\varepsilon + f\sqrt{d_K}}{2}.$$

Then

$$\mathcal{O}_f = \mathbb{Z} \oplus f\omega\mathbb{Z} = \mathbb{Z} \oplus \tau\mathbb{Z}$$

is an order in $\mathcal{O}_K$ with conductor $\mathfrak{f} = f\mathcal{O}_K$, and every order in $\mathcal{O}_K$ has this form. With the notation of Section 2.4 we have

$$\mathcal{P}^* = \{\mathfrak{p} \in \mathfrak{X}(\mathcal{O}_f) \mid \mathfrak{p} \supset \mathfrak{f}\} = \{p\mathbb{Z} + f\omega\mathbb{Z} \mid p \in \mathbb{P}, p \mid f\}.$$

If $\alpha = a + b\sqrt{d} \in K$, then $\overline{\alpha} = a - b\sqrt{d}$ is its conjugate, $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} = a^2 - b^2 d$ is its norm, and $\operatorname{tr}(\alpha) = \alpha + \overline{\alpha} = 2a$ is its trace. For an $I \in \mathcal{I}(\mathcal{O}_f)$, $\overline{I} = \{\overline{\alpha} \mid \alpha \in I\}$ denotes the conjugate ideal. A simple calculation shows that

$$\mathcal{N}_{K/\mathbb{Q}}(r + \tau) = r^2 + \varepsilon r + \eta \quad \text{for each } r \in \mathbb{Z}.$$

If $\mathcal{O}$ is an order and $I \in \mathcal{I}^*(\mathcal{O})$, then $(\mathcal{O}_K : I\mathcal{O}_K) = (\mathcal{O} : I)$ and if $a \in \mathcal{O} \setminus \{0\}$, then

$$(\mathcal{O} : a\mathcal{O}) = (\mathcal{O}_K : aO_K) = |\mathcal{N}_{K/\mathbb{Q}}(a)|$$

(see [17, Pages 99 and 100] and note that the factor rings $\mathcal{O}_K/I\mathcal{O}_K$ and $\mathcal{O}/I$ need not be isomorphic). For $p \in \mathbb{P}$ and for $a \in \mathbb{Z}$ we denote by $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ the *Kronecker symbol* of $a$ modulo $p$. A prime number $p \in \mathbb{Z}$ is called

- *inert* if $p\mathcal{O}_K \in \operatorname{spec}(\mathcal{O}_K)$.
- *split* if $p\mathcal{O}_K$ is a product of two distinct prime ideals of $\mathcal{O}_K$.
- *ramified* if $p\mathcal{O}_K$ is the square of a prime ideal of $\mathcal{O}_K$.

An odd prime

$$p \text{ is } \begin{cases} \text{inert} & \text{if } \left(\frac{d_K}{p}\right) = -1; \\ \text{split} & \text{if } \left(\frac{d_K}{p}\right) = 1; \\ \text{ramified} & \text{if } \left(\frac{d_K}{p}\right) = 0. \end{cases} \quad \text{and 2 is } \begin{cases} \text{inert} & \text{if } d_K \equiv 5 \mod 8; \\ \text{split} & \text{if } d_K \equiv 1 \mod 8; \\ \text{ramified} & \text{if } d_K \equiv 0 \mod 2. \end{cases}$$

**Proposition 3.1.** *Let $p$ be a prime divisor of $f$, $\mathcal{O} = \mathcal{O}_f$, and $\mathfrak{p} = p\mathbb{Z} + f\omega\mathbb{Z}$.*

1. *The primary ideals with radical $\mathfrak{p}$ are exactly the ideals of the form*

$$\mathfrak{q} = p^\ell(p^m\mathbb{Z} + (r+\tau)\mathbb{Z})$$

*with $\ell, m \in \mathbb{N}_0$, $\ell + m \geq 1$, $0 \leq r < p^m$ and $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) \equiv 0 \mod p^m$. Moreover, $\mathcal{N}(\mathfrak{q}) = p^{2\ell+m}$.*

2. *A primary ideal $\mathfrak{q} = p^\ell(p^m\mathbb{Z} + (r+\tau)\mathbb{Z})$ is invertible if and only if*

$$\mathcal{N}_{K/\mathbb{Q}}(r+\tau) \not\equiv 0 \mod p^{m+1}.$$

*Proof.* 1. Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal in $\mathcal{O}$. By [25, Theorem 5.4.2] there exist nonnegative integers $\ell, m, r$ such that $\mathfrak{q} = \ell(m\mathbb{Z} + (r+\tau)\mathbb{Z})$, $r < m$ and $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) \equiv 0 \mod m$. Since $\mathfrak{q}$ is nonzero and proper, we have $\ell m > 1$. We prove, that $\ell m$ is a power of $p$. First observe that $\mathfrak{q} \subset \sqrt{\mathfrak{q}} = \mathfrak{p}$ implies that $p \mid \ell m$. Assume to the contrary that there exists another rational prime $p' \neq p$ dividing $\ell m$, say $\ell m = p's$. But then $p's \in \mathfrak{q}$, $s \notin \mathfrak{q}$ and $p' \notin \mathfrak{p} = \sqrt{\mathfrak{q}}$. A contradiction to $\mathfrak{q}$ being primary. Conversely, assume that $\mathfrak{q} = p^\ell(p^m\mathbb{Z} + (r+\tau)\mathbb{Z})$ for integers $\ell, m \in \mathbb{N}_0$, $\ell + m \geq 1$, $0 \leq r < p^m$ and $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) \equiv 0 \mod p^m$. By [25, Theorem 5.4.2], $\mathfrak{q}$ is an ideal of $\mathcal{O}$. Since $p \in \sqrt{\mathfrak{q}}$ and $\mathfrak{p}$ is the only prime ideal in $\mathcal{O}$ containing $p$ we obtain that $\sqrt{\mathfrak{q}} = \bigcap_{\mathfrak{a} \in \text{spec}(\mathcal{O}), \mathfrak{a} \supset \mathfrak{q}} \mathfrak{a} = \mathfrak{p}$. The nonzero prime ideal $\mathfrak{p}$ is maximal, since $\mathcal{O}$ is one-dimensional. Therefore, $\mathfrak{q}$ is $\mathfrak{p}$-primary. It follows from [25, Theorem 5.4.2] that $\mathcal{N}(\mathfrak{q}) = p^{2\ell+m}$.

2. By [25, Theorem 5.4.2], $\mathfrak{q} = p^\ell(p^m\mathbb{Z} + (r+\tau)\mathbb{Z})$ is invertible if and only if $\gcd\left(p^m, 2r+\varepsilon, \frac{\mathcal{N}_{K/\mathbb{Q}}(r+\tau)}{p^m}\right) = 1$. Since $p \mid f$ and $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) = \frac{1}{4}((2r+\varepsilon)^2 - f^2 d_K)$, this is the case if and only if $p \nmid \frac{\mathcal{N}_{K/\mathbb{Q}}(r+\tau)}{p^m}$, that is $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) \not\equiv 0 \mod p^{m+1}$. □

If $x \in \mathbb{Z}$ and $y \in \mathbb{N}$, then let $\text{rem}(x, y)$ be the unique $z \in [0, y-1]$ such that $y \mid x - z$. Let $p$ be a prime divisor of $f$. Note that $\mathrm{v}_p(0) = \infty$, and if $\emptyset \neq A \subset \mathbb{N}_0$, then $\min(A \cup \{\infty\}) = \min A$. We set

$$P_{f,p} = p\mathbb{Z} + f\omega\mathbb{Z}, \quad \mathcal{I}_p^*(\mathcal{O}_f) = \mathcal{I}_{P_{f,p}}^*(\mathcal{O}_f), \mathcal{I}_p(\mathcal{O}_f) = \mathcal{I}_{P_{f,p}}(\mathcal{O}_f), \quad \text{and}$$
$$\mathcal{M}_{f,p} = \{(x, y, z) \in \mathbb{N}_0^3 \mid z < p^y, \mathrm{v}_p(z^2 + \varepsilon z + \eta) \geq y\}.$$

Let $* : \mathcal{M}_{f,p} \times \mathcal{M}_{f,p} \to \mathcal{M}_{f,p}$ be defined by $(u, v, w) * (x, y, z) = (a, b, c)$, where

$$a = u + x + g,\ b = v + y + e - 2g,$$
$$c = \text{rem}\left(h - t\frac{h^2 + \varepsilon h + \eta}{p^g}, p^b\right),\ g = \min\{v, y, \text{v}_p(w + z + \varepsilon)\},$$
$$e = \min\{g, \text{v}_p(w - z), \text{v}_p(w^2 + \varepsilon w + \eta) - v, \text{v}_p(z^2 + \varepsilon z + \eta) - y\},$$
$$t \in \mathbb{Z} \text{ is such that } t\frac{w + z + \varepsilon}{p^g} \equiv 1 \mod p^{\min\{v,y\}-g}, \text{ and } h = \begin{cases} z & \text{if } y \geq v \\ w & \text{if } v > y \end{cases}.$$

Let $\xi_{f,p} : \mathcal{M}_{f,p} \to \mathcal{I}_p(\mathcal{O}_f)$ be defined by $\xi_{f,p}(x, y, z) = p^x(p^y\mathbb{Z} + (z + \tau)\mathbb{Z})$.

**Proposition 3.2.** *Let $p$ be a prime divisor of $f$ and $I, J \in \mathcal{I}_p(\mathcal{O}_f)$.*

1. *$(\mathcal{M}_{f,p}, *)$ is a reduced monoid and $\xi_{f,p}$ is a monoid isomorphism.*
2. *If $w, z \in \mathbb{Z}$ are such that $\text{v}_p(w^2 + \varepsilon w + \eta) > 0$ and $\text{v}_p(z^2 + \varepsilon z + \eta) > 0$, then $\text{v}_p(w + z + \varepsilon) > 0$ and $\text{v}_p(w - z) > 0$.*
3. *$\mathcal{N}(I)\mathcal{N}(J) \mid \mathcal{N}(IJ)$ and $\mathcal{N}(IJ) = \mathcal{N}(I)\mathcal{N}(J)$ if and only if $I$ is invertible or $J$ is invertible. If $I$ and $J$ are proper, then $IJ \subset p\mathcal{O}_f$.*
4. *If $I \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$, then there is some $I' \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(IJ) \mid \mathcal{N}(I'J)$. If $I \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$ is not invertible, then $\mathcal{N}(I) \mid \mathcal{N}(I')$ and $\mathcal{N}(I) < \mathcal{N}(I')$ for some $I' \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$.*
5. *If $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, then $\overline{I} \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ and $I\overline{I} = \mathcal{N}(I)\mathcal{O}_f$.*

*Proof.* 1. Let $(u, v, w), (x, y, z) \in \mathcal{M}_{f,p}$. Set $g = \min\{v, y, \text{v}_p(w + z + \varepsilon)\}$ and $e = \min\{g, \text{v}_p(w - z), \text{v}_p(w^2 + \varepsilon w + \eta) - v, \text{v}_p(z^2 + \varepsilon z + \eta) - y\}$. Note that $\gcd(p^{\min\{v,y\}}, w + z + \varepsilon) = p^g$, and hence there are some $s, t \in \mathbb{Z}$ such that $sp^{\min\{v,y\}} + t(w + z + \varepsilon) = p^g$. This implies that $t\frac{w+z+\varepsilon}{p^g} \equiv 1 \mod p^{\min\{v,y\}-g}$. Set $a = u + x + g, b = v + y + e - 2g$ and let $h = z$ if $y \geq v$ and $h = w$ if $v > y$. Finally, set $c = \text{rem}(h - t\frac{h^2+\varepsilon h+\eta}{p^g}, p^b)$. First we show that $c$ does not depend on the choice of $t$. Let $t' \in \mathbb{Z}$ be such that $t'\frac{w+z+\varepsilon}{p^g} \equiv 1 \mod p^{\min\{v,y\}-g}$. Then $p^{\min\{v,y\}-g} \mid t - t'$. Note that $\min\{v, y\} + \text{v}_p(h^2 + \varepsilon h + \eta) \geq v + y + e$, and hence $p^b \mid (t - t')\frac{h^2+\varepsilon h+\eta}{p^g}$. Consequently, $c = \text{rem}(h - t'\frac{h^2+\varepsilon h+\eta}{p^g}, p^b)$.

Next we show that $(a, b, c) \in \mathcal{M}_{f,p}$. It is clear that $(a, b, c) \in \mathbb{N}_0^3$ and $c < p^b$. It remains to show that $\text{v}_p(c^2 + \varepsilon c + \eta) \geq b$. Without restriction we can assume that $v \leq y$. Then $h = z$. Set $k = z - t\frac{z^2+\varepsilon z+\eta}{p^g}$. There is some $r \in \mathbb{Z}$ such that $c = k + rp^b$. Since $c^2 + \varepsilon c + \eta = k^2 + \varepsilon k + \eta + mp^b$ for some $m \in \mathbb{Z}$, it is sufficient to show that $\text{v}_p(k^2 + \varepsilon k + \eta) \geq b$.

Observe that $k^2 + \varepsilon k + \eta = \frac{z^2+\varepsilon z+\eta}{p^{2g}}(p^{2g} - tp^g(2z + \varepsilon) + t^2(z^2 + \varepsilon z + \eta)) = \frac{z^2+\varepsilon z+\eta}{p^{2g}}(sp^{v+g} + tp^g(w - z) + t^2(z^2 + \varepsilon z + \eta))$. Note that $g + \text{v}_p(w - z) = \min\{v + \text{v}_p(w - z), \text{v}_p(w + z + \varepsilon) + \text{v}_p(w - z)\} = \min\{v + \text{v}_p(w - z), \text{v}_p(w^2 + \varepsilon w + \eta - (z^2 + \varepsilon z + \eta))\} \geq \min\{v + \text{v}_p(w - z), \text{v}_p(z^2 + \varepsilon z + \eta), \text{v}_p(w^2 + \varepsilon w + \eta)\} \geq v$. Moreover, we have $\text{v}_p(z^2 + \varepsilon z + \eta) \geq y + e$. Therefore, $\text{v}_p(k^2 + \varepsilon k + \eta) \geq \text{v}_p(z^2 + \varepsilon z + \eta) - 2g + \min\{v + g, g + \text{v}_p(w - z), \text{v}_p(z^2 + \varepsilon z + \eta)\} \geq y + e - 2g + v = b$.

Now we prove that $p^u(p^v\mathbb{Z}+(w+\tau)\mathbb{Z})p^x(p^y\mathbb{Z}+(z+\tau)\mathbb{Z}) = p^a(p^b\mathbb{Z}+(c+\tau)\mathbb{Z})$. (Note that this can be shown by using [25, Theorem 5.4.6].) Set $I = p^u(p^v\mathbb{Z}+(w+\tau)\mathbb{Z})p^x(p^y\mathbb{Z}+(z+\tau)\mathbb{Z})$. Without restriction let $v \le y$. Note that $(w+\tau)(z+\tau) = wz-\eta+(w+z+\varepsilon)\tau$. Set $\alpha = p^v(z+\tau)$ and $\beta = wz-\eta+(w+z+\varepsilon)\tau$. We infer that $I = p^{u+x}(p^{v+y}\mathbb{Z}+p^y(w+\tau)\mathbb{Z}+\alpha\mathbb{Z}+\beta\mathbb{Z})$.

Moreover, $p^y(w+\tau)\mathbb{Z}+\alpha\mathbb{Z} = p^y(w-z)\mathbb{Z}+\alpha\mathbb{Z}$. Observe that $s\alpha+t\beta = p^g z - t(z^2+\varepsilon z+\eta)+p^g\tau$. Set $k = z - t\frac{z^2+\varepsilon z+\eta}{p^g}$. Then $s\alpha+t\beta = p^g(k+\tau)$. We have $\alpha - p^v(k+\tau) = tp^{v-g}(z^2+\varepsilon z+\eta)$ and $(w+z+\varepsilon)(k+\tau)-\beta = sp^{v-g}(z^2+\varepsilon z+\eta)$. Set $r = p^{v-g}(z^2+\varepsilon z+\eta)$. Consequently, $\alpha\mathbb{Z}+\beta\mathbb{Z} = sr\mathbb{Z}+tr\mathbb{Z}+p^g(k+\tau)\mathbb{Z} = r\mathbb{Z}+p^g(k+\tau)\mathbb{Z}$, since $\gcd(s,t)=1$. Putting these facts together gives us $I = p^{u+x}(p^{v+y}\mathbb{Z}+p^y(w-z)\mathbb{Z}+r\mathbb{Z}+p^g(k+\tau)\mathbb{Z})$.

We have $\gcd(p^{v+y}, p^y(w-z), r) = p^\ell$ with $\ell = \min\{v+y, y+\mathrm{v}_p(w-z), v-g+\mathrm{v}_p(z^2+\varepsilon z+\eta)\}$ and $p^{v+y}\mathbb{Z}+p^y(w-z)\mathbb{Z}+r\mathbb{Z} = p^\ell\mathbb{Z}$. Note that $\ell = v+y-g+\min\{g, \mathrm{v}_p(w-z)-v+g, \mathrm{v}_p(z^2+\varepsilon z+\eta)-y\}$ and $\mathrm{v}_p(w-z)-v+g = \min\{\mathrm{v}_p(w-z), \mathrm{v}_p(w-z)+\mathrm{v}_p(w+z+\varepsilon)-v\} = \min\{\mathrm{v}_p(w-z), \mathrm{v}_p(w^2+\varepsilon w+\eta-(z^2+\varepsilon z+\eta))-v\}$, and hence $\ell = v+y-g+\min\{g, \mathrm{v}_p(w-z), \mathrm{v}_p(w^2+\varepsilon w+\eta-(z^2+\varepsilon z+\eta))-v, \mathrm{v}_p(z^2+\varepsilon z+\eta)-y\}$.

CASE 1: $\mathrm{v}_p(w^2+\varepsilon w+\eta) \ge \mathrm{v}_p(z^2+\varepsilon z+\eta)$. Then $\mathrm{v}_p(w^2+\varepsilon w+\eta)-v \ge \mathrm{v}_p(z^2+\varepsilon z+\eta)-y$ and $\mathrm{v}_p(w^2+\varepsilon w+\eta-(z^2+\varepsilon z+\eta))-v \ge \mathrm{v}_p(z^2+\varepsilon z+\eta)-y$.

CASE 2: $\mathrm{v}_p(z^2+\varepsilon z+\eta) > \mathrm{v}_p(w^2+\varepsilon w+\eta)$. Then $\mathrm{v}_p(w^2+\varepsilon w+\eta-(z^2+\varepsilon z+\eta))-v = \mathrm{v}_p(w^2+\varepsilon w+\eta)-v$.

In any case we have $\min\{\mathrm{v}_p(w^2+\varepsilon w+\eta-(z^2+\varepsilon z+\eta))-v, \mathrm{v}_p(z^2+\varepsilon z+\eta)-y\} = \min\{\mathrm{v}_p(w^2+\varepsilon w+\eta)-v, \mathrm{v}_p(z^2+\varepsilon z+\eta)-y\}$. Obviously, $\ell = v+y+e-g$ and $I = p^{u+x+g}(p^{v+y+e-2g}\mathbb{Z}+(z-t\frac{z^2+\varepsilon z+\eta}{p^g}+\tau)\mathbb{Z})$. Consequently, $I = p^a(p^b\mathbb{Z}+(c+\tau)\mathbb{Z})$.

So far we know that $*$ is an inner binary operation on $\mathcal{M}_{f,p}$. It follows from Proposition 3.1.1 that $\xi_{f,p}$ is surjective. It follows from [25, Theorem 5.4.2] that $\xi_{f,p}$ is injective. It is clear that $(\mathcal{I}_p(\mathcal{O}_f),\cdot)$ is a reduced monoid. We have shown that $\xi_{f,p}$ maps products of elements of $\mathcal{M}_{f,p}$ to products of elements of $\mathcal{I}_p(\mathcal{O}_f)$. It is clear that $(0,0,0)$ is an identity element of $\mathcal{M}_{f,p}$ and $\xi_{f,p}(0,0,0) = \mathcal{O}_f$. Therefore, $(\mathcal{M}_{f,p},*)$ is a reduced monoid and $\xi_{f,p}$ is a monoid isomorphism.

2. Let $w,z \in \mathbb{Z}$ be such that $\mathrm{v}_p(w^2+\varepsilon w+\eta) > 0$ and $\mathrm{v}_p(z^2+\varepsilon z+\eta) > 0$. Then $p \mid z^2+\varepsilon z+\eta = \frac{1}{4}((2z+\varepsilon)^2 - f^2 d_K)$, and hence $p \mid 2z+\varepsilon$. Moreover $p \mid w^2+\varepsilon w+\eta-(z^2+\varepsilon z+\eta) = (w+z+\varepsilon)(w-z)$, and thus $p \mid w+z+\varepsilon$ or $p \mid w-z$. Since $p \mid 2z+\varepsilon$, we infer that $p \mid w+z+\varepsilon$ if and only if $p \mid w-z$. Consequently, $\min\{\mathrm{v}_p(w+z+\varepsilon), \mathrm{v}_p(w-z)\} > 0$.

3. By 1., there are $(u,v,w),(x,y,z),(a,b,c) \in \mathcal{M}_{f,p}$ such that $I = p^u(p^v\mathbb{Z}+(w+\tau)\mathbb{Z})$, $J = p^x(p^y\mathbb{Z}+(z+\tau)\mathbb{Z})$, and $IJ = p^a(p^b\mathbb{Z}+(c+\tau)\mathbb{Z})$ with $a = u+x+g$, $b = v+y+e-2g$, $g = \min\{v, y, \mathrm{v}_p(w+z+\varepsilon)\}$ and $e = \min\{g, \mathrm{v}_p(w-z), \mathrm{v}_p(w^2+\varepsilon w+\eta)-v, \mathrm{v}_p(z^2+\varepsilon z+\eta)-y\}$. It follows by Proposition 3.1.1 that $\mathcal{N}(I) = p^{2u+v}$, $\mathcal{N}(J) = p^{2x+y}$, and $\mathcal{N}(IJ) = p^{2a+b} = p^{2(u+x)+v+y+e}$. It is obvious that $\mathcal{N}(I)\mathcal{N}(J) \mid \mathcal{N}(IJ)$. Moreover, $\mathcal{N}(IJ) = \mathcal{N}(I)$

$\mathcal{N}(J)$ if and only if $e = 0$. We infer by 2. that $e = 0$ if and only if $v = 0$ or $y = 0$ or $\mathrm{v}_p(w^2 + \varepsilon w + \eta) = v$ or $\mathrm{v}_p(z^2 + \varepsilon z + \eta) = y$, which is the case if and only if $I$ is invertible or $J$ is invertible by Proposition 3.1.2. If $I$ and $J$ are proper, then $u + v > 0$ and $x + y > 0$, and hence $a > 0$ by 2. This implies that $IJ \subset p(p^b\mathbb{Z} + (c + \tau)\mathbb{Z}) \subset p\mathcal{O}_f$.

4. Let $I \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$. Without restriction let $I$ be not invertible. We have $I = p^b\mathbb{Z} + (r + \tau)\mathbb{Z}$ for some $(0, b, r) \in \mathcal{M}_{f,p}$ and $b < \mathrm{v}_p(r^2 + \varepsilon r + \eta)$. Set $c = \mathrm{v}_p(r^2 + \varepsilon r + \eta)$ and $I' = p^c\mathbb{Z} + (r + \tau)\mathbb{Z}$. Then $I' \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, $\mathcal{N}(I) \mid \mathcal{N}(I')$, and $\mathcal{N}(I) < \mathcal{N}(I')$ by Proposition 3.1. There is some $(x, y, z) \in \mathcal{M}_{f,p}$ such that $J = p^x(p^y\mathbb{Z} + (z + \tau)\mathbb{Z})$. Then $\mathcal{N}(I'J) = p^{c+2x+y}$ and $\mathcal{N}(IJ) = p^{b+2x+y+e}$ with $e = \min\{b, y, \mathrm{v}_p(r + z + \varepsilon), \mathrm{v}_p(r - z), c - b, \mathrm{v}_p(z^2 + \varepsilon z + \eta) - y\} \le c - b$. Therefore, $\mathcal{N}(IJ) \mid \mathcal{N}(I'J)$.

5. Let $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. If $I = p\mathcal{O}_f$, then $\overline{I} = p\mathcal{O}_f$ and $\mathcal{N}(I) = p^2$ by Proposition 3.1.1. Therefore, $I\overline{I} = \mathcal{N}(I)\mathcal{O}_f$. Now let $I \neq p\mathcal{O}_f$. There is some $(0, m, r) \in \mathcal{M}_{f,p}$ such that $I = p^m\mathbb{Z} + (r + \tau)\mathbb{Z}$. Set $s = p^m - r - \varepsilon$. It follows that $\overline{I} = p^m\mathbb{Z} + (r + \overline{\tau})\mathbb{Z} = p^m\mathbb{Z} + (r + \varepsilon - \tau)\mathbb{Z} = p^m\mathbb{Z} + (s + \tau)\mathbb{Z}$. Observe that $s^2 + \varepsilon s + \eta = r^2 + \varepsilon r + \eta + p^m(p^m - (2r + \varepsilon))$. Since $p \mid r^2 + \varepsilon r + \eta = \frac{1}{4}((2r + \varepsilon)^2 - f^2 d_K)$, we have $\mathrm{v}_p(2r + \varepsilon) > 0$, and hence $\mathrm{v}_p(p^m(p^m - (2r + \varepsilon))) > m$. Since $\mathrm{v}_p(r^2 + \varepsilon r + \eta) = m$, we infer that $\mathrm{v}_p(s^2 + \varepsilon s + \eta) = m$, and thus $(0, m, s) \in \mathcal{M}_{f,p}$. Therefore, $\overline{I} \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. Note that $\min\{m, \mathrm{v}_p(r + s + \varepsilon)\} = m$, and thus $I\overline{I} = p^m\mathcal{O}_f = \mathcal{N}(I)\mathcal{O}_f$ by 1. and Proposition 3.1.1. □

**Proposition 3.3.** *Let $p$ be a prime divisor of $f$ and $f' = p^{\mathrm{v}_p(f)}$. Set $\mathcal{O} = \mathcal{O}_f$, $\mathcal{O}' = \mathcal{O}_{f'}$, $P = P_{f,p}$ and $P' = P_{f',p}$. For $g \in \mathbb{N}$ let $\varphi_{g,p} : \mathcal{I}_p(\mathcal{O}_g) \to \mathcal{I}((\mathcal{O}_g)_{P_{g,p}})$ be defined by $\varphi_{g,p}(I) = I_{P_{g,p}}$ and $\zeta_{g,p} : \mathcal{I}((\mathcal{O}_g)_{P_{g,p}}) \to \mathcal{I}_p(\mathcal{O}_g)$ be defined by $\zeta_{g,p}(J) = J \cap \mathcal{O}_g$.*

1. $\mathcal{O}_P = \mathcal{O}'_{P'}$.
2. *$\varphi_{f,p}$ and $\zeta_{f,p}$ are mutually inverse monoid isomorphisms.*
3. *There is a monoid isomorphism $\delta : \mathcal{I}_p(\mathcal{O}) \to \mathcal{I}_p(\mathcal{O}')$ such that $\delta(p\mathcal{O}) = p\mathcal{O}'$ and $\delta_{|\mathcal{I}_p^*(\mathcal{O})} : \mathcal{I}_p^*(\mathcal{O}) \to \mathcal{I}_p^*(\mathcal{O}')$ is a monoid isomorphism.*

*Proof.* 1. It is clear that $\mathcal{O} \subset \mathcal{O}'$ and $P' \cap \mathcal{O} = P$. Therefore, $\mathcal{O}_P \subset \mathcal{O}'_{P'}$. Observe that $\mathcal{O} \setminus P = (\mathbb{Z} \setminus p\mathbb{Z}) + f\omega\mathbb{Z}$ and $\mathcal{O}' \setminus P' = (\mathbb{Z} \setminus p\mathbb{Z}) + f'\omega\mathbb{Z}$. It remains to show that $\{f'\omega\} \cup \{x^{-1} \mid x \in (\mathbb{Z} \setminus p\mathbb{Z}) + f'\omega\mathbb{Z}\} \subset \mathcal{O}_P$. Since $\frac{f}{f'} f'\omega = f\omega \in \mathcal{O}$ and $\frac{f}{f'} \in \mathbb{Z} \setminus p\mathbb{Z} \subset \mathcal{O} \setminus P$, we have $f'\omega \in \mathcal{O}_P$. Therefore, $\mathcal{O}' \subset \mathcal{O}_P$. Now let $a \in \mathbb{Z} \setminus p\mathbb{Z}$ and $b \in \mathbb{Z}$. Observe that $a + bf'\overline{\omega} \in \mathcal{O}' \subset \mathcal{O}_P$. Since $\omega + \overline{\omega}, \omega\overline{\omega} \in \mathbb{Z}$, we have $(a + bf'\omega)(a + bf'\overline{\omega}) = a^2 + abf'(\omega + \overline{\omega}) + b^2(f')^2\omega\overline{\omega} \in \mathbb{Z} \setminus p\mathbb{Z} \subset \mathcal{O} \setminus P$. Therefore, $\frac{1}{a + bf'\omega} = \frac{a + bf'\overline{\omega}}{(a + bf'\omega)(a + bf'\overline{\omega})} \in \mathcal{O}_P$.

2. It is clear that $\varphi_{f,p}$ is a well-defined monoid homomorphism. Note that $\zeta_{f,p}$ is a well-defined map (since every nonzero proper ideal $J$ of $\mathcal{O}_P$ is $P_P$-primary, and hence $J \cap \mathcal{O}$ is $P$-primary). Moreover, $\zeta_{f,p}(\mathcal{O}_P) = \mathcal{O}$. Now let $J_1, J_2 \in \mathcal{I}(\mathcal{O}_P)$. Observe that $J_1J_2 \cap \mathcal{O}$ and $(J_1 \cap \mathcal{O})(J_2 \cap \mathcal{O})$ coincide locally (note that both are either $P$-primary or not proper). Therefore, $J_1J_2 \cap \mathcal{O} = (J_1 \cap \mathcal{O})(J_2 \cap \mathcal{O})$, and hence $\zeta_{f,p}$ is a monoid homomorphism. If $J \in \mathcal{I}(\mathcal{O}_P)$, then $(J \cap \mathcal{O})_P = J$. Therefore,

$\varphi_{f,p} \circ \zeta_{f,p} = \mathrm{id}_{\mathcal{I}(\mathcal{O}_P)}$. If $I$ is a $P$-primary ideal of $\mathcal{O}$, then $I_P \cap \mathcal{O} = I$. This implies that $\zeta_{f,p} \circ \varphi_{f,p} = \mathrm{id}_{\mathcal{I}_p(\mathcal{O})}$.

3. Set $\delta = \zeta_{f',p} \circ \varphi_{f,p}$. Then $\delta : \mathcal{I}_p(\mathcal{O}) \to \mathcal{I}_p(\mathcal{O}')$ is a monoid isomorphism by 1. and 2. Furthermore, we have by 1. that $\delta(p\mathcal{O}) = \zeta_{f',p}(\varphi_{f,p}(p\mathcal{O})) = \zeta_{f',p}(p\mathcal{O}_P) = \zeta_{f',p}(p\mathcal{O}'_{P'}) = p\mathcal{O}'_{P'} \cap \mathcal{O}' = p\mathcal{O}'$.

Since $\mathcal{O}$ is noetherian, we have $\mathcal{I}_p^*(\mathcal{O})$ is the set of cancellative elements of $\mathcal{I}_p(\mathcal{O})$. It follows by analogy that $\mathcal{I}_p^*(\mathcal{O}')$ is the set of cancellative elements of $\mathcal{I}_p(\mathcal{O}')$. Therefore, $\delta(\mathcal{I}_p^*(\mathcal{O})) = \mathcal{I}_p^*(\mathcal{O}')$, and hence $\delta_{|\mathcal{I}_p^*(\mathcal{O})}$ is a monoid isomorphism. □

**Lemma 3.4.** *Let $p$ be a prime number, let $k \in \mathbb{N}_0$, let $c, n \in \mathbb{N}$ be such that* $\gcd(c, p) = 1$ *and for each $\ell \in \mathbb{N}$ let* $g_\ell = |\{y \in [0, p^\ell - 1] \mid y^2 \equiv c \mod p^\ell\}|$.

1. *If $p \neq 2$, then $p^k c$ is a square modulo $p^n$ if and only if $k \geq n$ or ($k < n$, $k$ is even and $(\frac{c}{p}) = 1$).*
2. *$2^k c$ is a square modulo $2^n$ if and only if one of the following conditions holds.*
   (a) *$k \geq n$.*
   (b) *$k$ is even and $n = k + 1$.*
   (c) *$k$ is even, $n = k + 2$ and $c \equiv 1 \mod 4$.*
   (d) *$k$ is even, $n \geq k + 3$ and $c \equiv 1 \mod 8$.*
3. *If $\ell \in \mathbb{N}$, then* $g_\ell = \begin{cases} 4 & \text{if } p = 2, \ell \geq 3, c \equiv 1 \mod 8 \\ 2 & \text{if } (p \neq 2, (\frac{c}{p}) = 1) \text{ or } (p = 2, \ell = 2, c \equiv 1 \mod 4) \\ 1 & \text{if } p = 2, \ell = 1 \\ 0 & \text{else} \end{cases}$.

*Proof.* Note that $p^k c$ is a square modulo $p^n$ if and only if $k \geq n$ or ($k < n$, $k$ is even and $c$ is a square modulo $p^{n-k}$).

1. Let $p \neq 2$. It remains to show that if $\ell \in \mathbb{N}$, then $c$ is a square modulo $p^\ell$ if and only if $(\frac{c}{p}) = 1$. If $\ell \in \mathbb{N}$ and $c$ is a square modulo $p^\ell$, then $c$ is a square modulo $p$, and hence $(\frac{c}{p}) = 1$. Now let $(\frac{c}{p}) = 1$. It suffices to show by induction that $c$ is a square modulo $p^\ell$ for all $\ell \in \mathbb{N}$. The statement is clearly true for $\ell = 1$. Now let $\ell \in \mathbb{N}$ and let $x \in \mathbb{Z}$ be such that $x^2 \equiv c \mod p^\ell$. Without restriction let $\mathrm{v}_p(x^2 - c) = \ell$. Note that $p \nmid x$, and hence $2bx \equiv -1 \mod p$ for some $b \in \mathbb{Z}$. Set $y = x + b(x^2 - c)$. Then $y^2 \equiv c \mod p^{\ell+1}$.

2. It remains to show that if $\ell \in \mathbb{N}$, then $c$ is a square modulo $2^\ell$ if and only if $\ell = 1$ or ($\ell = 2$ and $c \equiv 1 \mod 4$) or ($\ell \geq 3$ and $c \equiv 1 \mod 8$). Let $\ell \in \mathbb{N}$ and let $c$ be a square modulo $2^\ell$. If $\ell = 2$, then $c$ is a square modulo 4 and $c \equiv 1 \mod 4$. Moreover, if $\ell \geq 3$, then $c$ is a square modulo 8 and $c \equiv 1 \mod 8$.

Clearly, if $\ell = 1$ or ($\ell = 2$ and $c \equiv 1 \mod 4$), then $c$ is a square modulo $2^\ell$. Now let $c \equiv 1 \mod 8$. It is sufficient to show by induction that $c$ is a square modulo $2^\ell$ for each $\ell \in \mathbb{N}_{\geq 3}$. The statement is obviously true for $\ell = 3$. Now let $\ell \in \mathbb{N}_{\geq 3}$ and let $x \in \mathbb{Z}$ be such that $x^2 \equiv c \mod 2^\ell$. Without restriction let $\mathrm{v}_2(x^2 - c) = \ell$. Set $y = x + 2^{\ell-1}$. Then $y^2 \equiv c \mod 2^{\ell+1}$.

3. Let $\ell \in \mathbb{N}$. By 1. and 2., it is sufficient to consider the case $g_\ell > 0$. Let $g_\ell > 0$. Observe that $g_\ell = |\{y \in [0, p^\ell - 1] \mid y^2 \equiv 1 \mod p^\ell\}| = |\{y \in (\mathbb{Z}/p^\ell\mathbb{Z})^\times \mid \mathrm{ord}(y) \le 2\}|$. If $p = 2$ and $\ell = 1$, then $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$ is trivial, and hence $g_\ell = 1$. If $(p = 2, \ell = 2$ and $c \equiv 1 \mod 4)$ or $(p \ne 2$ and $(\frac{c}{p}) = 1)$, then $(\mathbb{Z}/p^\ell\mathbb{Z})^\times$ is a cyclic group of even order, and thus $g_\ell = 2$. Finally, if $p = 2$, $\ell \ge 3$ and $c \equiv 1 \mod 8$, then $(\mathbb{Z}/2^\ell\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathcal{C}_{2^{\ell-2}}$ is the product of two cyclic groups of even order. Consequently, $g_\ell = 4$. □

**Lemma 3.5.** *Let $p$ be a prime number, $a, m \in \mathbb{N}$, $c = \frac{a}{p^{\mathrm{v}_p(a)}}$, $M = \{x \in [0, p^m - 1] \mid \mathrm{v}_p(x^2 - a) = m\}$, $N = |M|$ and for each $\ell \in \mathbb{N}$ let $g_\ell = |\{y \in [0, p^\ell - 1] \mid y^2 \equiv c \mod p^\ell\}|$.*

1. *If $m < \mathrm{v}_p(a)$, then* $N = \begin{cases} \varphi(p^{m/2}) & \text{if } m \text{ is even} \\ 0 & \text{if } m \text{ is odd} \end{cases}$.
2. *Let $m = \mathrm{v}_p(a)$.*
   (a) *If $a$ is a square modulo $p^{m+1}$, then* $N = \begin{cases} p^{m/2-1}(p-2) & \text{if } p \ne 2 \\ 2^{m/2-1} & \text{if } p = 2 \end{cases}$.
   (b) *If $a$ is not a square modulo $p^{m+1}$, then $N = p^{\lfloor m/2 \rfloor}$.*
3. *If $m > \mathrm{v}_p(a)$ and $a$ is not a square modulo $p^m$, then $N = 0$.*
4. *If $k \in \mathbb{N}$ is such that $m = k + \mathrm{v}_p(a)$ and $a$ is a square modulo $p^m$, then $N = p^{\mathrm{v}_p(a)/2-1}(pg_k - g_{k+1})$.*

*Proof.* 1. Let $m < \mathrm{v}_p(a)$. Observe that $M = \{x \in [0, p^m - 1] \mid 2\mathrm{v}_p(x) = m\}$. Clearly, if $m$ is odd, then $N = 0$. Now let $m$ be even. We have $M = \{p^{m/2}y \mid y \in [0, p^{m/2} - 1], \gcd(y, p) = 1\}$, and thus $N = |\{y \in [0, p^{m/2} - 1] \mid \gcd(y, p) = 1\}| = \varphi(p^{m/2})$.

2. Note that $M = \{x \in [0, p^m - 1] \mid 2\mathrm{v}_p(x) \ge m, x^2 \not\equiv a \mod p^{m+1}\}$ and $|\{x \in [0, p^m - 1] \mid 2\mathrm{v}_p(x) \ge m\}| = p^{\lfloor m/2 \rfloor}$. Set $M' = \{x \in [0, p^m - 1] \mid x^2 \equiv a \mod p^{m+1}\}$. Then $M' = \{x \in [0, p^m - 1] \mid 2\mathrm{v}_p(x) \ge m, x^2 \equiv a \mod p^{m+1}\}$ and $N = p^{\lfloor m/2 \rfloor} - |M'|$. If $a$ is not a square modulo $p^{m+1}$, then $M' = \emptyset$, and hence $N = p^{\lfloor m/2 \rfloor}$. Now let $a$ be a square modulo $p^{m+1}$. Then $M' \ne \emptyset$, and thus $m$ is even. Observe that $M' = \{x \in [0, p^m - 1] \mid 2\mathrm{v}_p(x) = m, x^2 \equiv a \mod p^{m+1}\} = \{p^{m/2}y \mid y \in [0, p^{m/2} - 1], y^2 \equiv c \mod p\}$. Therefore, $|M'| = |\{y \in [0, p^{m/2} - 1] \mid y^2 \equiv c \mod p\}| = p^{m/2-1}|\{y \in [0, p - 1] \mid y^2 \equiv c \mod p\}|$.

If $p \ne 2$, then $N = p^{\lfloor m/2 \rfloor} - |M'| = p^{m/2} - 2p^{m/2-1} = p^{m/2-1}(p-2)$ by Lemma 3.4.3. Moreover, if $p = 2$, then $N = 2^{\lfloor m/2 \rfloor} - |M'| = 2^{m/2} - 2^{m/2-1} = 2^{m/2-1}$ by Lemma 3.4.3.

3. This is obvious.

4. Let $k \in \mathbb{N}$ be such that $m = k + \mathrm{v}_p(a)$ and let $a$ be a square modulo $p^m$. It follows by Lemma 3.4 that $\mathrm{v}_p(a)$ is even. Set $r = \mathrm{v}_p(a)/2$ and for $\theta \in \{0, 1\}$ set $M_\theta = \{x \in [0, p^m - 1] \mid 2\mathrm{v}_p(x) = \mathrm{v}_p(a), x^2 \equiv a \mod p^{m+\theta}\}$. Then $M = \{x \in [0, p^m - 1] \mid \mathrm{v}_p(x) = r, \mathrm{v}_p(x^2 - a) = m\} = M_0 \setminus M_1$. Since $\{x \in [0, p^m - 1] \mid \mathrm{v}_p(x) = r\} = \{p^r y \mid y \in [0, p^{k+r} - 1], \gcd(y, p) = 1\}$, we infer that $M_\theta = \{p^r y \mid y \in$

$[0, p^{k+r} - 1]$, $y^2 \equiv c \mod p^{k+\theta}\}$. Therefore, $|M_\theta| = |\{y \in [0, p^{k+r} - 1] \mid y^2 \equiv c \mod p^{k+\theta}\}| = p^{r-\theta}|\{y \in [0, p^{k+\theta} - 1] \mid y^2 \equiv c \mod p^{k+\theta}\}| = p^{r-\theta} g_{k+\theta}$. This implies that $N = |M_0| - |M_1| = p^r g_k - p^{r-1} g_{k+1} = p^{r-1}(pg_k - g_{k+1})$. □

**Theorem 3.6.** *Let $\mathcal{O}$ be an order in a quadratic number field $K$ with conductor $\mathfrak{f} = f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$, $p$ be a prime divisor of $f$, and $\mathfrak{p} = P_{f,p}$.*

1. *The primary ideals with radical $\mathfrak{p}$ are exactly the ideals of the form*

$$\mathfrak{q} = p^\ell(p^m\mathbb{Z} + (r + \tau)\mathbb{Z})$$

   *with $\ell, m \in \mathbb{N}_0$, $\ell + m \geq 1$, $0 \leq r < p^m$, and $\mathcal{N}_{K/\mathbb{Q}}(r + \tau) \equiv 0 \mod p^m$. Moreover, $\mathcal{N}(\mathfrak{q}) = p^{2\ell+m}$.*
2. *A primary ideal $\mathfrak{q} = p^\ell(p^m\mathbb{Z} + (r + \tau)\mathbb{Z})$ is invertible if and only if*

$$\mathcal{N}_{K/\mathbb{Q}}(r + \tau) \not\equiv 0 \mod p^{m+1}.$$

3. *A primary ideal $\mathfrak{q}$ with radical $\mathfrak{p}$ is an ideal atom if and only if $\mathfrak{q} = p\mathcal{O}$ or $\mathfrak{q} = p^m\mathbb{Z} + (r + \tau)\mathbb{Z}$ with $m \in \mathbb{N}$ and $p^m \mid \mathcal{N}_{K/\mathbb{Q}}(r + \tau)$.*
4. *Table 1 gives the number of invertible ideal atoms of the form $p^m\mathbb{Z} + (r + \tau)\mathbb{Z}$ with norm $p^m$; this number is $0$ if $m$ is not listed in the table.*

**Table 1** Number of nontrivial invertible $\mathfrak{p}$-primary ideal atoms

| $m$ | $2h$, $1 \leq h < \mathrm{v}_p(f)$ | $2\mathrm{v}_p(f)$ | $2\mathrm{v}_p(f) + 1$ | $> 2\mathrm{v}_p(f) + 1$ |
|---|---|---|---|---|
| $p$ is inert | $\varphi\left(p^{m/2}\right)$ | $p^{\mathrm{v}_p(f)}$ | | 0 |
| $p$ is ramified | | | $p^{\mathrm{v}_p(f)}$ | |
| $p$ splits | | $p^{\mathrm{v}_p(f)-1}(p-2)$ | $2\varphi\ p^{\mathrm{v}_p(f)}$ | |

5. *The number of ideal atoms with radical $\mathfrak{p}$ is finite if and only if the number of invertible ideal atoms with radical $\mathfrak{p}$ is finite if and only if $p$ does not split.*

*Proof.* 1. and 2. are an immediate consequence of Proposition 3.1.

3. In 1. we have seen, that all $\mathfrak{p}$-primary ideals of $\mathcal{O}$ are of the form $\mathfrak{q} = p^\ell(p^m\mathbb{Z} + (r + \tau)\mathbb{Z})$. If both $\ell$ and $m$ are greater than 0, then $\mathfrak{q}$ is not an ideal atom. Indeed, $\mathfrak{q} = (p\mathcal{O})^\ell(p^m\mathbb{Z} + (r + \tau)\mathbb{Z})$ is a nontrivial factorization. It remains to be proven that $p\mathcal{O}$ and $p^m\mathbb{Z} + (r + \tau)\mathbb{Z}$ are ideal atoms.

Assume that there exist proper ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of $\mathcal{O}$ such that $p\mathcal{O} = \mathfrak{a}_1\mathfrak{a}_2$. Since $p\mathcal{O}$ is $\mathfrak{p}$-primary, we have $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are $\mathfrak{p}$-primary. Using this information, we deduce that $p\mathcal{O} \subset \mathfrak{p}^2$, implying

$$p \in p\mathcal{O} \subset \mathfrak{p}^2 = (p^2, pf\omega, f^2\omega^2) = p(p, f\omega, \frac{f}{p}\omega f\omega) = p(p, f\omega) = p\mathfrak{p}.$$

Therefore, $1 \in \mathfrak{p}$, a contradiction.

Assume that there exist proper ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of $\mathcal{O}$ such that $p^m\mathbb{Z} + (r+\tau)\mathbb{Z} = \mathfrak{a}_1\mathfrak{a}_2$. Note that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are $\mathfrak{p}$-primary. By Proposition 3.2.3, it follows that $p^m\mathbb{Z} + (r+\tau)\mathbb{Z} \subset p\mathcal{O}$, a contradiction to $r+\tau \notin p\mathcal{O}$.

4. By 1. and 3., the nontrivial $\mathfrak{p}$-primary ideal atoms of norm $p^m$ are all $\mathfrak{q} = p^m\mathbb{Z} + (r+\tau)\mathbb{Z}$ with $m \in \mathbb{N}$, $0 \le r < p^m$ and $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) \equiv 0 \mod p^m$. By 2., an ideal of this form is invertible if and only if $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) \not\equiv 0 \mod p^{m+1}$.

Thus if we want to count the number of invertible $\mathfrak{p}$-primary ideal atoms of the form $\mathfrak{q} = p^m\mathbb{Z} + (r+\tau)\mathbb{Z}$, we have to count the number of solutions $r \in [0, p^m - 1]$ of the equation

$$\mathrm{v}_p(\mathcal{N}_{K/\mathbb{Q}}(r+\tau)) = m. \tag{3.1}$$

Set $N = |\{r \in [0, p^m-1] \mid \mathrm{v}_p(\mathcal{N}_{K/\mathbb{Q}}(r+\tau)) = m\}|$ and $a = \begin{cases} (\frac{f}{2})^2 d_K & \text{if } p = 2 \\ f^2 d_K & \text{if } p \neq 2 \end{cases}$.
Next we show that $N = |\{r \in [0, p^m-1] \mid \mathrm{v}_p(r^2 - a) = m\}|$. Note that $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) = \frac{(2r+\varepsilon)^2 - f^2 d_K}{4}$ for each $r \in [0, p^m-1]$. If $p = 2$, then $\varepsilon = 0$, and hence $\mathcal{N}_{K/\mathbb{Q}}(r+\tau) = r^2 - a$. Now let $p \neq 2$. Then $\mathrm{v}_p(\mathcal{N}_{K/\mathbb{Q}}(r+\tau)) = \mathrm{v}_p((2r+\varepsilon)^2 - a)$ for each $r \in [0, p^m-1]$. Let $f : \{r \in [0, p^m-1] \mid \mathrm{v}_p(r^2-a) = m\} \to \{r \in [0, p^m-1] \mid \mathrm{v}_p((2r+\varepsilon)^2 - a) = m\}$ and $g : \{r \in [0, p^m-1] \mid \mathrm{v}_p((2r+\varepsilon)^2 - a) = m\} \to \{r \in [0, p^m-1] \mid \mathrm{v}_p(r^2-a) = m\}$ be defined by $f(r) = \begin{cases} \frac{r-\varepsilon}{2} & \text{if } r-\varepsilon \text{ is even} \\ \frac{r+p^m-\varepsilon}{2} & \text{if } r-\varepsilon \text{ is odd} \end{cases}$ and $g(r) = \mathrm{rem}(2r+\varepsilon, p^m)$ for each $r \in [0, p^m-1]$. Observe that $f$ and $g$ are well-defined injective maps. Therefore, $N = |\{r \in [0, p^m-1] \mid \mathrm{v}_p(r^2-a) = m\}|$ in any case. Set $c = \frac{a}{p^{\mathrm{v}_p(a)}}$ and for $\ell \in \mathbb{N}$ set $g_\ell = |\{y \in [0, p^\ell - 1] \mid y^2 \equiv c \mod p^\ell\}|$. If $m < \mathrm{v}_p(a)$, then the statement follows immediately by Lemma 3.5.1. Therefore, let $m \ge \mathrm{v}_p(a)$. In what follows we use Lemmas 3.4 and 3.5 without further citation.

CASE 1: $p = 2$ and 2 is inert. We have $\mathrm{v}_2(a) = 2\mathrm{v}_2(f) - 2$, $c \equiv d_K \equiv 5 \mod 8$, $g_1 = 1$, $g_2 = 2$ and $g_3 = 0$. If $m = \mathrm{v}_2(a)$, then $a$ is a square modulo $2^{m+1}$, and hence $N = 2^{m/2-1} = \varphi(2^{m/2})$. If $m = \mathrm{v}_2(a)+1$, then $a$ is a square modulo $2^m$, and thus $N = 2^{\mathrm{v}_2(a)/2-1}(2g_1 - g_2) = 0$. If $m = \mathrm{v}_2(a)+2$, then $a$ is a square modulo $2^m$, whence $N = 2^{\mathrm{v}_2(a)/2-1}(2g_2 - g_3) = 2^{\mathrm{v}_2(a)/2+1} = 2^{\mathrm{v}_2(f)}$. Finally, let $m \ge \mathrm{v}_2(a)+3$. Then $a$ is not a square modulo $2^m$, and hence $N = 0$.

CASE 2: $p = 2$ and 2 is ramified. Note that $\mathrm{v}_2(a) \in \{2\mathrm{v}_2(f), 2\mathrm{v}_2(f)+1\}$. First let $\mathrm{v}_2(a) = 2\mathrm{v}_2(f)$. Then $a = f^2 d$ with $c \equiv d \equiv 3 \mod 4$, $g_1 = 1$ and $g_\ell = 0$ for each $\ell \in \mathbb{N}_{\ge 2}$. If $m = \mathrm{v}_2(a)$, then $a$ is a square modulo $2^{m+1}$, and thus $N = 2^{m/2-1} = 2^{\mathrm{v}_2(f)-1} = \varphi(2^{\mathrm{v}_2(f)})$. If $m = \mathrm{v}_2(a)+1$, then $a$ is a square modulo $2^m$, and hence $N = 2^{\mathrm{v}_2(a)/2-1}(2g_1 - g_2) = 2^{\mathrm{v}_2(f)}$. Finally, let $m \ge \mathrm{v}_2(a)+2$. Then $a$ is not a square modulo $2^m$, and thus $N = 0$.

Now let $\mathrm{v}_2(a) = 2\mathrm{v}_2(f)+1$. If $m = \mathrm{v}_2(a)$, then $a$ is not a square modulo $2^{m+1}$, and hence $N = 2^{\lfloor m/2 \rfloor} = 2^{\mathrm{v}_2(f)}$. If $m > \mathrm{v}_2(a)$, then $a$ is not a square modulo $2^m$, and thus $N = 0$.

CASE 3: $p = 2$ and 2 splits. Observe that $\mathrm{v}_2(a) = 2\mathrm{v}_2(f) - 2$, $c \equiv d_K \equiv 1 \mod 8$, $g_1 = 1$, $g_2 = 2$ and $g_\ell = 4$ for each $\ell \in \mathbb{N}_{\geq 3}$. If $m = \mathrm{v}_2(a)$, then $a$ is a square modulo $2^{m+1}$, and hence $N = 2^{m/2-1} = \varphi(2^{m/2})$. Now let $m > \mathrm{v}_2(a)$ and set $k = m - \mathrm{v}_2(a)$. Note that $a$ is a square modulo $2^m$, and hence $N = 2^{\mathrm{v}_2(a)/2-1}(2g_k - g_{k+1})$. If $m < \mathrm{v}_2(a) + 3$, then $N = 0$. Finally, let $m \geq \mathrm{v}_2(a) + 3$. Then $N = 2^{\mathrm{v}_2(a)/2+1} = 2^{\mathrm{v}_2(f)} = 2\varphi(2^{\mathrm{v}_2(f)})$.

CASE 4: $p \neq 2$ and $p$ is inert. We have $\mathrm{v}_p(a) = 2\mathrm{v}_p(f)$, $(\frac{c}{p}) = (\frac{d_K}{p}) = -1$ and $g_\ell = 0$ for each $\ell \in \mathbb{N}$. If $m = \mathrm{v}_p(a)$, then $a$ is not a square modulo $p^{m+1}$, and hence $N = p^{\lfloor m/2 \rfloor} = p^{\mathrm{v}_p(f)}$. If $m > \mathrm{v}_p(a)$, then $a$ is not a square modulo $p^m$, and thus $N = 0$.

CASE 5: $p \neq 2$ and $p$ is ramified. It follows that $\mathrm{v}_p(a) = 2\mathrm{v}_p(f) + 1$. If $m = \mathrm{v}_p(a)$, then $a$ is not a square modulo $p^{m+1}$, and thus $N = p^{\lfloor m/2 \rfloor} = p^{\mathrm{v}_p(f)}$. If $m > \mathrm{v}_p(a)$, then $a$ is not a square modulo $p^m$, and thus $N = 0$.

CASE 6: $p \neq 2$ and $p$ splits. Note that $\mathrm{v}_p(a) = 2\mathrm{v}_p(f)$, $(\frac{c}{p}) = (\frac{d_K}{p}) = 1$ and $g_\ell = 2$ for each $\ell \in \mathbb{N}$. If $m = \mathrm{v}_p(a)$, then $a$ is a square modulo $p^{m+1}$, and hence $N = p^{m/2-1}(p-2) = p^{\mathrm{v}_p(f)-1}(p-2)$. If $m > \mathrm{v}_p(a)$, then $a$ is a square modulo $p^m$, and thus $N = p^{\mathrm{v}_p(a)/2-1}(pg_k - g_{k+1}) = 2p^{\mathrm{v}_p(f)-1}(p-1) = 2\varphi(p^{\mathrm{v}_p(f)})$.

5. It is an immediate consequence of 4. that the number of invertible ideal atoms with radical $\mathfrak{p}$ is finite if and only if $p$ does not split. It remains to show that $\mathcal{A}(\mathcal{I}_p(\mathcal{O}))$ is finite if and only if $\mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ is finite. It follows from [1, Theorem 4.3] that $\mathcal{I}(\mathcal{O}_\mathfrak{p})$ is a finitely generated monoid if and only if $\mathcal{I}^*(\mathcal{O}_\mathfrak{p})$ is a finitely generated monoid. Therefore, Proposition 3.3.2 implies that $\mathcal{I}_p(\mathcal{O})$ is a finitely generated monoid if and only if $\mathcal{I}_p^*(\mathcal{O})$ is a finitely generated monoid. Observe that $\mathcal{I}_p(\mathcal{O})$ and $\mathcal{I}_p^*(\mathcal{O})$ are atomic monoids. Therefore, $\mathcal{A}(\mathcal{I}_p(\mathcal{O}))$ is finite if and only if $\mathcal{I}_p(\mathcal{O})$ is a finitely generated monoid if and only if $\mathcal{I}_p^*(\mathcal{O})$ is a finitely generated monoid if and only if $\mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ is finite. □

## 4 Sets of Distances and Sets of Catenary Degrees

The goal in this section is to prove Theorem 1.1. The proof is based on the precise description of ideals given in Theorem 3.6. We proceed in a series of lemmas and propositions and use all notation on orders as introduced at the beginning of Section 3. In particular, $\mathcal{O} = \mathcal{O}_f$ is an order in a quadratic number with conductor $f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$.

**Proposition 4.1.** *Let $H$ be a reduced atomic monoid and suppose there is a cancellative atom $u \in \mathcal{A}(H)$ such that for each $a \in H \setminus H^\times$ there are $n \in \mathbb{N}_0$ and $v \in \mathcal{A}(H)$ such that $a = u^n v$.*

1. *For all $n, m \in \mathbb{N}_0$ and $v, w \in \mathcal{A}(H)$ such that $u^n v = u^m w$, it follows that $n = m$ and $v = w$.*
2. *For all $n \in \mathbb{N}_0$ and $v \in \mathcal{A}(H)$, it follows that* $\max \mathsf{L}(u^n v) = n + 1$.

3. $\mathsf{c}(H) = \sup\{\mathsf{c}(w \cdot y, u^n \cdot v) \mid n \in \mathbb{N}$ *and* $v, w, y \in \mathcal{A}(H)$ *such that* $wy = u^n v\}$.
4. *If* $H$ *is half-factorial, then* $\mathsf{c}(H) \le 2$.
5. $\sup \Delta(H) = \sup\{\ell - 2 \mid \ell \in \mathbb{N}_{\ge 3}$ *such that* $\mathsf{L}(vw) \cap [2, \ell] = \{2, \ell\}$ *for some* $v, w \in \mathcal{A}(H)\}$.

*Proof.* 1. Let $n, m \in \mathbb{N}_0$ and $v, w \in \mathcal{A}(H)$ be such that $u^n v = u^m w$. Without restriction let $n \le m$. Since $u$ is cancellative, we infer that $v = u^{m-n} w$. Since $v \in \mathcal{A}(H)$, we have $n = m$, and thus $v = w$.

2. It is clear that $n + 1 \in \mathsf{L}(u^n v)$ for all $n \in \mathbb{N}_0$ and $v \in \mathcal{A}(H)$. Therefore, it is sufficient to show by induction that for all $n \in \mathbb{N}_0$ and $v \in \mathcal{A}(H)$, $\max \mathsf{L}(u^n v) \le n + 1$. Let $n \in \mathbb{N}_0$ and $v \in \mathcal{A}(H)$. If $n = 0$, then the assertion is obviously true. Now let $n > 0$ and $z \in \mathsf{Z}(u^n v)$. Then there are some $z', z'' \in \mathsf{Z}(H) \setminus \{1\}$ such that $z = z' \cdot z''$. There are some $m', m'' \in \mathbb{N}_0$ and $w', w'' \in \mathcal{A}(H)$ such that $\pi(z') = u^{m'} w'$ and $\pi(z'') = u^{m''} w''$. There are some $\ell \in \mathbb{N}$ and $y \in \mathcal{A}(H)$ such that $w'w'' = u^\ell y$. We infer that $u^n v = u^{m'+m''+\ell} y$, and thus $n = m' + m'' + \ell$ by 1. Since $m', m'' < n$, it follows by the induction hypothesis that $|z'| \le m' + 1$ and $|z''| \le m'' + 1$. Consequently, $|z| \le m' + m'' + 2 \le m' + m'' + \ell + 1 = n + 1$.

3. Set $k = \sup\{\mathsf{c}(w \cdot y, u^n \cdot v) \mid n \in \mathbb{N}_0$ and $v, w, y \in \mathcal{A}(H)$ such that $wy = u^n v\}$. Since $\mathsf{c}(H) = \sup\{\mathsf{c}(z, z') \mid a \in H, z, z' \in \mathsf{Z}(a)\}$, it is obvious that $k \le \mathsf{c}(H)$. It remains to show by induction that for all $n \in \mathbb{N}_0$ and $v \in \mathcal{A}(H)$, it follows that $\mathsf{c}(u^n v) \le k$. Let $n \in \mathbb{N}_0$ and $v \in \mathcal{A}(H)$. Since $\mathsf{c}(v) = 0$, we can assume without restriction that $n > 0$. Since $\mathsf{c}(u^n v) = \sup\{\mathsf{c}(z, u^n \cdot v) \mid z \in \mathsf{Z}(u^n v)\}$, it remains to show that $\mathsf{c}(z, u^n \cdot v) \le k$ for all $z \in \mathsf{Z}(u^n v)$. Let $z \in \mathsf{Z}(u^n v)$.

CASE 1: For all $w, y \in \mathcal{A}(H) \setminus \{u\}$, we have $w \cdot y \nmid z$. There are some $m \in \mathbb{N}$ and $w \in \mathcal{A}(H)$ such that $z = u^m \cdot w$. We infer by 1. that $z = u^n \cdot v$, and thus $\mathsf{c}(z, u^n \cdot v) = 0 \le k$.

CASE 2: There are some $w, y \in \mathcal{A}(H) \setminus \{u\}$ such that $w \cdot y \mid z$. Set $z' = \frac{z}{w \cdot y}$. There exist $m \in \mathbb{N}$ and $a \in \mathcal{A}(H)$ such that $wy = u^m a$. We infer that $m \le n$ and $u^n v = \pi(z) = \pi(w \cdot y)\pi(z') = u^m a \pi(z')$, and thus $a\pi(z') = u^{n-m} v$. Observe that $\mathsf{c}(z, u^m \cdot a \cdot z') \le \mathsf{c}(w \cdot y, u^m \cdot a) \le k$. Since $n - m < n$, it follows by the induction hypothesis that $\mathsf{c}(u^m \cdot a \cdot z', u^n \cdot v) \le \mathsf{c}(a \cdot z', u^{n-m} \cdot v) \le k$, and hence $\mathsf{c}(z, u^n \cdot v) \le k$.

4. Let $H$ be half-factorial, $n \in \mathbb{N}$ and $v, w, y \in \mathcal{A}(H)$ be such that $wy = u^n v$. We infer that $n = 1$, and thus $\mathsf{c}(w \cdot y, u^n \cdot v) \le \mathsf{d}(w \cdot y, u \cdot v) \le 2$. Therefore, $\mathsf{c}(H) \le 2$ by 3.

5. Set $N = \sup\{\ell - 2 \mid \ell \in \mathbb{N}_{\ge 3}$ such that $\mathsf{L}(vw) \cap [2, \ell] = \{2, \ell\}$ for some $v, w \in \mathcal{A}(H)\}$. It is obvious that $N \le \sup \Delta(H)$. It remains to show that $k \le N$ for each $k \in \Delta(H)$. Let $k \in \Delta(H)$. Then there are some $a \in H$ and $r, s \in \mathsf{L}(a)$ such that $r < s$, $\mathsf{L}(a) \cap [r, s] = \{r, s\}$, and $k = s - r$. Let $z \in \mathsf{Z}(a)$ with $|z| = r$ be such that $\mathrm{v}_u(z) = \max\{\mathrm{v}_u(z') \mid z' \in \mathsf{Z}(a)$ with $|z'| = r\}$. Since $r < \max \mathsf{L}(a)$, it follows by 2., that there are some $v, w \in \mathcal{A}(H) \setminus \{u\}$ such that $v \cdot w \mid z$. There are some $n \in \mathbb{N}$ and $y \in \mathcal{A}(H)$ such that $vw = u^n y$. Since $\mathrm{v}_u(z)$ is maximal among all factorizations of $a$ of length $r$, we have $n \ge 2$. Consequently, there is some $\ell \in \mathsf{L}(vw)$ such that

$2 < \ell \le n+1$ and $\mathsf{L}(vw) \cap [2, \ell] = \{2, \ell\}$. Note that $r + \ell - 2 \in \mathsf{L}(a)$, and thus $s \le r + \ell - 2$. This implies that $k \le \ell - 2 \le N$. □

Theorem 3.6 implies that, for all prime divisors $p$ of $f$, $\mathcal{I}_p^*(\mathcal{O}_f)$ and $\mathcal{I}_p(\mathcal{O}_f)$ are reduced atomic monoids satisfying the assumption in Proposition 4.1.

**Lemma 4.2.** *Let $p$ be a prime divisor of $f$.*

1. $\mathsf{Z}(pP_{f,p}) = \{A \cdot P_{f,p} \mid A = P_{f,p}$ *or* $A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ *such that* $\mathcal{N}(A) = p^2\}$ *and* $1 \in \mathrm{Ca}(\mathcal{I}_p(\mathcal{O}_f))$.
2. *If* $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ *are such that* $\mathcal{N}(I) = p^2$ *and* $\mathcal{N}(J) > p^2$, *then* $IJ = pL$ *for some* $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$.
3. $2 \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$.

*Proof.* 1. Note that $\{I \in \mathcal{I}_p(\mathcal{O}_f) \mid \mathcal{N}(I) = p\} = \{P_{f,p}\}$. First we show that $\mathsf{Z}(pP_{f,p}) = \{A \cdot P_{f,p} \mid A = P_{f,p}$ or $A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(A) = p^2\}$.

Let $z \in \mathsf{Z}(pP_{f,p})$. It follows from Proposition 4.1.2 that $|z| \le 2$, and hence $|z| = 2$. Consequently, $z = A \cdot B$ for some $A, B \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$. By Proposition 3.2.1 there are some $(u, v, w), (x, y, t) \in \mathcal{M}_{f,p}$ such that $A = p^u(p^v\mathbb{Z} + (w+\tau)\mathbb{Z})$ and $B = p^x(p^y\mathbb{Z} + (t+\tau)\mathbb{Z})$. Set $g = \min\{v, y, \mathrm{v}_p(w+t+\varepsilon)\}$ and $e = \min\{g, \mathrm{v}_p(w-t), \mathrm{v}_p(w^2+\varepsilon w+\eta) - v, \mathrm{v}_p(t^2+\varepsilon t+\eta) - y\}$. We infer by Proposition 3.2.1 that $u + x + g = 1$ and $v + y + e - 2g = 1$. Note that $g \in \{0, 1\}$. If $g = 0$, then $u + x = v + y = 1$, and thus ($A = p\mathcal{O}_f$ and $B = P_{f,p}$) or ($A = P_{f,p}$ and $B = p\mathcal{O}_f$). Now let $g = 1$. Then $u = x = 0$, $v, y \ge 1$, $v + y + e = 3$, and $e \in \{0, 1\}$. If $e = 1$, then $v = y = 1$, and thus $A = B = P_{f,p}$. Now let $e = 0$. Then ($v = 1$ and $y = 2$) or ($v = 2$ and $y = 1$). Without restriction let $v = 2$ and $y = 1$. Then $B = P_{f,p}$, $\mathcal{N}(A) = p^v = p^2$, and $\mathcal{N}(A)\mathcal{N}(B) = p^3 = \mathcal{N}(pP_{f,p}) = \mathcal{N}(AB)$. Since $B$ is not invertible, it follows by Proposition 3.2.3 that $A$ is invertible.

To prove the converse inclusion note that $P_{f,p} = p\mathbb{Z} + (r+\tau)\mathbb{Z}$ for some $(0, 1, r) \in \mathcal{M}_{f,p}$. By Proposition 3.2.1 we have $P_{f,p}^2 = p^a(p^b\mathbb{Z} + (c+\tau)\mathbb{Z}$ with $(a, b, c) \in \mathcal{M}_{f,p}$, $a = \min\{1, \mathrm{v}_p(2r+\varepsilon)\}$ and $b = 2 + e - 2a$ with $e = \min\{a, \mathrm{v}_p(r^2+\varepsilon r+\eta) - 1\}$. By Proposition 3.2.3 we have $a > 0$, and thus $a = b = e = 1$. Consequently, $P_{f,p}^2 = pP_{f,p}$. Now let $A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ be such that $\mathcal{N}(A) = p^2$. It follows by Proposition 3.2.3 that $\mathcal{N}(AP_{f,p}) = \mathcal{N}(A)\mathcal{N}(P_{f,p}) = p^3$ and $AP_{f,p} = pI$ for some $I \in \mathcal{I}_p(\mathcal{O}_f)$. We infer that $\mathcal{N}(I) = p$, and hence $I = P_{f,p}$.

Observe that $\mathsf{d}(z', z'') \le 1$ for all $z', z'' \in \mathsf{Z}(pP_{f,p})$ and $(p\mathcal{O}_f) \cdot P_{f,p}$ and $P_{f,p}^2$ are distinct factorizations of $pP_{f,p}$. Therefore, $1 = \mathsf{c}(pP_{f,p}) \in \mathrm{Ca}(\mathcal{I}_p(\mathcal{O}_f))$.

2. Let $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ be such that $\mathcal{N}(I) = p^2$ and $\mathcal{N}(J) > p^2$. Without restriction we can assume that $I \ne p\mathcal{O}_f$. There are some $(0, 2, r), (0, k, s) \in \mathcal{M}_{f,p}$ such that $I = p^2\mathbb{Z} + (r+\tau)\mathbb{Z}$ and $J = p^k\mathbb{Z} + (s+\tau)\mathbb{Z}$. Since $I$ and $J$ are invertible, we have $\mathrm{v}_p(r^2+\varepsilon r+\eta) = 2$ and $\mathrm{v}_p(s^2+\varepsilon s+\eta) = k > 2$. Therefore, $\mathrm{v}_p(r+s+\varepsilon) + \mathrm{v}_p(r-s) = \mathrm{v}_p(r^2+\varepsilon r+\eta - (s^2+\varepsilon s+\eta)) = 2$, and thus $\mathrm{v}_p(r+s+\varepsilon) = 1$, by Proposition 3.2.2. Therefore, $\min\{2, k, \mathrm{v}_p(r+s+\varepsilon)\} = 1$, and hence $IJ = pL$ for some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ by Proposition 3.2.1.

3. We distinguish two cases.

CASE 1: $p \neq 2$ or $\mathrm{v}_p(f) \geq 2$ or $d \not\equiv 1 \mod 8$. It follows from Theorem 3.6 that there is some $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = p^2$ and $I \neq p\mathcal{O}_f$. We have $I\overline{I} = (p\mathcal{O}_f)^2$, and hence $\mathsf{L}(I\overline{I}) = \{2\}$. Since $I \cdot \overline{I}$ and $(p\mathcal{O}_f) \cdot (p\mathcal{O}_f)$ are distinct factorizations of $I\overline{I}$, we have $2 = \mathsf{c}(I\overline{I}) \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$.

CASE 2: $p = 2$, $\mathrm{v}_p(f) = 1$ and $d \equiv 1 \mod 8$. By Proposition 3.3.3 we can assume without restriction that $f = 2$. By Theorem 3.6 there is some $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = 8$. There is some $(0, 3, r) \in \mathcal{M}_{f,2}$ such that $I = 8\mathbb{Z} + (r + \tau)\mathbb{Z}$. We have $\mathrm{v}_2(r^2 - d) = 3$, and hence $\mathrm{v}_2(r) = 0$. Therefore, $\min\{3, \mathrm{v}_2(2r)\} = 1$, and thus $I^2 = 2J$ for some $J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. Consequently, $\mathsf{L}(I^2) = \{2\}$. Since $I \cdot I$ and $(2\mathcal{O}_f) \cdot J$ are distinct factorizations of $I^2$, it follows that $2 = \mathsf{c}(I^2) \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$. □

**Proposition 4.3.** *Let $p$ be an odd prime divisor of $f$ such that $\mathrm{v}_p(f) \geq 2$.*

1. *There is a $C \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathsf{L}(C^2) = \{2, 3\}$ whence $1 \in \Delta(\mathcal{I}_p^*(\mathcal{O}_f))$ and $3 \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$. Moreover, if ($p \neq 3$ or $d \not\equiv 2 \mod 3$ or $\mathrm{v}_p(f) > 2$), then there are $I, J, L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $I^2 = p^2 J$ and $J^2 = p^2 L$.*
2. *If $|\mathrm{Pic}(\mathcal{O}_f)| \leq 2$ and ($p \neq 3$ or $d \not\equiv 2 \mod 3$ or $\mathrm{v}_p(f) > 2$), then there is a nonzero primary $a \in \mathcal{O}_f$ such that $2, 3 \in \mathsf{L}(a)$ whence $1 \in \Delta(\mathcal{O}_f)$.*

*Proof.* 1. By Proposition 3.3.3 there is a monoid isomorphism $\delta : \mathcal{I}_p^*(\mathcal{O}_f) \to \mathcal{I}_p^*(\mathcal{O}_{\frac{f}{2^{\mathrm{v}_2(f)}}})$ such that $\delta(p\mathcal{O}_f) = p\mathcal{O}_{\frac{f}{2^{\mathrm{v}_2(f)}}}$. Therefore, we can assume without restriction that $f$ is odd.

CLAIM: $\mathsf{L}(I^2) = \{2, 3\}$ for some $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, $1 \in \Delta(\mathcal{I}_p^*(\mathcal{O}_f))$, $3 \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$ and if $\mathrm{v}_p(p^4 + f^2 d) = 4$, then $I^2 = p^2 J$ and $J^2 = p^2 L$ for some $I, J, L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$.

For $r \in \mathbb{N}_0$ set $k = \mathrm{v}_p(\mathcal{N}_{K/\mathbb{Q}}(r + \tau))$ and $I = p^k\mathbb{Z} + (r + \tau)\mathbb{Z}$. Let $k > 0$ and $r < p^k$. Then $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. Moreover, $I^2 = p^a(p^b\mathbb{Z} + (c + \tau)\mathbb{Z})$ with $a = \min\{k, \mathrm{v}_p(2r + \varepsilon)\}$, $b = 2(k - a)$ and $c = \mathrm{rem}(r - t\frac{\mathcal{N}_{K/\mathbb{Q}}(r+\tau)}{p^a}, p^b)$ for each $t \in \mathbb{Z}$ with $t\frac{2r+\varepsilon}{p^a} \equiv 1 \mod p^{k-a}$. Set $J = p^b\mathbb{Z} + (c + \tau)\mathbb{Z}$. Then $I^2 = p^a J$ and if $b > 0$, then $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. In particular, if $a = 2$ and $b > 0$, then $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ and $\mathsf{L}(I^2) = \{2, 3\}$, and hence $1 \in \Delta(I^2) \subset \Delta(\mathcal{I}_p^*(\mathcal{O}_f))$ and $3 = \mathsf{c}(I^2) \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$. Observe that $J^2 = p^{a'}(p^{b'}\mathbb{Z} + (c' + \tau)\mathbb{Z})$ with $a' = \min\{b, \mathrm{v}_p(2c + \varepsilon)\}$, $b' = 2(b - a')$ and $c' \in \mathbb{N}_0$ such that $c' < p^{b'}$. Set $L = p^{b'}\mathbb{Z} + (c' + \tau)\mathbb{Z}$. Then $J^2 = p^{a'} L$ and if $b' > 0$, then $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$.

CASE 1: $d \not\equiv 1 \mod 4$. Set $r = p^2$. We have $\mathcal{N}_{K/\mathbb{Q}}(r + \tau) = p^4 - f^2 d$, $k \geq 4$, $a = 2$, $b = 2(k - 2) > 0$, $r < p^k$, and $t = \frac{p^{k-2}+1}{2}$ satisfies the congruence. Therefore, $c = \mathrm{rem}(p^2 - \frac{(p^{k-2}+1)(p^4 - f^2 d)}{2p^2}, p^{2(k-2)}) = \frac{p^4 + f^2 d + p^{k-2} f^2 d - p^{k+2} + 2\ell p^{2(k-1)}}{2p^2}$ for some $\ell \in \mathbb{Z}$. For the rest of this case let $\mathrm{v}_p(p^4 + f^2 d) = 4$. It follows that $\mathrm{v}_p(c) = 2$, and hence $a' = \min\{2(k - 2), \mathrm{v}_p(2c)\} = 2$ and $b' = 4(k - 3) > 0$.

CASE 2: $d \equiv 1 \mod 4$. Set $r = \frac{p^2-1}{2}$. Observe that $\mathcal{N}_{K/\mathbb{Q}}(r + \tau) = \frac{p^4 - f^2 d}{4}$, $k \geq 4$, $a = 2$, $b = 2(k - 2) > 0$, $r < p^k$, and $t = 1$ satisfies the congruence. Consequently, $2c + \varepsilon = 2\mathrm{rem}(\frac{p^2-1}{2} - \frac{p^4 - f^2 d}{4p^2}, p^{2(k-2)}) + 1 = \frac{p^4 + f^2 d + 4\ell p^{2(k-1)}}{2p^2}$ for some

$\ell \in \mathbb{Z}$. For the rest of this case let $\mathsf{v}_p(p^4 + f^2 d) = 4$. We infer that $a' = \min\{2(k-2), \mathsf{v}_p(2c+\varepsilon)\} = 2$. Moreover, $b' = 4(k-3) > 0$. This proves the claim.

Note that if $g \in \mathbb{N}$ with $\mathsf{v}_p(g) = \mathsf{v}_p(f)$, then there is a monoid isomorphism $\alpha : \mathcal{I}_p^*(\mathcal{O}_f) \to \mathcal{I}_p^*(\mathcal{O}_g)$ such that $\alpha(p\mathcal{O}_f) = p\mathcal{O}_g$ by Proposition 3.3.3. By the claim it remains to show that if ($p \neq 3$ or $d \not\equiv 2 \mod 3$ or $\mathsf{v}_p(f) > 2$), then there is some odd $g \in \mathbb{N}$ such that $\mathsf{v}_p(g) = \mathsf{v}_p(f)$ and $\mathsf{v}_p(p^4 + g^2 d) = 4$.

Let ($p \neq 3$ or $d \not\equiv 2 \mod 3$ or $\mathsf{v}_p(f) > 2$). Furthermore, let $\mathsf{v}_p(p^4 + f^2 d) > 4$. This implies that $\mathsf{v}_p(f) = 2$ and $p \nmid d$. Without restriction we can assume that $\mathsf{v}_p(p^4 + (p^2)^2 d) > 4$. We have $\mathsf{v}_p(1+d) > 0$, and hence $p \neq 3$. Set $g = (p-2)p^2$. Then $\mathsf{v}_p(g) = \mathsf{v}_p(f)$. Assume that $\mathsf{v}_p(p^4 + g^2 d) > 4$. Then $p^5 \mid p^4 + (p-2)^2 p^4 d - p^4(1+d)$, and thus $p \mid (p-2)^2 - 1 = p^2 - 4p + 3$. It follows that $p = 3$, a contradiction.

2. Let $|\mathrm{Pic}(\mathcal{O}_f)| \le 2$ and let $p \neq 3$ or $d \not\equiv 2 \mod 3$ or $\mathsf{v}_p(f) > 2$. By 1. there are some $I, J, L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $I^2 = p^2 J$ and $J^2 = p^2 L$. We infer that $I^2$ is principal, and hence $J$ and $L$ are principal. Consequently, there are some $u, v \in \mathcal{A}(\mathcal{O}_f)$ such that $J = u\mathcal{O}_f$, $L = v\mathcal{O}_f$ and $u^2 = p^2 v$. Note that $u^2$ is primary. Since $p \in \mathcal{A}(\mathcal{O}_f)$, we have $2, 3 \in \mathsf{L}(u^2)$. Therefore, $1 \in \Delta(\mathcal{O}_f)$. □

**Proposition 4.4.** *Let $p$ be a prime divisor of $f$ such that $\mathsf{v}_p(f) \ge 2$. Then there are $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathsf{L}(IJ) = \{2, 4\}$ whence $2 \in \Delta(\mathcal{I}_p^*(\mathcal{O}_f))$ and $4 \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$.*

*Proof.* CASE 1: $p \neq 2$ or $\mathsf{v}_p(f) > 2$ or $d \not\equiv 1 \mod 8$. By Theorem 3.6 there is some $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = p^4$. Set $J = \overline{I}$. We infer that $IJ = (p\mathcal{O}_f)^4$, and hence $\{2, 4\} \subset \mathsf{L}(IJ) \subset \{2, 3, 4\}$. Assume that $3 \in \mathsf{L}(IJ)$. Then there are some $A, B, C \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $IJ = ABC$ and $\mathcal{N}(A) \le \mathcal{N}(B) \le \mathcal{N}(C)$. Again by Theorem 3.6 we have $\mathcal{N}(L) \in \{p^2\} \cup \{p^n \mid n \in \mathbb{N}_{\ge 4}\}$ for all $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. This implies that $\mathcal{N}(A) = \mathcal{N}(B) = p^2$ and $\mathcal{N}(C) = p^4$. It follows by Lemma 4.2.2 that $ABC = p^2 L$ for some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. Consequently, $L = p^2\mathcal{O}_f$, a contradiction. We infer that $\mathsf{L}(IJ) = \{2, 4\}$ whence $2 \in \Delta(\mathcal{I}_2^*(\mathcal{O}_f))$ and $4 \in \mathrm{Ca}(\mathcal{I}_2^*(\mathcal{O}_f))$.

CASE 2: $p = 2$, $\mathsf{v}_p(f) = 2$ and $d \equiv 1 \mod 8$. Since $\mathcal{I}_2^*(\mathcal{O}_4) \cong \mathcal{I}_2^*(\mathcal{O}_f)$ by Proposition 3.3.3, we can assume without restriction that $f = 4$. We set

$$w = \begin{cases} 6 & \text{if } d \equiv 1 \mod 16 \\ 2 & \text{if } d \equiv 9 \mod 16 \end{cases} \quad \text{and} \quad z = \begin{cases} 18 & \text{if } d \equiv 1 \mod 32 \\ 22 & \text{if } d \equiv 9 \mod 32 \\ 2 & \text{if } d \equiv 17 \mod 32 \\ 6 & \text{if } d \equiv 25 \mod 32 \end{cases}.$$

In any case, we have $\mathsf{v}_2(\mathcal{N}_{K/\mathbb{Q}}(w+\tau)) = 5$ and $\mathsf{v}_2(\mathcal{N}_{K/\mathbb{Q}}(z+\tau)) = 6$. Set $I = 32\mathbb{Z} + (w+\tau)\mathbb{Z}$ and $J = 64\mathbb{Z} + (z+\tau)\mathbb{Z}$. Then $I, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_4))$ and Proposition 3.2.1 implies that $IJ = 2^a(2^b\mathbb{Z} + (c+\tau)\mathbb{Z})$ with $a = \min\{5, 6, \mathsf{v}_2(w+z)\}$, $b = 5 + 6 - 2a$ and $c \in \mathbb{N}_0$ such that $c < 2^b$. Observe that $\mathsf{v}_2(w+z) = 3$, and thus $a = 3$ and $b = 5$. Set $L = 32\mathbb{Z} + (c+\tau)\mathbb{Z}$. Then $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_4))$ and $IJ = (2\mathcal{O}_4)^3 L$. We infer that $\{2, 4\} \subset \mathsf{L}(IJ) \subset \{2, 3, 4\}$, by Proposition 4.1.2.

Assume that $3 \in \mathsf{L}(IJ)$. Then there are some $A, B, C \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_4))$ such that $IJ = ABC$ and $\mathcal{N}(A) \le \mathcal{N}(B) \le \mathcal{N}(C)$. It follows by Theorem 3.6 that $\mathcal{N}(U) \in \{4\} \cup \{2^n \mid n \ge 5\}$ for all $U \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_4))$. Since $\mathcal{N}(A)\mathcal{N}(B)\mathcal{N}(C) = \mathcal{N}(I)\mathcal{N}(J) = 2048$, we infer that $\mathcal{N}(A) = \mathcal{N}(B) = 4$ and $\mathcal{N}(C) = 128$. It follows by Lemma 4.2.2 that $ABC = 4D$ for some $D \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_4))$. This implies that $D = 2L$, a contradiction. Consequently, $\mathsf{L}(IJ) = \{2, 4\}$, and thus $2 \in \Delta(\mathcal{I}_2^*(\mathcal{O}_4))$ and $4 = \mathsf{c}(IJ) \in \mathrm{Ca}(\mathcal{I}_2^*(\mathcal{O}_4))$. $\square$

**Proposition 4.5.** *Suppose that one of the following conditions hold:*

(a) $\mathrm{v}_2(f) \ge 5$ *or* ($\mathrm{v}_2(f) = 4$ *and* $d \not\equiv 1 \mod 4$).
(b) $\mathrm{v}_2(f) = 3$ *and* $d \equiv 2 \mod 4$.
(c) $\mathrm{v}_2(f) = 2$ *and* $d \equiv 1 \mod 4$.

*Then there are* $I, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ *with* $\mathsf{L}(IJ) = \{2, 3\}$ *whence* $1 \in \Delta(\mathcal{I}_2^*(\mathcal{O}_f))$ *and* $3 \in \mathrm{Ca}(\mathcal{I}_2^*(\mathcal{O}_f))$. *If* $|\mathrm{Pic}(\mathcal{O}_f)| \le 2$, *then there is a nonzero primary* $a \in \mathcal{O}_f$ *with* $2, 3 \in \mathsf{L}(a)$ *whence* $1 \in \Delta(\mathcal{O}_f)$.

*Proof.* CASE 1: $\mathrm{v}_2(f) \ge 5$ or ($\mathrm{v}_2(f) = 4$ and $d \not\equiv 1 \mod 4$). We show that there are some $A, B, I, J, L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $A^2 = 32I$, $B^2 = 16J$ and $IJ = 4L$. Set $k = \mathrm{v}_2(\mathcal{N}_{K/\mathbb{Q}}(16 + \tau))$ and $A = 2^k\mathbb{Z} + (16 + \tau)\mathbb{Z}$. Then $k \ge 8$, $A \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $A^2 = 32(2^{2k-10}\mathbb{Z} + (c + \tau)\mathbb{Z})$ with $(5, 2k - 10, c) \in \mathcal{M}_{f,2}$ and $\mathrm{v}_2(c) \ge 3$. Set $I = 2^{2k-10}\mathbb{Z} + (c + \tau)\mathbb{Z}$. Then $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. Set $B = 64\mathbb{Z} + (8 + \tau)\mathbb{Z}$. Then $B \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $B^2 = 16(16\mathbb{Z} + (4 + \tau)\mathbb{Z})$. Set $J = 16\mathbb{Z} + (4 + \tau)\mathbb{Z}$. Then $B^2 = 16J$, $J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $IJ = 4L$ with $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$.

CASE 2: $\mathrm{v}_2(f) = 3$ and $d \equiv 2 \mod 4$. We show that $AB = 2I$, $AC = 2I'$, $BC = 8I''$, $B^2 = 16J$, $IJ = 4L$, $I'J = 4L'$, $I''J = 4L''$ for some $A, B, C, I, I', I'', J, L, L', L'' \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. By Proposition 3.3.3, we can assume without restriction that $f = 8$. Set $A = 4\mathbb{Z} + (2 + \tau)\mathbb{Z}$, $B = 64\mathbb{Z} + (8 + \tau)\mathbb{Z}$ and $C = 128\mathbb{Z} + \tau\mathbb{Z}$. Then $A, B, C \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$, $AB = 2(64\mathbb{Z} + (40 + \tau)\mathbb{Z})$, $AC = 2(128\mathbb{Z} + (64 + \tau)\mathbb{Z})$, $B^2 = 16(16\mathbb{Z} + (12 + \tau)\mathbb{Z})$ and $BC = 8(128\mathbb{Z} + (c + \tau)\mathbb{Z})$ with $(3, 7, c) \in \mathcal{M}_{f,2}$ and $\mathrm{v}_2(c) = 4$. Furthermore, $(64\mathbb{Z} + (40 + \tau)\mathbb{Z})(16\mathbb{Z} + (12 + \tau)\mathbb{Z}) = 4(64\mathbb{Z} + (56 + \tau)\mathbb{Z})$, $(128\mathbb{Z} + (64 + \tau)\mathbb{Z})(16\mathbb{Z} + (12 + \tau)\mathbb{Z}) = 4(128\mathbb{Z} + (r + \tau)\mathbb{Z})$ with $(2, 7, r) \in \mathcal{M}_{f,2}$ and $(128\mathbb{Z} + (c + \tau)\mathbb{Z})(16\mathbb{Z} + (12 + \tau)\mathbb{Z}) = 4(128\mathbb{Z} + (s + \tau)\mathbb{Z})$ with $(2, 7, s) \in \mathcal{M}_{f,2}$. Set $J = 16\mathbb{Z} + (12 + \tau)\mathbb{Z}$. In particular, if $I \in \{64\mathbb{Z} + (40 + \tau)\mathbb{Z}, 128\mathbb{Z} + (64 + \tau)\mathbb{Z}, 128\mathbb{Z} + (c + \tau)\mathbb{Z}\}$, then $I, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $IJ = 4L$ for some $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$.

CASE 3: $\mathrm{v}_2(f) = 2$ and $d \equiv 1 \mod 4$. We show that $A^2 = 4I$ and $I^2 = 4L$ for some $A, I, L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. By Proposition 3.3.3, we can assume without restriction that $f = 4$. First let $d \equiv 1 \mod 8$. If $d \equiv 1 \mod 16$, then set $A = 32\mathbb{Z} + (6 + \tau)\mathbb{Z}$ and if $d \equiv 9 \mod 16$, then set $A = 32\mathbb{Z} + (2 + \tau)\mathbb{Z}$. In any case, we have $A \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $A^2 = 4(64\mathbb{Z} + (c + \tau)\mathbb{Z})$ with $(2, 6, c) \in \mathcal{M}_{f,2}$ and $\mathrm{v}_2(c) = 1$. Set $I = 64\mathbb{Z} + (c + \tau)\mathbb{Z}$. Then $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$, $A^2 = 4I$ and $I^2 = 4(256\mathbb{Z} + (r + \tau)\mathbb{Z})$ with $(2, 8, r) \in \mathcal{M}_{f,2}$.

Now let $d \equiv 5 \mod 8$. Set $A = 16\mathbb{Z} + (2 + \tau)\mathbb{Z}$. Then $A \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $A^2 = 4(16\mathbb{Z} + (c + \tau)\mathbb{Z})$ with $(2, 4, c) \in \mathcal{M}_{f,2}$ and $\mathrm{v}_2(c) = 1$. Set $I = 16\mathbb{Z} + (c + \tau)\mathbb{Z}$. Then $A^2 = 4I$ and $I^2 = 4(16\mathbb{Z} + (z + \tau)\mathbb{Z})$ with $(2, 4, z) \in \mathcal{M}_{f,2}$.

Using the case analysis above we can find $I, J, L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $IJ = 4L$. In particular, $\mathsf{L}(IJ) = \{2, 3\}$, $1 \in \Delta(\mathcal{I}_p^*(\mathcal{O}_f))$ and $3 = \mathsf{c}(IJ) \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$. Now let $|\mathrm{Pic}(\mathcal{O}_f)| \le 2$. Observe that if $A, B, C \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$, then $A^2$ is principal and $\{AB, AC, BC\}$ contains a principal ideal of $\mathcal{O}_f$. In any case we can choose $I, J, L$ to be principal. There are some $u, v, w \in \mathcal{A}(\mathcal{O}_f)$ such that $I = u\mathcal{O}_f$, $J = v\mathcal{O}_f$, $L = w\mathcal{O}_f$ and $uv = 4w$. Note that $uv$ is primary. Since $2 \in \mathcal{A}(\mathcal{O}_f)$, we have $2, 3 \in \mathsf{L}(uv)$, and thus $1 \in \Delta(\mathcal{O}_f)$. □

**Proposition 4.6.** *Let $p$ be a prime divisor of $f$. Then the following statements are equivalent:*

(a) *$\mathcal{I}_p^*(\mathcal{O}_f)$ is half-factorial.*
(b) *$\mathcal{I}_p(\mathcal{O}_f)$ is half-factorial.*
(c) $\mathsf{c}(\mathcal{I}_p^*(\mathcal{O}_f)) = 2$.
(d) $\mathsf{c}(\mathcal{I}_p(\mathcal{O}_f)) = 2$.
(e) $\mathrm{v}_p(f) = 1$ *and $p$ is inert.*

*Proof.* (a) ⇒ (e) If $\mathrm{v}_p(f) > 1$ or $p$ is not inert, then there is some $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) > p^2$ by Theorem 3.6.4. Set $k = \mathrm{v}_p(\mathcal{N}(I))$. Then $k \ge 3$ and $I\overline{I} = (p\mathcal{O}_f)^k$ by Proposition 3.2.5. Since $\overline{I} \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, we have $2, k \in \mathsf{L}(I\overline{I})$.

(e) ⇒ (b) Observe that $\mathcal{N}(A) \in \{p, p^2\}$ for each $A \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$, and thus $\mathcal{A}(\mathcal{I}_p(\mathcal{O}_f)) = \{P_{f,p}\} \cup \{A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f)) \mid \mathcal{N}(A) = p^2\}$. Let $I \in \mathcal{I}_p(\mathcal{O}_f) \setminus \{\mathcal{O}_f\}$. There are some $k \in \mathbb{N}_0$ and $J \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$ such that $I = p^k J$. Let $z \in \mathsf{Z}(I)$. Then $z = (\prod_{i=1}^n I_i) \cdot P_{f,p}^{\ell}$ with $\ell, n \in \mathbb{N}_0$ and $I_i \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ for each $i \in [1, n]$. Note that $|z| = n + \ell$. It is sufficient to show that $n + \ell = k + 1$.

CASE 1: $I$ is invertible. Then $J$ is invertible and $\ell = 0$. It follows that $p^{2n} = \mathcal{N}(\prod_{i=1}^n I_i) = \mathcal{N}(I) = \mathcal{N}(p^k J) = p^{2k+2}$ by Proposition 3.2.3, and thus $n + \ell = n = k + 1$.

CASE 2: $I$ is not invertible. Then $J = P_{f,p}$ and $\ell > 0$. It follows from Lemma 4.2 that $P_{f,p}^{\ell} = p^{\ell-1} P_{f,p}$. Consequently,

$$p^{2(n+\ell)-1} = \mathcal{N}(\prod_{i=1}^n I_i)\mathcal{N}(p^{\ell-1} P_{f,p}) = \mathcal{N}(I) = \mathcal{N}(p^k P_{f,p}) = p^{2k+1}$$

by Proposition 3.2.3, and hence $n + \ell = k + 1$.

(b) ⇒ (d) Since $\mathcal{I}_p^*(\mathcal{O}_f)$ is a cancellative divisor-closed submonoid of $\mathcal{I}_p(\mathcal{O}_f)$ and not factorial, we infer by Proposition 4.1.4 that

$$2 \le \mathsf{c}(\mathcal{I}_p^*(\mathcal{O}_f)) \le \mathsf{c}(\mathcal{I}_p(\mathcal{O}_f)) \le 2.$$

(d) ⇒ (c) Note that $\mathcal{I}_p^*(\mathcal{O}_f)$ is a divisor-closed submonoid of $\mathcal{I}_p(\mathcal{O}_f)$, and thus $\mathsf{c}(\mathcal{I}_p^*(\mathcal{O}_f)) \le \mathsf{c}(\mathcal{I}_p(\mathcal{O}_f)) = 2$. Since $\mathcal{I}_p^*(\mathcal{O}_f)$ is not factorial, we infer that $\mathsf{c}(\mathcal{I}_p^*(\mathcal{O}_f)) = 2$.

(c) $\Rightarrow$ (a) Since $\mathcal{I}_p^*(\mathcal{O}_f)$ is cancellative and not factorial, it follows that $2 + \sup \Delta(\mathcal{I}_p^*(\mathcal{O}_f)) \le \mathsf{c}(\mathcal{I}_p^*(\mathcal{O}_f)) = 2$, and thus $\sup \Delta(\mathcal{I}_p^*(\mathcal{O}_f)) = 0$. Consequently, $\Delta(\mathcal{I}_p^*(\mathcal{O}_f)) = \emptyset$, and hence $\mathcal{I}_p^*(\mathcal{O}_f)$ is half-factorial. □

**Lemma 4.7.** *Let $p$ be a prime divisor of $f$, $|\mathrm{Pic}(\mathcal{O}_f)| \le 2$, $I, J, L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$.*

1. *If $J$ is principal and $IJ = p^2L$, then $1 \in \Delta(\mathcal{O}_f)$.*
2. *If $I$ and $J$ are not principal and $IJ = pL$, then $1 \in \Delta(\mathcal{O}_f)$.*

*Proof.* Note that if $|\mathrm{Pic}(\mathcal{O}_f)| > 1$, then it follows from [16, Corollary 2.11.16] that there is some invertible prime ideal $P$ of $\mathcal{O}_f$ that is not principal. Observe that $p \in \mathcal{A}(\mathcal{O}_f)$. Also note that if $I$ is not principal, then $PI$ is principal, and hence $PI$ is generated by an atom of $\mathcal{O}_f$, since $PI$ has no nontrivial factorizations in $\mathcal{I}^*(\mathcal{O}_f)$.

1. Let $J$ be principal and $IJ = p^2L$. There is some $v \in \mathcal{A}(\mathcal{O}_f)$ such that $J = v\mathcal{O}_f$.

CASE 1: $I$ is principal. Then $L$ is principal, and hence there are some $u, w \in \mathcal{A}(\mathcal{O}_f)$ such that $I = u\mathcal{O}_f$, $L = w\mathcal{O}_f$ and $uv = p^2w$. We infer that $2, 3 \in \mathsf{L}(uv)$, and thus $1 \in \Delta(\mathcal{O}_f)$.

CASE 2: $I$ is not principal. Then $L$ is not principal and $|\mathrm{Pic}(\mathcal{O}_f)| > 1$, and thus there are some $u, w \in \mathcal{A}(\mathcal{O}_f)$ such that $PI = u\mathcal{O}_f$, $PL = w\mathcal{O}_f$ and $uv = p^2w$. It follows that $2, 3 \in \mathsf{L}(uv)$, and thus $1 \in \Delta(\mathcal{O}_f)$.

2. Let $I$ and $J$ not be principal and $IJ = pL$. Then $L$ is principal and $|\mathrm{Pic}(\mathcal{O}_f)| > 1$, and hence there are some $u, v, w, y \in \mathcal{A}(\mathcal{O}_f)$ such that $PI = u\mathcal{O}_f$, $PJ = v\mathcal{O}_f$, $P^2 = w\mathcal{O}_f$, $L = y\mathcal{O}_f$ and $uv = pwy$. Therefore, $2, 3 \in \mathsf{L}(uv)$, and hence $1 \in \Delta(\mathcal{O}_f)$. □

**Proposition 4.8.** *Let $p$ be a prime divisor of $f$.*

1. *If $\mathrm{v}_p(f) \ge 2$ or $p$ is not inert, then there are $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathsf{L}(IJ) = \{2, 3\}$ whence $1 \in \Delta(\mathcal{I}_p^*(\mathcal{O}_f))$ and $3 \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$.*
2. *Suppose that $\mathcal{O}_f$ is not half-factorial and that one of the following conditions holds:*
   (i) *$|\mathrm{Pic}(\mathcal{O}_f)| \ge 3$ or $\mathrm{v}_p(f) \ge 2$ or $p$ does split.*
   (ii) *$p$ is inert and there is some $C \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ that is not principal.*
   (iii) *$p$ is ramified and there is some principal $C \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(C) = p^3$.*
   (iv) *$f$ is a squarefree product of inert primes.*

   *Then $1 \in \Delta(\mathcal{O}_f)$.*

*Proof.* We prove 1. and 2. simultaneously. Set $G = \mathrm{Pic}(\mathcal{O}_f)$. Let $\mathcal{B}(G)$ be the monoid of zero-sum sequences of $G$. It follows by [16, Theorem 6.7.1.2] that if $|G| \ge 3$, then $1 \in \Delta(\mathcal{B}(G))$. We infer by [16, Proposition 3.4.7 and Theorems 3.4.10.3 and 3.7.1.1] that there exists an atomic monoid $\mathcal{B}(\mathcal{O}_f)$ such that $\Delta(\mathcal{B}(\mathcal{O}_f)) = \Delta(\mathcal{O}_f)$ and $\mathcal{B}(G)$ is a divisor-closed submonoid of $\mathcal{B}(\mathcal{O}_f)$. In particular, if $|G| \ge 3$, then

$1 \in \Delta(\mathcal{O}_f)$. Thus, for the second assertion we only need to consider the case $|G| \le 2$. By Propositions 4.3 and 4.5 we can restrict to the following cases.

CASE 1: $p = 2$ and $((\mathrm{v}_2(f) \in \{3, 4\}$ and $d \equiv 1 \mod 4)$ or $(\mathrm{v}_2(f) \in \{2, 3\}$ and $d \equiv 3 \mod 4))$. If $(\mathrm{v}_2(f) = 4$ and $d \equiv 1 \mod 4)$ or $(\mathrm{v}_2(f) = 3$ and $d \equiv 3 \mod 4)$, then set $I = 16\mathbb{Z} + (4 + \tau)\mathbb{Z}$. If $\mathrm{v}_2(f) = 3$ and $d \equiv 1 \mod 4$, then set $I = 16\mathbb{Z} + \tau\mathbb{Z}$. Finally, if $\mathrm{v}_2(f) = 2$ and $d \equiv 3 \mod 4$, then there is some $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = 32$ by Theorem 3.6. In any case, it follows that $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$.

It is a consequence of Proposition 3.2.1 and Theorem 3.6 that there are some $A, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $\ell \in \mathbb{N}$ such that $A^2 = \ell J$ with values according to the following table. Let $k \in \{1, 3, 5, 7\}$ be such that $d \equiv k \mod 8$. Note that $I = 2^a\mathbb{Z} + (r + \tau)\mathbb{Z}$ and $J = 2^b\mathbb{Z} + (s + \tau)\mathbb{Z}$ with $(0, a, r), (0, b, s) \in \mathcal{M}_{f,2}$.

| $\mathrm{v}_2(f)$ | $k$ | $\mathcal{N}(A)$ | $\ell$ | $\mathcal{N}(J)$ | $\mathrm{v}_2(r)$ | $\mathrm{v}_2(s)$ |
|---|---|---|---|---|---|---|
| 4 | 1 | 512 | 16 | 1024 | 2 | 3 |
| 4 | 5 | 256 | 16 | 256 | 2 | 3 |
| 3 | 1 | 128 | 8 | 256 | $\infty$ | 2 |
| 3 | 5 | 64 | 8 | 64 | $\infty$ | 2 |
| 3 | 3 or 7 | 128 | 16 | 64 | 2 | $\ge 4$ |
| 2 | 3 or 7 | 32 | 8 | 16 | 2 | $\ge 3$ |

Since $\mathrm{v}_2(r + s) = 2$ in any case, we infer that $IJ = 4L$ for some $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. Now let $|G| \le 2$. We have $J$ is principal, and hence $1 \in \Delta(\mathcal{O}_f)$ by Lemma 4.7.1.

CASE 2: $p = 2$, $\mathrm{v}_2(f) = 2$ and $d \equiv 2 \mod 4$. Set $A = 32\mathbb{Z} + \tau\mathbb{Z}$ and $B = 32\mathbb{Z} + (8 + \tau)\mathbb{Z}$. Then $A, B \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $AB = 8I$ for some $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ with $I = 16\mathbb{Z} + (r + \tau)\mathbb{Z}$, $(0, 4, r) \in \mathcal{M}_{f,2}$, and $\mathrm{v}_2(r) = 2$. Therefore, we have $AI = 4J$ and $BI = 4L$ for some $J, L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. Now let $|G| \le 2$. Since $\{A, B, I\}$ contains a principal ideal of $\mathcal{O}_f$, we infer by Lemma 4.7.1 that $1 \in \Delta(\mathcal{O}_f)$.

CASE 3: $p = 3$, $\mathrm{v}_3(f) = 2$ and $d \equiv 2 \mod 3$. First let $d \not\equiv 1 \mod 4$. Set $I = 81\mathbb{Z} + \tau\mathbb{Z}$ and $J = 81\mathbb{Z} + (9 + \tau)\mathbb{Z}$. Then $I, J \in \mathcal{A}(\mathcal{I}_3^*(\mathcal{O}_f))$ and $IJ = 9L$ for some $L \in \mathcal{A}(\mathcal{I}_3^*(\mathcal{O}_f))$ with $L = 81\mathbb{Z} + (r + \tau)\mathbb{Z}$, $(0, 4, r) \in \mathcal{M}_{f,3}$, and $\mathrm{v}_3(r) = 2$. It follows that $IL = 9A$ for some $A \in \mathcal{A}(\mathcal{I}_3^*(\mathcal{O}_f))$.

Now let $d \equiv 1 \mod 4$. By Proposition 3.3.3 we can assume without restriction that $f$ is odd. Set $I = 81\mathbb{Z} + (4 + \tau)\mathbb{Z}$ and $J = 81\mathbb{Z} + (13 + \tau)\mathbb{Z}$. Then $I, J \in \mathcal{A}(\mathcal{I}_3^*(\mathcal{O}_f))$ and $IJ = 9L$ for some $L \in \mathcal{A}(\mathcal{I}_3^*(\mathcal{O}_f))$. There is some $(0, 4, r) \in \mathcal{M}_{f,3}$ such that $L = 81\mathbb{Z} + (r + \tau)\mathbb{Z}$. Since $\mathrm{v}_3(2r + 1) \ge 2$, we have $IL = 9A$ for some $A \in \mathcal{A}(\mathcal{I}_3^*(\mathcal{O}_f))$ or $JL = 9A$ for some $A \in \mathcal{A}(\mathcal{I}_3^*(\mathcal{O}_f))$.

In any case if $|G| \le 2$, then $\{I, J, L\}$ contains a principal ideal of $\mathcal{O}_f$, and hence $1 \in \Delta(\mathcal{O}_f)$ by Lemma 4.7.1.

CASE 4: $\mathrm{v}_p(f) = 1$ and $p$ splits. By Theorem 3.6 there is some $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = p^3$. There is some $(0, 3, r) \in \mathcal{M}_{f,p}$ such that $I = p^3\mathbb{Z} + (r + \tau)\mathbb{Z}$. Observe that $\mathrm{v}_p(2r + \varepsilon) = 1$. We infer that $I^2 = pJ$ for some $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$

and $I\overline{I} = p^2L$ with $\overline{I} \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ and $L = p\mathcal{O}_f \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. Now let $|G| \le 2$. We infer by Lemma 4.7 that $1 \in \Delta(\mathcal{O}_f)$.

CASE 5: $\mathrm{v}_p(f) = 1$ and $p$ is ramified. By Theorem 3.6 there is some $C \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(C) = p^3$. Note that $C\overline{C} = p^3\mathcal{O}_f$ and $\overline{C} \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. Now let $C$ be principal. It follows by Lemma 4.7.1 that $1 \in \Delta(\mathcal{O}_f)$.

Cases 1-5 show that there are some $I, J, L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $IJ = p^2L$. In particular, $\mathsf{L}(IJ) = \{2, 3\}$, $1 \in \Delta(\mathcal{I}_p^*(\mathcal{O}_f))$ and $3 = \mathsf{c}(IJ) \in \mathrm{Ca}(\mathcal{I}_p^*(\mathcal{O}_f))$. This proves 1. For the rest of this proof let $\mathcal{O}_f$ be not half-factorial and $|G| \le 2$.

CASE 6: $\mathrm{v}_p(f) = 1$, $p$ is inert and there is some $C \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ that is not principal. We have $C^2 = pL$ for some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, and thus $1 \in \Delta(\mathcal{O}_f)$ by Lemma 4.7.2.

CASE 7: $f$ is a squarefree product of inert primes. Then $\mathcal{I}_p^*(\mathcal{O}_f)$ is half-factorial by Proposition 4.6. If $G$ is trivial, then $\mathcal{O}_f$ is half-factorial, a contradiction. Note that $\mathcal{O}_f$ is seminormal by [10, Corollary 4.5]. It follows from [18, Theorem 6.2.2.(a)] that $1 \in \Delta(\mathcal{O}_f)$. □

**Lemma 4.9.** *Let $p$ be a prime divisor of $f$, $k \in \mathbb{N}_{\ge 2}$, and $N = \sup\{\mathrm{v}_p(\mathcal{N}(A)) \mid A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))\}$. If $\ell \in \mathbb{N}$ and $A \in \mathcal{I}_p(\mathcal{O}_f))$ is both a product of $k$ atoms and a product of $\ell$ atoms, then $\ell \le \frac{kN}{2}$.*

*Proof.* Let $\ell \in \mathbb{N}$ and suppose that a product of $k$ atoms can be written as a product of $\ell$ atoms and set $P = P_{f,p}$. There are some $a, b \in \mathbb{N}_0$, $I_i \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f)) \setminus \{P\}$ for each $[1, b]$ and $J_j \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$ for each $j \in [1, k]$ such that $\ell = a + b$ and $\prod_{j=1}^k J_j = P^a \prod_{i=1}^b I_i$. Note that $p^2 \mid \mathcal{N}(I_i)$ for each $i \in [1, b]$.

CASE 1: $a = 0$. Then $b = \ell$. It follows by induction from Proposition 3.2.4 that there are $J_j' \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ for each $j \in [1, k]$ such that $\mathcal{N}(\prod_{j=1}^k J_j) \mid \mathcal{N}(\prod_{j=1}^k J_j')$. Set $M = \mathrm{lcm}\{\mathcal{N}(J_j') \mid j \in [1, k]\}$. Then $p^{2\ell} \mid \prod_{i=1}^{\ell} \mathcal{N}(I_i) \mid \mathcal{N}(\prod_{i=1}^{\ell} I_i) = \mathcal{N}(\prod_{j=1}^k J_j) \mid \mathcal{N}(\prod_{j=1}^k J_j') = \prod_{j=1}^k \mathcal{N}(J_j') \mid M^k$. This implies that $2\ell \le k\mathrm{v}_p(M) \le kN$, and thus $\ell \le \frac{kN}{2}$.

CASE 2: $a > 0$. By Lemma 4.2 we have $P^a = p^{a-1}P$, and thus $\mathcal{N}(P^a) = p^{2a-1}$. Note that $\prod_{j=1}^k J_j$ is not invertible, and hence one member of the product, say $J_1$, is not invertible. Observe that $\mathrm{v}_p(\mathcal{N}(J_1)) \le N - 1$ by Proposition 3.2.4. We infer by induction from Proposition 3.2.4 that there are $J_j' \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ for each $j \in [2, k]$ such that $\mathcal{N}(\prod_{j=1}^k J_j) \mid \mathcal{N}(J_1 \prod_{j=2}^k J_j')$. Set $M = \mathrm{lcm}\{\mathcal{N}(J_j') \mid j \in [2, k]\}$. Then $p^{2\ell-1} \mid \mathcal{N}(P^a) \prod_{i=1}^b \mathcal{N}(I_i) \mid \mathcal{N}(P^a \prod_{i=1}^b I_i) = \mathcal{N}(\prod_{j=1}^k J_j) \mid \mathcal{N}(J_1 \prod_{j=2}^k J_j') = \mathcal{N}(J_1) \prod_{j=2}^k \mathcal{N}(J_j') \mid \mathcal{N}(J_1)M^{k-1}$. This implies that $2\ell - 1 \le \mathrm{v}_p(\mathcal{N}(J_1)) + (k-1)\mathrm{v}_p(M) \le kN - 1$, and hence $\ell \le \frac{kN}{2}$. □

**Lemma 4.10.** *Let $p$ be a prime divisor of $f$. For every $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, we set $\mathrm{v}_I = \mathrm{v}_p(\mathcal{N}(I))$, and let $\mathcal{B} = \{\mathrm{v}_A \mid A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))\}$.*

1. *For all $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, we have $\mathsf{c}(I \cdot \overline{I}, (p\mathcal{O}_f)^{\mathrm{v}_I}) \le 2 + \sup \Delta(\mathcal{B})$.*

2. *Let* $p = 2$, $d \equiv 1 \mod 8$, *and* $\mathsf{v}_p(f) \geq 4$. *Then* $\mathsf{c}(I \cdot \overline{I}, (p\mathcal{O}_f)^{\mathsf{v}_I}) \leq 4$ *for all* $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$.

*Proof.* 1. It is sufficient to show by induction that for all $n \in \mathbb{N}_{\geq 2}$ and $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ with $\mathsf{v}_I = n$, it follows that $\mathsf{c}(I \cdot \overline{I}, (p\mathcal{O}_f)^n) \leq 2 + \sup \Delta(\mathcal{B})$. Let $n \in \mathbb{N}_{\geq 2}$ and $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ be such that $\mathsf{v}_I = n$. If $n = 2$, then $\mathsf{c}(I \cdot \overline{I}, (p\mathcal{O}_f)^2) \leq \mathsf{d}(I \cdot \overline{I}, (p\mathcal{O}_f)^2) \leq 2 \leq 2 + \sup \Delta(\mathcal{B})$. Now let $n > 2$. Note that $2 = \mathsf{v}_{p\mathcal{O}_f} \in \mathcal{B}$, and hence there is some $k \in \mathcal{B}$ such that $2 \leq k < n$ and $\mathcal{B} \cap [k, n] = \{k, n\}$. Observe that $n - k \in \Delta(\mathcal{B})$. Furthermore, there is some $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $k = \mathsf{v}_J$. Note that $J\overline{J} = (p\mathcal{O}_f)^k$, and thus $I\overline{I} = (p\mathcal{O}_f)^{n-k} J\overline{J}$. By the induction hypothesis, we infer that $c((p\mathcal{O}_f)^{n-k} \cdot J \cdot \overline{J}, (p\mathcal{O}_f)^n) \leq c(J \cdot \overline{J}, (p\mathcal{O}_f)^k) \leq 2 + \sup \Delta(\mathcal{B})$. Since $\mathsf{d}(I \cdot \overline{I}, (p\mathcal{O}_f)^{n-k} \cdot J \cdot \overline{J}) \leq 2 + (n - k) \leq 2 + \sup \Delta(\mathcal{B})$, it follows that $\mathsf{c}(I \cdot \overline{I}, (p\mathcal{O}_f)^n) \leq 2 + \sup \Delta(\mathcal{B})$.

2. By Proposition 3.3.3 we can assume without restriction that $f = 2^{\mathsf{v}_2(f)}$. We show by induction that for all $n \in \mathbb{N}_{\geq 2}$ and $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ with $\mathsf{v}_I = n$, we have $\mathsf{c}(I \cdot \overline{I}, (2\mathcal{O}_f)^n) \leq 4$. Let $n \in \mathbb{N}_{\geq 2}$ and $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ be such that $\mathsf{v}_I = n$. If $n = 2$, then $\mathsf{c}(I \cdot \overline{I}, (2\mathcal{O}_f)^2) \leq \mathsf{d}(I \cdot \overline{I}, (2\mathcal{O}_f)^2) \leq 2 \leq 2 + \sup \Delta(\mathcal{B})$. Next let $n > 2$. Observe that $2 = \mathsf{v}_{2\mathcal{O}_f} \in \mathcal{B}$, and hence there is some $k \in \mathcal{B}$ such that $2 \leq k < n$ and $\mathcal{B} \cap [k, n] = \{k, n\}$. There is some $J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $k = \mathsf{v}_J$. Note that $J\overline{J} = (2\mathcal{O}_f)^k$, and hence $I\overline{I} = (2\mathcal{O}_f)^{n-k} J\overline{J}$. By the induction hypothesis, we have $c((2\mathcal{O}_f)^{n-k} \cdot J \cdot \overline{J}, (2\mathcal{O}_f)^n) \leq c(J \cdot \overline{J}, (2\mathcal{O}_f)^k) \leq 4$.

CASE 1: $n \neq 2\mathsf{v}_2(f) + 1$. It follows from Theorem 3.6 that $n - k \leq 2$. Since $\mathsf{d}(I \cdot \overline{I}, (2\mathcal{O}_f)^{n-k} \cdot J \cdot \overline{J}) \leq 4$, we infer that $\mathsf{c}(I \cdot \overline{I}, (2\mathcal{O}_f)^n) \leq 4$.

CASE 2: $n = 2\mathsf{v}_2(f) + 1$. By Theorem 3.6 we have $n - k = 3$. Set $A = 16\mathbb{Z} + (4 + \tau)\mathbb{Z}$, $B = 2^{n-3}\mathbb{Z} + (2^{n-5} + \tau)\mathbb{Z}$, and $C = 2^{n-3}\mathbb{Z} + (2^{n-4} + \tau)\mathbb{Z}$. Then $A, B, C \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $ABC = 2^{n-5}A(16\mathbb{Z} + (12 + \tau)\mathbb{Z}) = (2\mathcal{O}_f)^{n-1}$. Observe that $\mathsf{d}(I \cdot \overline{I}, (2\mathcal{O}_f) \cdot A \cdot B \cdot C) \leq 4$ and $\mathsf{d}((2\mathcal{O}_f) \cdot A \cdot B \cdot C, (2\mathcal{O}_f)^{n-k} \cdot J \cdot \overline{J})) \leq 4$. Therefore, $\mathsf{c}(I \cdot \overline{I}, (2\mathcal{O}_f)^n) \leq 4$. □

**Proposition 4.11.** *Let* $p$ *be a prime divisor of* $f$ *and set* $\mathcal{B} = \{\mathsf{v}_p(\mathcal{N}(\mathcal{A})) \mid A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))\}$.

1. $\sup \Delta(\mathcal{I}_p(\mathcal{O}_f)) \leq \sup \Delta(\mathcal{B})$ *and* $\mathsf{c}(\mathcal{I}_p(\mathcal{O}_f)) \leq 2 + \sup \Delta(\mathcal{B})$.
2. *Let* $p = 2$, $d \equiv 1 \mod 8$, *and* $\mathsf{v}_p(f) \geq 4$. *Then* $\sup \Delta(\mathcal{I}_2(\mathcal{O}_f)) \leq 2$ *and* $\mathsf{c}(\mathcal{I}_2(\mathcal{O}_f)) \leq 4$.

*Proof.* 1. First we consider the case that $\mathsf{v}_p(f) = 1$ and $p$ is inert. It follows from Theorem 3.6 that $\sup \Delta(\mathcal{B}) = 0$. Proposition 4.6 implies that $\sup \Delta(\mathcal{I}_p(\mathcal{O}_f)) = 0$ and $\mathsf{c}(\mathcal{I}_p(\mathcal{O}_f)) = 2$. Now let $\mathsf{v}_p(f) \geq 2$ or $p$ not inert. Observe that $\sup \Delta(\mathcal{B}) \geq 1$ by Theorem 3.6. Let $I, J \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$. There are some $n \in \mathbb{N}$ and $L \in \mathcal{A}(\mathcal{I}_p(\mathcal{O}_f))$ such that $IJ = p^n L$.

By Proposition 4.1, it remains to show that $\mathsf{c}(I \cdot J, (p\mathcal{O}_f)^n \cdot L) \leq 2 + \sup \Delta(\mathcal{B})$ and if $\ell \in \mathbb{N}_{\geq 3}$ is such that $\mathsf{L}(IJ) \cap [2, \ell] = \{2, \ell\}$, then $\ell - 2 \leq \sup \Delta(\mathcal{B})$. Set $N = \sup \mathcal{B}$. Since a product of two atoms of $\mathcal{I}_p(\mathcal{O}_f)$ can be written as a product of $n + 1$ atoms, Lemma 4.9 implies that $n + 1 \leq N$. If $n = 1$, then $\mathsf{d}(I \cdot J, (p\mathcal{O}_f) \cdot L) \leq 2 \leq$

$2 + \sup \Delta(\mathcal{B})$ and there is no $\ell \in \mathbb{N}_{\geq 3}$ with $\mathsf{L}(IJ) \cap [2, \ell] = \{2, \ell\}$. Now let $n \geq 2$ and $\ell \in \mathbb{N}_{\geq 3}$ be such that $\mathsf{L}(IJ) \cap [2, \ell] = \{2, \ell\}$.

CASE 1: $n \in \mathcal{B}$. Then $A\overline{A} = (p\mathcal{O}_f)^n$ for some $A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$. Therefore, $\mathsf{c}(A \cdot \overline{A} \cdot L, (p\mathcal{O}_f)^n \cdot L) \leq \mathsf{c}(A \cdot \overline{A}, (p\mathcal{O}_f)^n) \leq 2 + \sup \Delta(\mathcal{B})$ by Lemma 4.10.1. Moreover, $\mathsf{d}(I \cdot J, A \cdot \overline{A} \cdot L) \leq 3 \leq 2 + \sup \Delta(\mathcal{B})$, and thus $\mathsf{c}(I \cdot J, (p\mathcal{O}_f)^n \cdot L) \leq 2 + \sup \Delta(\mathcal{B})$ and $\ell - 2 = 1 \leq \sup \Delta(\mathcal{B})$.

CASE 2: $n \notin \mathcal{B}$. Note that $n \geq 3$. It follows by Theorem 3.6 that $\mathrm{v}_p(f) \geq 2$ and $\sup \Delta(\mathcal{B}) \geq 2$.

CASE 2.1: $p \neq 2$ or $d \not\equiv 1 \mod 8$ or $n \neq 2\mathrm{v}_p(f)$. Since $n \leq N$, it follows from Theorem 3.6 that $n - 1 = \mathcal{N}(A)$ for some $A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, and hence $A\overline{A} = (p\mathcal{O}_f)^{n-1}$. We infer that $\mathsf{c}((p\mathcal{O}_f) \cdot A \cdot \overline{A} \cdot L, (p\mathcal{O}_f)^n \cdot L) \leq \mathsf{c}(A \cdot \overline{A}, (p\mathcal{O}_f)^{n-1}) \leq 2 + \sup \Delta(\mathcal{B})$ by Lemma 4.10.1. Moreover, we have $\mathsf{d}(I \cdot J, A \cdot \overline{A} \cdot (p\mathcal{O}_f) \cdot L) \leq 4 \leq 2 + \sup \Delta(\mathcal{B})$, and thus $\mathsf{c}(I \cdot J, (p\mathcal{O}_f)^n \cdot L) \leq 2 + \sup \Delta(\mathcal{B})$ and $\ell - 2 \leq 2 \leq \sup \Delta(\mathcal{B})$.

CASE 2.2: $p = 2$, $d \equiv 1 \mod 8$ and $n = 2\mathrm{v}_p(f)$. We infer by Theorem 3.6 that $\sup \Delta(\mathcal{B}) = 3$. By Theorem 3.6 there is some $A \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $n - 2 = \mathcal{N}(A)$, and thus $A\overline{A} = (2\mathcal{O}_f)^{n-2}$. This implies that $\mathsf{c}((2\mathcal{O}_f)^2 \cdot A \cdot \overline{A} \cdot L, (2\mathcal{O}_f)^n \cdot L) \leq \mathsf{c}(A \cdot \overline{A}, (2\mathcal{O}_f)^{n-2}) \leq 2 + \sup \Delta(\mathcal{B})$ by Lemma 4.10.1. Observe that $\mathsf{d}(I \cdot J, A \cdot \overline{A} \cdot (2\mathcal{O}_f)^2 \cdot L) \leq 5 = 2 + \sup \Delta(\mathcal{B})$, and hence $\mathsf{c}(I \cdot J, (2\mathcal{O}_f)^n \cdot L) \leq 2 + \sup \Delta(\mathcal{B})$ and $\ell - 2 \leq 3 = \sup \Delta(\mathcal{B})$.

2. By Proposition 3.3.3 we can assume without restriction that $f = 2^{\mathrm{v}_2(f)}$. Let $I, J \in \mathcal{A}(\mathcal{I}_2(\mathcal{O}_f))$. There are some $n \in \mathbb{N}$ and $L \in \mathcal{A}(\mathcal{I}_2(\mathcal{O}_f))$ such that $IJ = 2^n L$. It follows from Lemma 4.9 that $n + 1 \leq \sup \mathcal{B}$. By Proposition 4.1, it is sufficient to show that $\mathsf{c}(I \cdot J, (2\mathcal{O}_f)^n \cdot L) \leq 4$ and if $\ell \in \mathbb{N}_{\geq 3}$ is such that $\mathsf{L}(IJ) \cap [2, \ell] = \{2, \ell\}$, then $\ell - 2 \leq 2$. The assertion is trivially true for $n = 1$. Let $n \geq 2$ and let $\ell \in \mathbb{N}_{\geq 3}$ be such that $\mathsf{L}(IJ) \cap [2, \ell] = \{2, \ell\}$.

CASE 1: $n \in \mathcal{B}$. There is some $A \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $A\overline{A} = (2\mathcal{O}_f)^n$. It follows by Lemma 4.10.2 that $\mathsf{c}(A \cdot \overline{A} \cdot L, (2\mathcal{O}_f)^n \cdot L) \leq \mathsf{c}(A \cdot \overline{A}, (2\mathcal{O}_f)^n) \leq 4$. Furthermore, $\mathsf{d}(I \cdot J, A \cdot \overline{A} \cdot L) \leq 3$, and thus $\mathsf{c}(I \cdot J, (2\mathcal{O}_f)^n \cdot L) \leq 4$ and $\ell - 2 \leq 1$.

CASE 2: $n \notin \mathcal{B}$ and $n \neq 2\mathrm{v}_2(f)$. It follows by Theorem 3.6 that there is some $A \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $A\overline{A} = (2\mathcal{O}_f)^{n-1}$. We infer by Lemma 4.10.2 that $\mathsf{c}((2\mathcal{O}_f) \cdot A \cdot \overline{A} \cdot L, (2\mathcal{O}_f)^n \cdot L) \leq \mathsf{c}(\cdot A \cdot \overline{A}, (2\mathcal{O}_f)^{n-1}) \leq 4$. Furthermore, $\mathsf{d}(I \cdot J, (2\mathcal{O}_f) \cdot A \cdot \overline{A} \cdot L) \leq 4$, and thus $\mathsf{c}(I \cdot J, (2\mathcal{O}_f)^n \cdot L) \leq 4$ and $\ell - 2 \leq 2$.

CASE 3: $n = 2\mathrm{v}_2(f)$. By Theorem 3.6 there is some $D \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $D\overline{D} = (2\mathcal{O}_f)^{n-2}$. Set $A = 16\mathbb{Z} + (4 + \tau)\mathbb{Z}$, $B = 2^{n-2}\mathbb{Z} + (2^{n-4} + \tau)\mathbb{Z}$ and $C = 2^{n-2}\mathbb{Z} + (2^{n-3} + \tau)\mathbb{Z}$. Then $A, B, C \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $ABC = 2^{n-4}A(16\mathbb{Z} + (12 + \tau)\mathbb{Z}) = (2\mathcal{O}_f)^n$. This implies that $\mathsf{c}((2\mathcal{O}_f)^2 \cdot D \cdot \overline{D} \cdot L, (2\mathcal{O}_f)^n \cdot L) \leq \mathsf{c}(D \cdot \overline{D}, (2\mathcal{O}_f)^{n-2}) \leq 4$ by Lemma 4.10.2. Moreover, $\mathsf{d}(A \cdot B \cdot C \cdot L, (2\mathcal{O}f)^2 \cdot D \cdot \overline{D} \cdot L) \leq 4$ and $\mathsf{d}(I \cdot J, A \cdot B \cdot C \cdot L) \leq 4$. Consequently, $\mathsf{c}(I \cdot J, (2\mathcal{O}_f)^n \cdot L) \leq 4$ and $\ell - 2 \leq 2$. $\square$

**Proposition 4.12.** *Let* $\mathrm{v}_2(f) \in \{2, 3\}$ *and* $d \equiv 1 \mod 8$. *Then* $3 \in \Delta(\mathcal{I}_2^*(\mathcal{O}_f))$ *and* $5 \in \mathrm{Ca}(\mathcal{I}_2^*(\mathcal{O}_f))$.

*Proof.* We distinguish two cases.

CASE 1: $v_2(f) = 2$. By Theorem 3.6 there is some $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = 32$. Set $J = \overline{I}$. Then $IJ = 32\mathcal{O}_f$, and hence $\{2, 5\} \subset \mathsf{L}(IJ) \subset [2, 5]$. Again by Theorem 3.6 we have $\mathcal{N}(L) \in \{4\} \cup \{2^n \mid n \in \mathbb{N}_{\geq 5}\}$ for all $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. Note that if $A, B, C, D \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$, then $\mathcal{N}(ABCD) \in \{256\} \cup \mathbb{N}_{\geq 2048}$. Since $\mathcal{N}(IJ) = 1024$, we have $4 \notin \mathsf{L}(IJ)$. Assume that $3 \in \mathsf{L}(IJ)$. Then there are some $A, B, C \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $IJ = ABC$ and $\mathcal{N}(A) \leq \mathcal{N}(B) \leq \mathcal{N}(C)$. Therefore, $\mathcal{N}(A) = \mathcal{N}(B) = 4$ and $\mathcal{N}(C) = 64$. We infer by Lemma 4.2.2 that $ABC = 4L$ for some $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$, and hence $L = 8\mathcal{O}_f$, a contradiction. We have $\mathsf{L}(IJ) = \{2, 5\}$, and thus $3 \in \Delta(\mathcal{I}_2^*(\mathcal{O}_f))$ and $5 = \mathsf{c}(IJ) \in \mathrm{Ca}(\mathcal{I}_2^*(\mathcal{O}_f))$.

CASE 2: $v_2(f) = 3$. By Proposition 3.3.3 we can assume without restriction that $f = 8$. By Theorem 3.6 there are some $I, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = 128$ and $\mathcal{N}(J) = 16$. We have $I\overline{I} = 128\mathcal{O}_f$ and $J\overline{J} = 16\mathcal{O}_f$, and hence $I\overline{I} = 8J\overline{J}$. This implies that $\{2, 5\} \subset \mathsf{L}(I\overline{I})$. It follows from Theorem 3.6 that $\mathcal{N}(L) \in \{4, 16\} \cup \{2^n \mid n \in \mathbb{N}_{\geq 7}\}$ for all $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$.

First assume that $3 \in \mathsf{L}(I\overline{I})$. Then there exist $A, B, C \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $I\overline{I} = ABC$, and $\mathcal{N}(A) \leq \mathcal{N}(B) \leq \mathcal{N}(C)$. Therefore, $(\mathcal{N}(A), \mathcal{N}(B), \mathcal{N}(C)) \in \{(4, 16, 256), (4, 4, 1024)\}$. If $(\mathcal{N}(A), \mathcal{N}(B), \mathcal{N}(C)) = (4, 16, 256)$, then it follows by Lemma 4.2.2 that $AB = 2D$ for some $D \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ with $\mathcal{N}(D) = 16$. We infer that $DC = 64\mathcal{O}_f$, and hence $C = 4\overline{D}$, a contradiction. Now let $(\mathcal{N}(A), \mathcal{N}(B), \mathcal{N}(C)) = (4, 4, 1024)$. Then $ABC = 4D$ for some $D \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ by Lemma 4.2.2, and thus $D = 32\mathcal{O}_f$, a contradiction. Consequently, $3 \notin \mathsf{L}(I\overline{I})$.

Next assume that $4 \in \mathsf{L}(I\overline{I})$. Then there exist $A, B, C, D \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $I\overline{I} = ABCD$, and $\mathcal{N}(A) \leq \mathcal{N}(B) \leq \mathcal{N}(C) \leq \mathcal{N}(D)$.

Then $(\mathcal{N}(A), \mathcal{N}(B), \mathcal{N}(C), \mathcal{N}(D)) \in \{(4, 4, 4, 256), (4, 16, 16, 16)\}$.

If $(\mathcal{N}(A), \mathcal{N}(B), \mathcal{N}(C), \mathcal{N}(D)) = (4, 4, 4, 256)$, then $ABCD = 8E$ for $E \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ by Lemma 4.2.2, and hence $E = 16\mathcal{O}_f$, a contradiction. Now let $(\mathcal{N}(A), \mathcal{N}(B), \mathcal{N}(C), \mathcal{N}(D)) = (4, 16, 16, 16)$. By Lemma 4.2.2 there is some $E \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ with $\mathcal{N}(E) = 16$ such that $AB = 2E$. Therefore, $ECD = 64\mathcal{O}_f$, and hence $CD = 4\overline{E}$. There are some $(0, 4, r), (0, 4, s) \in \mathcal{M}_{f,2}$ such that $C = 16\mathbb{Z} + (r + \tau)\mathbb{Z}$ and $D = 16\mathbb{Z} + (s + \tau)\mathbb{Z}$. We have $v_2(r^2 - 16d) = v_2(s^2 - 16d) = 4$. Since $d \equiv 1 \mod 8$, this implies that $v_2(r), v_2(s) \geq 3$. Therefore, $\min\{4, v_2(r + s + \varepsilon)\} \in \{3, 4\}$, and hence $CD = 8F$ for some $F \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. We infer that $\overline{E} = 2F$, a contradiction. Consequently, $4 \notin \mathsf{L}(I\overline{I})$.

Therefore, 2 and 5 are adjacent lengths of $I\overline{I}$, and hence $3 \in \Delta(\mathcal{I}_2^*(\mathcal{O}_f))$. Note that $\mathsf{c}(\mathcal{I}_2^*(\mathcal{O}_f)) \leq 5$ by Proposition 4.11.1 and Theorem 3.6. Moreover, since $\mathcal{I}_2^*(\mathcal{O}_f)$ is a cancellative monoid, we have $5 \leq 2 + \sup \Delta(\mathsf{L}(I\overline{I})) \leq \mathsf{c}(I\overline{I}) \leq 5$, and thus $5 = \mathsf{c}(I\overline{I}) \in \mathrm{Ca}(\mathcal{I}_2^*(\mathcal{O}_f))$. ☐

**Lemma 4.13.** *Let $H \in \{\mathcal{I}(\mathcal{O}_f), \mathcal{I}^*(\mathcal{O}_f)\}$. For every prime divisor $p$ of $f$, we set $H_p = \mathcal{I}_p(\mathcal{O}_f)$ if $H = \mathcal{I}(\mathcal{O}_f)$ and $H_p = \mathcal{I}_p^*(\mathcal{O}_f)$ if $H = \mathcal{I}^*(\mathcal{O}_f)$.*

1. *$H$ is half-factorial if and only if $H_p$ is half-factorial for every $p \in \mathbb{P}$ with $p \mid f$.*
2. *If $H$ is not half-factorial, then* $\sup \Delta(H) = \sup\{\sup \Delta(H_p) \mid p \in \mathbb{P}$ *with* $p \mid f\}$.
3. $\mathsf{c}(H) = \sup\{\mathsf{c}(H_p) \mid p \in \mathbb{P}$ *with* $p \mid f\}$.

*Proof.* By Eqs. 2.3 and 2.4, we have

$$\mathcal{I}^*(\mathcal{O}_f) \cong \coprod_{P \in \mathfrak{X}(\mathcal{O}_f)} \mathcal{I}_P^*(\mathcal{O}_f) \quad \text{and} \quad \mathcal{I}(\mathcal{O}_f) \cong \coprod_{P \in \mathfrak{X}(\mathcal{O}_f)} \mathcal{I}_P(\mathcal{O}_f).$$

Thus the assertions are easy consequences (see [16, Propositions 1.4.5.3 and 1.6.8.1]). □

*Proof (Proof of Theorem 1.1).* 1. This is an immediate consequence of Proposition 4.6 and Lemma 4.13.

2. First, suppose that $f$ is squarefree. By 1., we have $f$ is not a product of inert primes. It follows from Lemma 4.13, Proposition 4.11.1, and Theorem 3.6 that $\mathsf{c}(\mathcal{I}^*(\mathcal{O})) \le \mathsf{c}(\mathcal{I}(\mathcal{O})) \le 3$ and $\sup \Delta(\mathcal{I}^*(\mathcal{O})) \le \sup \Delta(\mathcal{I}(\mathcal{O})) \le 1$. By Lemma 4.2 and Proposition 4.8.1, it follows that $1 \in \Delta(\mathcal{I}^*(\mathcal{O}))$, $1 \in \mathrm{Ca}(\mathcal{I}(\mathcal{O}))$ and $[2, 3] \subset \mathrm{Ca}(\mathcal{I}^*(\mathcal{O}))$, and thus $\mathrm{Ca}(\mathcal{I}(\mathcal{O})) = [1, 3]$, $\mathrm{Ca}(\mathcal{I}^*(\mathcal{O})) = [2, 3]$, and $\Delta(\mathcal{I}(\mathcal{O})) = \Delta(\mathcal{I}^*(\mathcal{O})) = \{1\}$.

Now we suppose that $f$ is not squarefree and we distinguish two cases.

CASE 1: $\mathsf{v}_2(f) \notin \{2, 3\}$ or $d_K \not\equiv 1 \mod 8$. By Lemma 4.13, Proposition 4.11, and Theorem 3.6 it follows that $\mathsf{c}(\mathcal{I}^*(\mathcal{O})) \le \mathsf{c}(\mathcal{I}(\mathcal{O})) \le 4$ and $\sup \Delta(\mathcal{I}^*(\mathcal{O})) \le \sup \Delta(\mathcal{I}(\mathcal{O})) \le 2$. We infer by Lemma 4.2 and Propositions 4.4 and 4.8 that $[1, 2] \subset \Delta(\mathcal{I}^*(\mathcal{O}))$, $1 \in \mathrm{Ca}(\mathcal{I}(\mathcal{O}))$, and $[2, 4] \subset \mathrm{Ca}(\mathcal{I}^*(\mathcal{O}))$, and hence $\mathrm{Ca}(\mathcal{I}(\mathcal{O})) = [1, 4]$, $\mathrm{Ca}(\mathcal{I}^*(\mathcal{O})) = [2, 4]$, and $\Delta(\mathcal{I}(\mathcal{O})) = \Delta(\mathcal{I}^*(\mathcal{O})) = [1, 2]$.

CASE 2: $\mathsf{v}_2(f) \in \{2, 3\}$ and $d_K \equiv 1 \mod 8$. We infer by Lemma 4.13, Proposition 4.11.1, and Theorem 3.6 that $\mathsf{c}(\mathcal{I}^*(\mathcal{O})) \le \mathsf{c}(\mathcal{I}(\mathcal{O})) \le 5$ and $\sup \Delta(\mathcal{I}^*(\mathcal{O})) \le \sup \Delta(\mathcal{I}(\mathcal{O})) \le 3$. Lemma 4.2 and Propositions 4.4, 4.8 and 4.12 imply that $[1, 3] \subset \Delta(\mathcal{I}^*(\mathcal{O}))$, $1 \in \mathrm{Ca}(\mathcal{I}(\mathcal{O}))$ and $[2, 5] \subset \mathrm{Ca}(\mathcal{I}^*(\mathcal{O}))$. Consequently, $\mathrm{Ca}(\mathcal{I}(\mathcal{O})) = [1, 5]$, $\mathrm{Ca}(\mathcal{I}^*(\mathcal{O})) = [2, 5]$, and $\Delta(\mathcal{I}(\mathcal{O})) = \Delta(\mathcal{I}^*(\mathcal{O})) = [1, 3]$. □

Based on the results of this section we derive a result on the set of distances of orders. Let $\mathcal{O}$ be a non-half-factorial order in a number field. Then the set of distances $\Delta(\mathcal{O})$ is finite. If $\mathcal{O}$ is a principal order, then it is easy to show that $\min \Delta(\mathcal{O}) = 1$ (indeed much stronger results are known, namely, that sets of lengths of almost all elements—in a sense of density—are intervals, see [16, Theorem 9.4.11]). The same is true if $|\mathrm{Pic}(\mathcal{O})| \ge 3$ or if $\mathcal{O}$ is seminormal [24, Theorem 1.1]. However, it was unknown so far whether there exists an order $\mathcal{O}$ with $\min \Delta(\mathcal{O}) > 1$. In the next result of this section we characterize all non-half-factorial orders in quadratic number fields with $\min \Delta(\mathcal{O}) > 1$ which allows us to give the first explicit examples of orders $\mathcal{O}$ with $\min \Delta(\mathcal{O}) > 1$. A characterization of half-factorial orders in quadratic number fields is given in [16, Theorem 3.7.15].

Let $\mathcal{O}$ be an order in a quadratic number field $K$ with conductor $f \in \mathbb{N}_{\ge 2}$. Then the class numbers $|\mathrm{Pic}(\mathcal{O}_K)|$ and $|\mathrm{Pic}(\mathcal{O})|$ are linked by the formula [25, Corollary 5.9.8]

$$|\mathrm{Pic}(\mathcal{O})| = |\mathrm{Pic}(\mathcal{O}_K)| \frac{f}{(\mathcal{O}_K^\times : \mathcal{O}^\times)} \prod_{p \in \mathbb{P}, p \mid f} \left( 1 - \left( \frac{d_K}{p} \right) p^{-1} \right), \tag{4.1}$$

and $|\mathrm{Pic}(\mathcal{O})|$ is a multiple of $|\mathrm{Pic}(\mathcal{O}_K)|$.

Since the number of imaginary quadratic number fields with class number at most two is finite (an explicit list of these fields can be found, for example, in [31]), (4.1) shows that the number of orders in imaginary quadratic number fields with $|\mathrm{Pic}(\mathcal{O})| = 2$ is finite. The complete list of non-maximal orders in imaginary quadratic number fields with $|\mathrm{Pic}(\mathcal{O})| = 2$ is given in [27, page 16]. We refer to [25] for more information on class groups and class numbers and end with explicit examples of non-half-factorial orders $\mathcal{O}$ satisfying $\min \Delta(\mathcal{O}) > 1$.

**Theorem 4.14.** *Let $\mathcal{O}$ be a non-half-factorial order in a quadratic number field $K$ with conductor $f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$. Then the following statements are equivalent:*

(a) $\min \Delta(\mathcal{O}) > 1$.
(b) $|\mathrm{Pic}(\mathcal{O})| = 2$*, $f$ is a nonempty squarefree product of ramified primes times a (possibly empty) squarefree product of inert primes, and for every prime divisor $p$ of $f$ and every $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$, $I$ is principal if and only if $\mathcal{N}(I) = p^2$.*

*If these equivalent conditions are satisfied, then $K$ is a real quadratic number field and* $\min \Delta(\mathcal{O}) = 2$.

*Proof.* CLAIM: If $|\mathrm{Pic}(\mathcal{O})| = 2$, $p$ is a ramified prime with $\mathrm{v}_p(f) = 1$, and every $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(I) = p^3$ is not principal, then every $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(L) = p^2$ is principal.

Let $|\mathrm{Pic}(\mathcal{O})| = 2$, let $p$ be a ramified prime with $\mathrm{v}_p(f) = 1$, and suppose that every $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(I) = p^3$ is not principal. By Theorem 3.6 we have $\{\mathcal{N}(J) \mid J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))\} = \{p^2, p^3\}$. There is some $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ such that $\mathcal{N}(I) = p^3$. If $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(J) = p^3$, then $IJ = p^2 L$ for some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(L) = p^2$ (since there are no atoms with norm bigger than $p^3$). It follows by Theorem 3.6 that $|\{J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(J) = p^3\}| = |\{L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(L) = p^2\}| = p$ (note that $\mathcal{N}(p\mathcal{O}) = p^2$). Let $g : \{J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(J) = p^3\} \to \{L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(L) = p^2\}$ be defined by $g(J) = L$ where $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ is such that $\mathcal{N}(L) = p^2$ and $IJ = p^2 L$. Then $g$ is a well-defined bijection. Now let $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(L) = p^2$. There is some $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ such that $\mathcal{N}(J) = p^3$ and $IJ = p^2 L$. Since $|\mathrm{Pic}(\mathcal{O})| = 2$ and $I$ and $J$ are not principal, we have $IJ$ is principal, and hence $L$ is principal. This proves the claim.

(a) $\Rightarrow$ (b) Observe that if $p$ is an inert prime such that $\mathrm{v}_p(f) = 1$, then $\{\mathcal{N}(J) \mid J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))\} = \{p^2\}$ by Theorem 3.6. Also note that if $p$ is a ramified prime such that $\mathrm{v}_p(f) = 1$, then $\{\mathcal{N}(J) \mid J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))\} = \{p^2, p^3\}$ by Theorem 3.6. The assertion now follows by the claim and Proposition 4.8.2.

(b) $\Rightarrow$ (a) Assume to the contrary that $\min \Delta(\mathcal{O}) = 1$. Let $\mathcal{H}$ be the monoid of nonzero principal ideals of $\mathcal{O}$. There is some minimal $k \in \mathbb{N}$ such that $\prod_{i=1}^{k} U_i = \prod_{j=1}^{k+1} U_j'$ with $U_i \in \mathcal{A}(\mathcal{H})$ for each $i \in [1, k]$ and $U_j' \in \mathcal{A}(\mathcal{H})$ for each $j \in [1, k+1]$.

Set $\mathcal{Q}_1 = \{P \in \mathfrak{X}(\mathcal{O}) \mid P \text{ is principal}\}$, $\mathcal{Q}_2 = \{P \in \mathfrak{X}(\mathcal{O}) \mid P \text{ is invertible and not principal}\}$, $\mathcal{L} = \{p \in \mathbb{P} \mid p \mid f, p \text{ is ramified}\}$, and $\mathcal{K} = \{\{p, q\} \mid p, q \in \mathcal{L}, p \neq q\}$.

For every prime divisor $p$ of $f$ set $\mathcal{A}_p = \{V \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(V) = p^2\}$, $a_p = |\{i \in [1,k] \mid U_i \in \mathcal{A}_p\}|$ and $a'_p = |\{j \in [1,k+1] \mid U'_j \in \mathcal{A}_p\}|$. For $p \in \mathcal{L}$ set $\mathcal{D}_p = \{V \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(V) = p^3\}$, $\mathcal{B}_p = \{PV \mid P \in \mathcal{Q}_2$ and $V \in \mathcal{D}_p\}$, $b_p = |\{i \in [1,k] \mid U_i \in \mathcal{B}_p\}|$ and $b'_p = |\{j \in [1,k+1] \mid U'_j \in \mathcal{B}_p\}|$. Set $\mathcal{C} = \{PQ \mid P, Q \in \mathcal{Q}_2\}$, $c = |\{i \in [1,k] \mid U_i \in \mathcal{C}\}|$ and $c' = |\{j \in [1,k+1] \mid U'_j \in \mathcal{C}\}|$. If $z \in \mathcal{K}$ is such that $z = \{p,q\}$ with $p,q \in \mathcal{L}$ and $p \neq q$, then set $\mathcal{E}_z = \{VW \mid V \in \mathcal{D}_p, W \in \mathcal{D}_q\}$, $e_z = |\{i \in [1,k] \mid U_i \in \mathcal{E}_z\}|$ and $e'_z = |\{j \in [1,k+1] \mid U'_j \in \mathcal{E}_z\}|$.

Since $|\mathrm{Pic}(\mathcal{O})| = 2$, we have $\mathcal{A}(\mathcal{H}) \subset (\mathcal{A}(\mathcal{I}^*(\mathcal{O})) \cap \mathcal{H}) \cup \{VW \mid V, W \in \mathcal{A}(\mathcal{I}^*(\mathcal{O})), V$ and $W$ are not principal$\}$. As shown in the proof of the claim, $VW \notin \mathcal{A}(\mathcal{H})$ for all $p \in \mathcal{L}$ and $V, W \in \mathcal{D}_p$. We infer that $\mathcal{A}(\mathcal{H}) = \mathcal{Q}_1 \cup \bigcup_{p \in \mathbb{P}, p \mid f} \mathcal{A}_p \cup \bigcup_{p \in \mathcal{L}} \mathcal{B}_p \cup \mathcal{C} \cup \bigcup_{z \in \mathcal{K}} \mathcal{E}_z$.

Since $k$ is minimal, we have $U_i, U'_j \notin \mathcal{Q}_1$ for all $i \in [1,k]$ and $j \in [1,k+1]$. Again since $k$ is minimal and $\mathcal{I}_p^*(\mathcal{O})$ is half-factorial for all inert prime divisors $p$ of $f$ by Proposition 4.6, we have $a_p = a'_p = 0$ for all inert prime divisors $p$ of $f$. Therefore,

$$k = \sum_{p \in \mathcal{L}} (a_p + b_p) + c + \sum_{z \in \mathcal{K}} e_z \text{ and } k+1 = \sum_{p \in \mathcal{L}} (a'_p + b'_p) + c' + \sum_{z \in \mathcal{K}} e'_z.$$

If $i \in [1,k]$, then $\sum_{P \in \mathcal{Q}_2} \mathrm{v}_P(U_i) = \begin{cases} 2 & \text{if } U_i \in \mathcal{C} \\ 1 & \text{if } U_i \in \bigcup_{p \in \mathcal{L}} \mathcal{B}_p \\ 0 & \text{else} \end{cases}$. This implies that $\sum_{P \in \mathcal{Q}_2} \mathrm{v}_P(\prod_{i=1}^k U_i) = \sum_{i=1}^k \sum_{P \in \mathcal{Q}_2} \mathrm{v}_P(U_i) = \sum_{p \in \mathcal{L}} b_p + 2c$. It follows by analogy that $\sum_{P \in \mathcal{Q}_2} \mathrm{v}_P(\prod_{j=1}^{k+1} U'_j) = \sum_{p \in \mathcal{L}} b'_p + 2c'$. Therefore, $\sum_{p \in \mathcal{L}} b_p + 2c = \sum_{p \in \mathcal{L}} b'_p + 2c'$. Let $r \in \mathcal{L}$.

If $i \in [1,k]$, then $\mathrm{v}_r(\mathcal{N}((U_i)_{P_{f,r}} \cap \mathcal{O})) = \begin{cases} 3 & \text{if } U_i \in \mathcal{B}_r \cup \bigcup_{q \in \mathcal{L} \setminus \{r\}} \mathcal{E}_{\{r,q\}} \\ 2 & \text{if } U_i \in \mathcal{A}_r \\ 0 & \text{else} \end{cases}$.

Consequently,

$$\mathrm{v}_r(\mathcal{N}((\prod_{i=1}^k U_i)_{P_{f,r}} \cap \mathcal{O})) = \sum_{i=1}^k \mathrm{v}_r(\mathcal{N}((U_i)_{P_{f,r}} \cap \mathcal{O})) = 2a_r + 3b_r + 3 \sum_{q \in \mathcal{L} \setminus \{r\}} e_{\{r,q\}}.$$

By analogy we have $\mathrm{v}_r(\mathcal{N}((\prod_{j=1}^{k+1} U'_j)_{P_{f,r}} \cap \mathcal{O})) = 2a'_r + 3b'_r + 3 \sum_{q \in \mathcal{L} \setminus \{r\}} e'_{\{r,q\}}$.

This implies that $2a_r + 3b_r + 3 \sum_{q \in \mathcal{L} \setminus \{r\}} e_{\{r,q\}} = 2a'_r + 3b'_r + 3 \sum_{q \in \mathcal{L} \setminus \{r\}} e'_{\{r,q\}}$. We infer that

$$\sum_{p\in\mathcal{L}}(a'_p - a_p + b'_p - b_p) + c' - c + \sum_{z\in\mathcal{K}}(e'_z - e_z) = 1,\ \sum_{p\in\mathcal{L}}(b'_p - b_p) = 2(c - c')$$

and $2\sum_{p\in\mathcal{L}}(a'_p - a_p) + 3\sum_{p\in\mathcal{L}}(b'_p - b_p) + 3\sum_{p\in\mathcal{L}}\sum_{q\in\mathcal{L}\setminus\{p\}}(e'_{\{p,q\}} - e_{\{p,q\}}) = 0.$

Note that $\sum_{p\in\mathcal{L}}\sum_{q\in\mathcal{L}\setminus\{p\}}(e'_{\{p,q\}} - e_{\{p,q\}}) = 2\sum_{z\in\mathcal{K}}(e'_z - e_z)$, and hence $\sum_{p\in\mathcal{L}}(a'_p - a_p) = 3(c' - c) - 3\sum_{z\in\mathcal{K}}(e'_z - e_z)$. Consequently,

$$\begin{aligned}1 &= \sum_{p\in\mathcal{L}}(a'_p - a_p + b'_p - b_p) + c' - c + \sum_{z\in\mathcal{K}}(e'_z - e_z)\\ &= 3(c' - c) - 3\sum_{z\in\mathcal{K}}(e'_z - e_z) + 2(c - c') + c' - c + \sum_{z\in\mathcal{K}}(e'_z - e_z)\\ &= 2(c' - c - \sum_{z\in\mathcal{K}}(e'_z - e_z)),\end{aligned}$$

a contradiction.

Now let the equivalent conditions be satisfied. Assume to the contrary that $K$ is an imaginary quadratic number field. Since $\mathcal{O}$ is a non-maximal order with $|\mathrm{Pic}(\mathcal{O})| = 2$, it follows from [27, page 16] that $(f, d_K) \in \{(2, -8), (2, -15)\} \cup \{(3, -4), (3, -8), (3, -11), (4, -3), (4, -4), (4, -7), (5, -3), (5, -4), (7, -3)\}$.

Since $f$ is squarefree and divisible by a ramified prime, we infer that $f = 2$ and $d_K = -8$. Therefore, $\mathcal{O} = \mathbb{Z} + 2\sqrt{-2}\mathbb{Z}$. Set $I = 8\mathbb{Z} + 2\sqrt{-2}\mathbb{Z}$. Observe that $I \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}))$ and $\mathcal{N}(I) = 8$. Moreover, $I = 2\sqrt{-2}\mathcal{O}$ is principal, a contradiction. Consequently, $K$ is a real quadratic number field.

It remains to show that $\min \Delta(\mathcal{O}) = 2$. There is some ramified prime $p$ which divides $f$ and there is some $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(J) = p^3$. As shown in the proof of the claim, $J^2 = p^2 L$ for some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$. By [16, Corollary 2.11.16], there is some invertible prime ideal $P$ of $\mathcal{O}$ that is not principal. Observe that $J$ is not principal. We have $PJ$, $P^2$ and $L$ are principal, and hence there are some $u, v, w \in \mathcal{A}(\mathcal{O})$ such that $PJ = u\mathcal{O}$, $P^2 = v\mathcal{O}$, $L = w\mathcal{O}$, and $u^2 = p^2 vw$. Therefore, $\{2, 4\} \subset \mathsf{L}(u^2)$, and since $\min \Delta(\mathcal{O}) > 1$, we infer that $\min \Delta(\mathcal{O}) = 2$. □

**Proposition 4.15.** *Let $\mathcal{O}$ be an order in the quadratic number field $K$ with conductor $f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$ such that* $\min \Delta(\mathcal{O}) > 1$, *let $g$ be the product of all inert prime divisors of $f$ and let $\mathcal{O}'$ be the order in $K$ with conductor $g\mathcal{O}_K$. Then $\mathcal{O}'$ is half-factorial and, in particular, $g \in \{1\} \cup \mathbb{P} \cup \{2p \mid p \in \mathbb{P} \setminus \{2\}\}$.*

*Proof.* Set $\mathcal{Q}_1 = \{P \in \mathfrak{X}(\mathcal{O}') \mid P \text{ is principal}\}$ and $\mathcal{Q}_2 = \{P \in \mathfrak{X}(\mathcal{O}') \mid P \text{ is invertible and not principal}\}$. Observe that $\mathcal{N}(I) = |\mathcal{O}/I| = |\mathcal{O}'/I\mathcal{O}'| = \mathcal{N}(I\mathcal{O}')$ for all $I \in \mathcal{I}^*(\mathcal{O})$. Note that for all inert prime divisors $p$ of $f$ and all $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ and $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}'))$, we have $\mathcal{N}(I) = \mathcal{N}(J) = p^2$. Moreover, for all ramified prime divisors $p$ of $f$, we have $\{\mathcal{N}(I) \mid I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))\} = \{p^2, p^3\}$. In this proof we will use Theorem 4.14 without further citation.

CLAIM 1: For all prime divisors $p$ of $g$ and all $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}'))$, it follows that $I$ is principal. Let $p$ be a prime divisor of $g$ and let $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}'))$. Set $P = P_{f,p}$ and $P' = P_{g,p}$. It follows by Proposition 3.3 that $\mathcal{O}_P = \mathcal{O}'_{P'}$ and that $\delta : \mathcal{I}_p^*(\mathcal{O}) \to \mathcal{I}_p^*(\mathcal{O}')$ defined by $\delta(J) = J_P \cap \mathcal{O}'$ for all $J \in \mathcal{I}_p^*(\mathcal{O})$ is a monoid isomorphism. In particular, we have $\mathcal{A}(\mathcal{I}_p^*(\mathcal{O}')) = \{J_P \cap \mathcal{O}' \mid J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))\}$. Therefore, there is some $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ such that $J_P \cap \mathcal{O}' = I$. Note that $\mathcal{N}(I) = p^2 = \mathcal{N}(J) = \mathcal{N}(J\mathcal{O}')$. Since $J\mathcal{O}' \subset J\mathcal{O}'_{P'} \cap \mathcal{O}' = J\mathcal{O}_P \cap \mathcal{O}' = I$, we infer that $I = J\mathcal{O}'$. Since $J$ is a principal ideal of $\mathcal{O}$, it follows that $I$ is principal. This proves Claim 1.

CLAIM 2: If $P \in \mathcal{Q}_2$, $p$ is a ramified prime divisor of $f$ such that $P \cap \mathbb{Z} = p\mathbb{Z}$ and $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(I) = p^3$, then $P^2$ is principal and $I\mathcal{O}' = P^3$. Let $P \in \mathcal{Q}_2$, $p$ a ramified prime divisor of $f$ such that $P \cap \mathbb{Z} = p\mathbb{Z}$ and $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(I) = p^3$. Since $p$ is ramified, there is some $A \in \mathfrak{X}(\mathcal{O}_K)$ such that $p\mathcal{O}_K = A^2$. Observe that $\mathcal{N}(A^2) = p^2$, and thus $\mathcal{N}(A) = p$. We have $A \cap \mathcal{O}' = P$, $P\mathcal{O}_K = A$ and $\mathcal{N}(P) = \mathcal{N}(A) = p$. Note that since $P$ is invertible, it follows that every $P$-primary ideal of $\mathcal{O}'$ is a power of $P$. Therefore, $p\mathcal{O}' = P^k$ for some $k \in \mathbb{N}$, and hence $p^k = \mathcal{N}(P^k) = \mathcal{N}(p\mathcal{O}') = p^2$. Consequently, $k = 2$ and $P^2$ is principal. Clearly, $I\mathcal{O}'$ is a $P$-primary ideal of $\mathcal{O}'$, and thus $I\mathcal{O}' = P^m$ for some $m \in \mathbb{N}$. We infer that $p^m = \mathcal{N}(P^m) = \mathcal{N}(I\mathcal{O}') = \mathcal{N}(I) = p^3$, and thus $m = 3$ and $I\mathcal{O}' = P^3$. This proves Claim 2.

CLAIM 3: $PQ$ is principal for all $P, Q \in \mathcal{Q}_2$. Let $P, Q \in \mathcal{Q}_2$.

CASE 1: $P \cap \mathcal{O}$ and $Q \cap \mathcal{O}$ are invertible. Note that $P = (P \cap \mathcal{O})\mathcal{O}'$, $Q = (Q \cap \mathcal{O})\mathcal{O}'$ and $P \cap \mathcal{O}$ and $Q \cap \mathcal{O}$ are not principal. Since $|\text{Pic}(\mathcal{O})| = 2$, we have $(P \cap \mathcal{O})(Q \cap \mathcal{O})$ is a principal ideal of $\mathcal{O}$, and thus $PQ = (P \cap \mathcal{O})(Q \cap \mathcal{O})\mathcal{O}'$ is principal.

CASE 2: ($P \cap \mathcal{O}$ is invertible and $Q \cap \mathcal{O}$ is not invertible) or ($P \cap \mathcal{O}$ is not invertible and $Q \cap \mathcal{O}$ is invertible). Without restriction let $P \cap \mathcal{O}$ be invertible and let $Q \cap \mathcal{O}$ be not invertible. Observe that $P = (P \cap \mathcal{O})\mathcal{O}'$. Moreover, there is some ramified prime $q$ that divides $f$ such that $Q \cap \mathbb{Z} = q\mathbb{Z}$ and there is some $J \in \mathcal{A}(\mathcal{I}_q^*(\mathcal{O}))$ with $\mathcal{N}(J) = q^3$. Observe that $P \cap \mathcal{O}$ and $J$ are not principal. Since $|\text{Pic}(\mathcal{O})| = 2$, it follows that $(P \cap \mathcal{O})J$ is a principal ideal of $\mathcal{O}$. Note that $PQ^3 = (P \cap \mathcal{O})J\mathcal{O}'$ by Claim 2, and thus $PQ^3$ is principal. Since $Q^2$ is principal by Claim 2, we infer that $PQ$ is principal.

CASE 3: $P \cap \mathcal{O}$ and $Q \cap \mathcal{O}$ are not invertible. There are ramified primes $p$ and $q$ that divide $f$ such that $P \cap \mathbb{Z} = p\mathbb{Z}$ and $Q \cap \mathbb{Z} = q\mathbb{Z}$. There are some $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ and $J \in \mathcal{A}(\mathcal{I}_q^*(\mathcal{O}))$ with $\mathcal{N}(I) = p^3$ and $\mathcal{N}(J) = q^3$. Since $|\text{Pic}(\mathcal{O})| = 2$ and $I$ and $J$ are not principal, we have $IJ$ is a principal ideal of $\mathcal{O}$. It follows that $P^3Q^3 = IJ\mathcal{O}'$ by Claim 2, and hence $P^3Q^3$ is principal. Since $P^2$ and $Q^2$ are principal by Claim 2, we have $PQ$ is principal. This proves Claim 3.

Finally, we show that $\mathcal{O}'$ is half-factorial. Set $\mathcal{C} = \{PQ \mid P, Q \in \mathcal{Q}_2\}$ and let $\mathcal{H}$ denote the monoid of nonzero principal ideals of $\mathcal{O}'$. It is an immediate consequence of Claim 1 and Claim 3 that $\mathcal{A}(\mathcal{H}) = \mathcal{Q}_1 \cup \mathcal{C} \cup \bigcup_{p \in \mathbb{P}, p|g} \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}'))$.

Let $k, \ell \in \mathbb{N}$ and $I_i, I'_j \in \mathcal{A}(\mathcal{H})$ for each $i \in [1, k]$ and $j \in [1, \ell]$ be such that $\prod_{i=1}^k I_i = \prod_{j=1}^\ell I'_j$. It remains to show that $k = \ell$. Set $b = |\{i \in [1, k] \mid I_i \in \mathcal{Q}_1\}|$,

$b' = |\{j \in [1, \ell] \mid I'_j \in \mathcal{Q}_1\}|$, $c = |\{i \in [1, k] \mid I_i \in \mathcal{C}\}|$, $c' = |\{j \in [1, \ell] \mid I'_j \in \mathcal{C}\}|$ and for each prime divisor $p$ of $g$ set $a_p = |\{i \in [1, k] \mid I_i \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}'))\}|$ and $a'_p = |\{j \in [1, \ell] \mid I'_j \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}'))\}|$. If $p$ is a prime divisor of $g$, then $\mathcal{I}_p^*(\mathcal{O}')$ is half-factorial by Proposition 4.6, and hence $a_p = a'_p$ by Claim 1. We have $b = \sum_{i=1}^{k} \sum_{P \in \mathcal{Q}_1} \mathrm{v}_P(I_i) = \sum_{P \in \mathcal{Q}_1} \mathrm{v}_P(\prod_{i=1}^{k} I_i) = \sum_{P \in \mathcal{Q}_1} \mathrm{v}_P(\prod_{j=1}^{\ell} I'_j) = \sum_{j=1}^{\ell} \sum_{P \in \mathcal{Q}_1} \mathrm{v}_P(I'_j) = b'$.

Moreover, $2c = \sum_{P \in \mathcal{Q}_2} \mathrm{v}_P(\prod_{i=1}^{k} I_i) = \sum_{P \in \mathcal{Q}_2} \mathrm{v}_P(\prod_{j=1}^{\ell} I'_j) = 2c'$. Therefore, $k = b + c + \sum_{p \in \mathbb{P}, p \mid g} a_p = b' + c' + \sum_{p \in \mathbb{P}, p \mid g} a'_p = \ell$.

The remaining assertion follows from [16, Theorem 3.7.15]. □

*Remark 4.16.* Let $\mathcal{O}$ be an order in the quadratic number field $K$ with conductor $f\mathcal{O}_K$ for some $f \in \mathbb{N}$ such that $|\mathrm{Pic}(\mathcal{O})| = 2$ and let $p$ be an odd ramified prime such that $\mathrm{v}_p(f) = 1$ and $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ such that $\mathcal{N}(I) = p^3$ and $I$ not principal. Then every $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(J) = p^3$ is not principal.

*Proof.* Set $\mathcal{L} = \{J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(J) = p^3\}$ and $\mathcal{K} = \{L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(L) = p^2\}$. It follows by the claim in the proof of Theorem 4.14 that for all $J \in \mathcal{L}$ and $L \in \mathcal{K}$, there is a unique $A \in \mathcal{L}$ such that $AJ = p^2 L$. By Theorem 3.6 we have $|\mathcal{L}| = |\mathcal{K}| = p$, and hence $|\{(A, J) \in \mathcal{L}^2 \mid AJ = p^2 L\}| = p$ for all $L \in \mathcal{K}$. Since $p$ is odd, we infer that for each $L \in \mathcal{K}$ there is some $A \in \mathcal{L}$ such that $A^2 = p^2 L$. Consequently, every $L \in \mathcal{K}$ is principal. Now let $J \in \mathcal{L}$. There is some $B \in \mathcal{K}$ such that $IJ = p^2 B$, and thus $IJ$ is principal. Therefore, $J$ is not principal. □

Next we show that the assumption that $p$ is odd in Remark 4.16 is crucial.

*Example 4.17.* Let $\mathcal{O} = \mathbb{Z} + 2\sqrt{-2}\mathbb{Z}$ be the order in the quadratic number field $K = \mathbb{Q}(\sqrt{-2})$ with conductor $2\mathcal{O}_K$. Let $I = 8\mathbb{Z} + 2\sqrt{-2}\mathbb{Z}$ and $J = 8\mathbb{Z} + (4 + 2\sqrt{-2})\mathbb{Z}$. Then 2 is ramified, $|\mathrm{Pic}(\mathcal{O})| = 2$, $I, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}))$, $\mathcal{N}(I) = \mathcal{N}(J) = 8$, $I$ is principal and $J$ is not principal.

*Proof.* It is clear that $J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}))$ and $\mathcal{N}(J) = 8$. By the proof of Theorem 4.14, it remains to show that $J$ is not principal. Assume that $J$ is principal. Then there are some $a, b \in \mathbb{Z}$ such that $J = (8a + 4b + 2\sqrt{-2}b)\mathcal{O}$, and hence $8 = \mathcal{N}(J) = |\mathcal{N}_{K/\mathbb{Q}}(8a + 4b + 2\sqrt{-2}b)| = |(8a + 4b)^2 + 8b^2|$. Therefore, $2(2a + b)^2 + b^2 = 1$. It is clear that $|b| \le 1$. If $b = 0$, then $8a^2 = 1$, a contradiction. Therefore, $|b| = 1$ and $2a + b = 0$, a contradiction. □

**Lemma 4.18.** *Let $d \in \mathbb{N}_{\ge 2}$ be squarefree, let $K = \mathbb{Q}(\sqrt{d})$, let $\mathcal{O}$ be the order in $K$ with conductor $f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\ge 2}$, and let $p$ be a ramified prime with $\mathrm{v}_p(f) = 1$. If ($p \equiv 1 \mod 4$ and $(\frac{d/p}{p}) = -1$) or ($(\frac{p}{q}) = -1$ for some prime $q$ with $q \equiv 1 \mod 4$ and $q \mid df$), then each $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(I) = p^3$ is not principal.*

*Proof.* Note that if $p$ is odd, then $\{I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(I) = p^3\} = \{p^3\mathbb{Z} + (p^2 k + \frac{\varepsilon p^2 + f\sqrt{d_K}}{2})\mathbb{Z} \mid k \in [0, p-1]\}$. Moreover, if $p = 2$ and $d$ is odd, then $\{I \in \mathcal{A}(\mathcal{I}_p^*$

$(\mathcal{O})) \mid \mathcal{N}(I) = p^3\} = \{8\mathbb{Z} + (2k + f\sqrt{d})\mathbb{Z} \mid k \in \{1, 3\}\}$. Furthermore, if $p = 2$ and $d$ is even, then $\{I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O})) \mid \mathcal{N}(I) = p^3\} = \{8\mathbb{Z} + (2k + f\sqrt{d})\mathbb{Z} \mid k \in \{0, 2\}\}$.

CASE 1: $p \equiv 1 \mod 4$ and $(\frac{d/p}{p}) = -1$. Let $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ be such that $\mathcal{N}(I) = p^3$. Since $p$ is odd, we have $I = p^3\mathbb{Z} + (p^2k + \frac{\varepsilon p^2 + f\sqrt{d_K}}{2})\mathbb{Z}$ for some $k \in [0, p-1]$. Assume that $I$ is principal. Then there are some $a, b \in \mathbb{Z}$ such that $I = (p^3a + p^2bk + \frac{\varepsilon p^2 + f\sqrt{d_K}}{2}b)\mathcal{O}$. We infer that $p^3 = \mathcal{N}(I) = |\mathcal{N}_{K/\mathbb{Q}}(p^3a + p^2bk + \frac{\varepsilon p^2 + f\sqrt{d_K}}{2}b)| = \frac{1}{4}|p^4(2pa + 2bk + \varepsilon b)^2 - f^2b^2d_K|$, and hence $\frac{f^2}{p^2}b^2\frac{d_K}{p} \equiv 4\beta \mod p$ for some $\beta \in \{-1, 1\}$. Since $p \equiv 1 \mod 4$, we have $(\frac{-1}{p}) = 1$, and thus $(\frac{d/p}{p}) = (\frac{d_K/p}{p}) = (\frac{f^2b^2d_K/p^3}{p}) = (\frac{4\beta}{p}) = 1$, a contradiction.

CASE 2: There is some prime $q$ such that $q \equiv 1 \mod 4$, $q \mid df$ and $(\frac{p}{q}) = -1$. Let $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ be such that $\mathcal{N}(I) = p^3$. First let $p$ be odd. Then $I = p^3\mathbb{Z} + (p^2k + \frac{\varepsilon p^2 + f\sqrt{d_K}}{2})\mathbb{Z}$ for some $k \in [0, p-1]$. Assume that $I$ is principal. Then there are some $a, b \in \mathbb{Z}$ such that $I = (p^3a + p^2bk + \frac{\varepsilon p^2 + f\sqrt{d_K}}{2}b)\mathcal{O}$. This implies that $p^3 = \mathcal{N}(I) = |\mathcal{N}_{K/\mathbb{Q}}(p^3a + p^2bk + \frac{\varepsilon p^2 + f\sqrt{d_K}}{2}b)| = \frac{1}{4}|p^4(2pa + 2bk + \varepsilon b)^2 - f^2b^2d_K|$, and thus $\ell^2 \equiv 4\beta p^3 \mod q$ for some $\ell \in \mathbb{Z}$ and $\beta \in \{-1, 1\}$. Since $q \equiv 1 \mod 4$, we have $(\frac{-1}{q}) = 1$, and hence $(\frac{p}{q})^3 = (\frac{4\beta p^3}{q}) = 1$. Therefore, $(\frac{p}{q}) = 1$, a contradiction.

Now let $p = 2$. Then $I = 8\mathbb{Z} + (2k + f\sqrt{d})\mathbb{Z}$ for some $k \in [0, 3]$. Assume that $I$ is principal. Then there are some $a, b \in \mathbb{Z}$ such that $I = (8a + 2bk + bf\sqrt{d})\mathcal{O}$. Consequently, $8 = \mathcal{N}(I) = |(8a + 2bk)^2 - b^2f^2d|$, and thus $\ell^2 \equiv 8\beta \mod q$ for some $\ell \in \mathbb{Z}$ and $\beta \in \{-1, 1\}$. This implies that $(\frac{2}{q})^3 = (\frac{8\beta}{q}) = 1$. Therefore, $(\frac{2}{q}) = 1$, a contradiction. □

**Proposition 4.19.** *Let $d \in \mathbb{N}_{\geq 2}$ be squarefree, let $K = \mathbb{Q}(\sqrt{d})$, and let $\mathcal{O}$ be the order in $K$ with conductor $f\mathcal{O}_K$ such that $f$ is a nonempty squarefree product of ramified primes times a squarefree product of inert primes and* $|\text{Pic}(\mathcal{O})| = |\text{Pic}(\mathcal{O}_K)| = 2$. *If for every ramified prime divisor $p$ of $f$, we have ($p \equiv 1 \mod 4$ and $(\frac{d/p}{p}) = -1$) or ($(\frac{p}{q}) = -1$ for some prime $q$ with $q \equiv 1 \mod 4$ and $q \mid df$), then* $\min \Delta(\mathcal{O}) = 2$.

*Proof.* It follows by Lemma 4.18 that for every ramified prime divisor $p$ of $f$ and every $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ with $\mathcal{N}(I) = p^3$, we have $I$ is not principal. It follows by the claim in the proof of Theorem 4.14 that $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$ is principal if and only if $\mathcal{N}(I) = p^2$. Now let $p$ be an inert prime divisor of $f$ and let $J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}))$. Since $|\text{Pic}(\mathcal{O})| = |\text{Pic}(\mathcal{O}_K)|$, it follows that the group epimorphism $\theta : \text{Pic}(\mathcal{O}) \to \text{Pic}(\mathcal{O}_K)$ defined by $\theta([L]) = [L\mathcal{O}_K]$ for all $L \in \mathcal{I}^*(\mathcal{O})$ is a group isomorphism. Set $P = p\mathcal{O}_K$. Then $J\mathcal{O}_K$ is a $P$-primary ideal of $\mathcal{O}_K$, and hence $J\mathcal{O}_K$ is a principal ideal of $\mathcal{O}_K$. Since $\theta$ is an isomorphism, we infer that $J$ is a principal ideal of $\mathcal{O}$. Now it follows by Theorem 4.14 that $\min \Delta(\mathcal{O}) = 2$. □

Next we provide two counterexamples that show that the additional assumption on the ramified prime divisors of $f$ in Proposition 4.19 is important.

*Example 4.20.* There is some real quadratic number field $K$ and some order $\mathcal{O}$ in $K$ with conductor $p\mathcal{O}_K$ for some ramified prime $p$ such that $p \equiv 1 \mod 4$, $|\mathrm{Pic}(\mathcal{O})| = |\mathrm{Pic}(\mathcal{O}_K)| = 2$, and $\min \Delta(\mathcal{O}) = 1$.

*Proof.* Let $\mathcal{O} = \mathbb{Z} + 5\sqrt{30}\mathbb{Z}$ be the order in the real quadratic number field $K = \mathbb{Q}(\sqrt{30})$ with conductor $5\mathcal{O}_K$. Observe that 5 is ramified, $5 \equiv 1 \mod 4$, $|\mathrm{Pic}(\mathcal{O}_K)| = 2$ and $\alpha = 11 + 2\sqrt{30}$ is a fundamental unit of $\mathcal{O}_K$. Since $\alpha \notin \mathcal{O}$ and $(\mathcal{O}_K^\times : \mathcal{O}^\times) \mid 5$, we infer that $(\mathcal{O}_K^\times : \mathcal{O}^\times) = 5$, and hence $|\mathrm{Pic}(\mathcal{O})| = |\mathrm{Pic}(\mathcal{O}_K)| \frac{5}{(\mathcal{O}_K^\times : \mathcal{O}^\times)} = 2$. Let $I = 125\mathbb{Z} + 5\sqrt{30}\mathbb{Z}$. Then $I \in \mathcal{A}(\mathcal{I}_5^*(\mathcal{O}))$ with $\mathcal{N}(I) = 125$. Since $I = (12625 + 2305\sqrt{30})\mathcal{O}$ is principal, we infer by Theorem 4.14 that $\min \Delta(\mathcal{O}) = 1$. □

*Example 4.21.* There is some real quadratic number field $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{N}_{\geq 2}$ squarefree and some order $\mathcal{O}$ in $K$ with conductor $p\mathcal{O}_K$ for some odd ramified prime $p$ such that $(\frac{d/p}{p}) = -1$, $|\mathrm{Pic}(\mathcal{O})| = |\mathrm{Pic}(\mathcal{O}_K)| = 2$, and $\min \Delta(\mathcal{O}) = 1$.

*Proof.* Let $\mathcal{O} = \mathbb{Z} + 7\sqrt{42}\mathbb{Z}$ be the order in the real quadratic number field $K = \mathbb{Q}(\sqrt{42})$ with conductor $7\mathcal{O}_K$. Note that 7 is an odd ramified prime, $(\frac{42/7}{7}) = -1$, $|\mathrm{Pic}(\mathcal{O}_K)| = 2$ and $\alpha = 13 + 2\sqrt{42}$ is a fundamental unit of $\mathcal{O}_K$. We have $\alpha \notin \mathcal{O}$ and $(\mathcal{O}_K^\times : \mathcal{O}^\times) \mid 7$. Therefore, $(\mathcal{O}_K^\times : \mathcal{O}^\times) = 7$, and thus $|\mathrm{Pic}(\mathcal{O})| = |\mathrm{Pic}(\mathcal{O}_K)| \frac{7}{(\mathcal{O}_K^\times : \mathcal{O}^\times)} = 2$. Set $I = 343\mathbb{Z} + 7\sqrt{42}\mathbb{Z}$. Then $I \in \mathcal{A}(\mathcal{I}_7^*(\mathcal{O}))$, $\mathcal{N}(I) = 343$, and $I = (825601 + 127393\sqrt{42})\mathcal{O}$ is principal. Consequently, $\min \Delta(\mathcal{O}) = 1$ by Theorem 4.14. □

Finally, we provide the examples of orders $\mathcal{O}$ in quadratic number fields with $\min \Delta(\mathcal{O}) = 2$.

*Example 4.22.* Let $K$ be a quadratic number field and $\mathcal{O}$ the order in $K$ with conductor $f\mathcal{O}_K$ such that $(f, d_K) \in \{(2, 60), (3, 60), (5, 60), (6, 60), (10, 60)\} \cup \{(15, 60), (30, 60), (10, 85), (35, 40), (195, 65), (30, 365)\}$.

1. If $(f, d_K) \in \{(2, 60), (3, 60), (5, 60)\}$, then $f$ is a ramified prime.
2. If $(f, d_K) \in \{(6, 60), (10, 60), (15, 60)\}$, then $f$ is the product of two distinct ramified primes.
3. If $(f, d_K) = (30, 60)$, then $f$ is the product of three distinct ramified primes.
4. If $(f, d_K) \in \{(10, 85), (35, 40)\}$, then $f$ is the product of an inert prime and a ramified prime.
5. If $(f, d_K) = (195, 65)$, then $f$ is the product of an inert prime and two distinct ramified primes.
6. If $(f, d_K) = (30, 365)$, then $f$ is the product of two distinct inert primes and a ramified prime.
7. $\min \Delta(\mathcal{O}) = 2$.

*Proof.* It is straightforward to prove the first six assertions. We prove the last assertion in the case that $d_K = 60$ and $f \in \mathbb{N}_{\geq 2}$ is a divisor of 30. The remaining cases can be proved in analogy by using Proposition 4.19. It is clear that 2, 3, and 5 are ramified primes. Note that $|\mathrm{Pic}(\mathcal{O}_K)| = 2$ (e.g., [25, page 22]) and $\alpha = 4 + \sqrt{15}$ is a fundamental unit of $\mathcal{O}_K$.

We have $\alpha^2 = 31 + 8\sqrt{15}$, $\alpha^3 = 244 + 63\sqrt{15}$, and $\alpha^5 = 15124 + 3905\sqrt{15}$. Moreover, $\alpha^6 = 119071 + 30744\sqrt{15}$, $\alpha^{10} = 457470751 + 118118440\sqrt{15}$, and $\alpha^{15} = 13837575261124 + 3572846569215\sqrt{15}$. Set $k = (\mathcal{O}_K^\times : \mathcal{O}^\times)$. Then $k$ is a divisor of $f$ by (4.1). Observe that $\alpha \notin \mathbb{Z} + 2\sqrt{15}\mathbb{Z}$, $\alpha \notin \mathbb{Z} + 3\sqrt{15}\mathbb{Z}$, $\alpha \notin \mathbb{Z} + 5\sqrt{15}\mathbb{Z}$, $\alpha^2, \alpha^3 \notin \mathbb{Z} + 6\sqrt{15}\mathbb{Z}$, $\alpha^2, \alpha^5 \notin \mathbb{Z} + 10\sqrt{15}\mathbb{Z}$, $\alpha^3, \alpha^5 \notin \mathbb{Z} + 15\sqrt{15}\mathbb{Z}$, and $\alpha^6, \alpha^{10}, \alpha^{15} \notin \mathbb{Z} + 30\sqrt{15}\mathbb{Z}$. This implies that $k = f$, and hence $|\mathrm{Pic}(\mathcal{O})| = \frac{f}{k}|\mathrm{Pic}(\mathcal{O}_K)| = |\mathrm{Pic}(\mathcal{O}_K)| = 2$ by (4.1). We have $5 \equiv 1 \mod 4$ and $(\frac{15/5}{5}) = (\frac{3}{5}) = (\frac{2}{5}) = -1$. We infer by Proposition 4.19 that $\min \Delta(\mathcal{O}) = 2$. □

## 5 Unions of Sets of Lengths

The goal of this section is to show that all unions of sets of lengths of the monoid of (invertible) ideals in orders of quadratic number fields are intervals (Theorem 5.2). To gather the background on unions of sets of lengths, let $H$ be an atomic monoid with $H \neq H^\times$ and $k \in \mathbb{N}_0$. Then

$$\mathcal{U}_k(H) = \bigcup_{k \in L \in \mathcal{L}(H)} L \quad \text{denotes the } \textit{union of sets of lengths} \text{ containing } k \text{ and}$$

$$\rho_k(H) = \sup \mathcal{U}_k(H) \quad \text{is the } \textit{kth elasticity} \text{ of } H.$$

Then, for the *elasticity* $\rho(H)$ of $H$, we have [12, Proposition 2.7],

$$\rho(H) = \sup\{\rho(L) \mid L \in \mathcal{L}(H)\} = \lim_{k \to \infty} \frac{\rho_k(H)}{k}.$$

Clearly, $\mathcal{U}_0(H) = \{0\}$, $\mathcal{U}_1(H) = \{1\}$ and $\mathcal{U}_k(H)$ is the set of all $\ell \in \mathbb{N}_0$ with the following property:

There are atoms $u_1, \ldots, u_k, v_1, \ldots, v_\ell$ in $H$ such that $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_\ell$.

Let $d \in \mathbb{N}$ and $M \in \mathbb{N}_0$. A subset $L \subset \mathbb{Z}$ is called an AAP (with difference $d$ and bound $M$) if

$$L = y + \left(L' \cup L^* \cup L''\right) \subset y + d\mathbb{Z},$$

where $y \in \mathbb{Z}$, $L^*$ is a nonempty arithmetical progression with difference $d$ and $\min L^* = 0$, $L' \subset [-M, -1]$, and $L'' \subset \sup L^* + [1, M]$ (with the convention that $L'' = \emptyset$ if $L^*$ is infinite). We say that $H$ satisfies the *Structure Theorem for Unions* if there are $d \in \mathbb{N}$ and $M \in \mathbb{N}_0$ such that $\mathcal{U}_k(H)$ is an AAP with difference $d$ and bound $M$ for all sufficiently large $k \in \mathbb{N}$. If $\Delta(H)$ is finite and the structure theorem for unions holds for some parameter $d \in \mathbb{N}$, then $d = \min \Delta(H)$ [12, Lemma 2.12].

The structure theorem for unions holds for a wealth of monoids and domains (see [2, 13, 34] for recent contributions and see [12, Theorem 4.2] for an example where it does not hold). Since it holds for C-monoids [14], it holds for the monoid of invertible ideals of orders in number fields. In some special cases (including Krull monoids having prime divisors in all classes) all unions of sets of lengths are intervals, in other words the structure theorem for unions holds with $d = 1$ and $M = 0$ [15, Theorem 3.1.3], [18, Theorem 5.8], [33]. In Theorem 5.2 we show that the same is true for the monoids of (invertible) ideals of orders in quadratic number fields.

**Proposition 5.1.** *Let $p$ be a prime divisor of $f$ and let $N = \sup\{\mathrm{v}_p(\mathcal{N}(A)) \mid A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))\}$.*

1. *If $p$ splits, then $\mathcal{U}_\ell(\mathcal{I}_p(\mathcal{O}_f)) = \mathcal{U}_\ell(\mathcal{I}_p^*(\mathcal{O}_f)) = \mathbb{N}_{\geq 2}$ for all $\ell \in \mathbb{N}_{\geq 2}$.*
2. *If $p$ does not split, then $\mathcal{U}_\ell(\mathcal{I}_p(\mathcal{O}_f)) \cap \mathbb{N}_{\geq \ell} = \mathcal{U}_\ell(\mathcal{I}_p^*(\mathcal{O}_f)) \cap \mathbb{N}_{\geq \ell} = [\ell, \lfloor \frac{\ell N}{2} \rfloor]$ for all $\ell \in \mathbb{N}_{\geq 2}$.*

*Proof.* We prove 1. and 2. simultaneously. By Proposition 3.3.3 we can assume without restriction that $f = p^{\mathrm{v}_p(f)}$. First we show that both assertions are true for $\ell = 2$. It follows from Theorem 3.6 that $[2, N] = [2, 2\mathrm{v}_p(f)] \cup \{\mathrm{v}_p(\mathcal{N}(A)) \mid A \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))\}$. It is obvious that $\mathcal{U}_2(\mathcal{I}_p^*(\mathcal{O}_f)) \subset \mathcal{U}_2(\mathcal{I}_p(\mathcal{O}_f))$. It follows from Lemma 4.9 that $\mathcal{U}_2(\mathcal{I}_p(\mathcal{O}_f)) \subset [2, N]$.

Let $k \in [2, N]$. It remains to show that $k \in \mathcal{U}_2(\mathcal{I}_p^*(\mathcal{O}_f))$. If $k > 2\mathrm{v}_p(f)$, then there is some $I \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = p^k$. It follows by Proposition 3.2.5 that $I\overline{I} = (p\mathcal{O}_f)^k$, and hence $k \in \mathcal{U}_2(\mathcal{I}_p^*(\mathcal{O}_f))$. Now let $k \leq 2\mathrm{v}_p(f)$. By Proposition 4.8.1 we can assume without restriction that $\mathrm{v}_p(f) \geq 2$ and $k \geq 4$.

CASE 1: $d \not\equiv 1 \mod 4$ or ($d \equiv 1 \mod 4$, $p = 2$ and $k \leq 2(\mathrm{v}_2(f) - 1)$). We set $a = \mathrm{v}_p(\mathcal{N}_{K/\mathbb{Q}}(p^{k-2} + \tau))$ and $b = \mathrm{v}_p(\mathcal{N}_{K/\mathbb{Q}}(p^{k-2}(p-1) + \tau))$. Observe that if $d \not\equiv 1 \mod 4$, then $a, b \geq \min\{2k - 4, 2\mathrm{v}_p(f)\} \geq k$. Moreover, if $d \equiv 1 \mod 4$, $p = 2$ and $k \leq 2(\mathrm{v}_2(f) - 1)$, then $a, b \geq \min\{2k - 4, 2(\mathrm{v}_2(f) - 1)\} \geq k$. Set $I = p^a\mathbb{Z} + (p^{k-2} + \tau)\mathbb{Z}$ and $J = p^b\mathbb{Z} + (p^{k-2}(p-1) + \tau)\mathbb{Z}$. Then $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, $\min\{a, b, \mathrm{v}_p(p^{k-2} + p^{k-2}(p-1) + \varepsilon)\} = k - 1$, and $a + b - 2(k-1) > 0$. Therefore, there is some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $IJ = p^{k-1}L$, and hence $k \in \mathsf{L}(IJ) \subset \mathcal{U}_2(\mathcal{I}_p^*(\mathcal{O}_f))$.

CASE 2: $d \equiv 1 \mod 4$ and $p \neq 2$. We set $a = \mathrm{v}_p(\mathcal{N}_{K/\mathbb{Q}}(\frac{p^{k-2}-1}{2} + \tau))$ and $b = \mathrm{v}_p(\mathcal{N}_{K/\mathbb{Q}}(\frac{p^{k-2}(p^2+p-1)-1}{2} + \tau))$. Note that $a, b \geq \min\{2k-4, 2\mathrm{v}_p(f)\} \geq k$. Set $I = p^a\mathbb{Z} + (\frac{p^{k-2}-1}{2} + \tau)\mathbb{Z}$ and $J = p^b\mathbb{Z} + (\frac{p^{k-2}(p^2+p-1)-1}{2} + \tau)\mathbb{Z}$. Then $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$, $\min\{a, b, \mathrm{v}_p(\frac{p^{k-2}-1}{2} + \frac{p^{k-2}(p^2+p-1)-1}{2} + \varepsilon)\} = k - 1$, and $a + b - 2(k-1) > 0$. Consequently, there is some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $IJ = p^{k-1}L$, and thus $k \in \mathsf{L}(IJ) \subset \mathcal{U}_2(\mathcal{I}_p^*(\mathcal{O}_f))$.

CASE 3: $d \equiv 1 \mod 8$, $p = 2$ and $k \in \{2\mathrm{v}_2(f) - 1, 2\mathrm{v}_2(f)\}$. Set $h = \mathrm{v}_2(f)$. If $h = 2$, then $k = 4$, and hence $k \in \mathcal{U}_2(\mathcal{I}_2^*(\mathcal{O}_f))$ by Proposition 4.4. Now let $h \geq 3$. Note that 2 splits. By Theorem 3.6 there are some $I, J, L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ such that $\mathcal{N}(I) = 2^{2h+1}$, $\mathcal{N}(J) = 2^{2h+2}$ and $\mathcal{N}(L) = 16$. By Proposition 3.2.5 we have $L\overline{L} = 16\mathcal{O}_f$, $I\overline{I} = 2^{2h+1}\mathcal{O}_f = 2^{2h-3}L\overline{L}$ and $J\overline{J} = 2^{2h+2}\mathcal{O}_f = 2^{2h-2}L\overline{L}$. We infer that $k \in \{2h-1, 2h\} \subset \mathcal{U}_2(\mathcal{I}_2^*(\mathcal{O}_f))$.

CASE 4: $d \equiv 5 \mod 8$, $p = 2$ and $k \in \{2\mathsf{v}_2(f) - 1, 2\mathsf{v}_2(f)\}$. Set $h = \mathsf{v}_2(f)$. If $h = 2$, then $k = 4$, and thus $k \in \mathcal{U}_2(\mathcal{I}_2^*(\mathcal{O}_f))$ by Proposition 4.4. Now let $h \geq 3$. Set $A = 2^{2h}\mathbb{Z} + (2^{h-1} + \tau)\mathbb{Z}$, $B = 2^{2h}\mathbb{Z} + (2^{2h-2} - 2^{h-1} + \tau)\mathbb{Z}$, and $C = 2^{2h}\mathbb{Z} + (2^{2h-1} - 2^{h-1} + \tau)\mathbb{Z}$. Then $A, B, C \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$, $AB = 2^{2h-2}I$ and $AC = 2^{2h-1}J$ for some $I, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$. Therefore, $k \in \{2h - 1, 2h\} \subset \mathcal{U}_2(\mathcal{I}_2^*(\mathcal{O}_f))$.

So far we have proved that both assertions are true for $\ell = 2$. If $p$ splits, then we have $N = \infty$ by Theorem 3.6, and hence $\mathcal{U}_2(\mathcal{I}_p(\mathcal{O}_f)) = \mathcal{U}_2(\mathcal{I}_p^*(\mathcal{O}_f)) = \mathbb{N}_{\geq 2}$. The first assertion now follows easily by induction on $\ell$. Now let $p$ not split. Then $N < \infty$. Next we show that 2. is true for $\ell = 3$.

Since $[3, N+1] = \{1\} + \mathcal{U}_2(\mathcal{I}_p^*(\mathcal{O}_f)) \subset \mathcal{U}_3(\mathcal{I}_p^*(\mathcal{O}_f)) \cap \mathbb{N}_{\geq 3} \subset \mathcal{U}_3(\mathcal{I}_p(\mathcal{O}_f)) \cap \mathbb{N}_{\geq 3} \subset [3, \lfloor \frac{3N}{2} \rfloor]$ by Lemma 4.9 and $N \in \{2\mathsf{v}_p(f), 2\mathsf{v}_p(f) + 1\}$, it remains to show that $N + m \in \mathcal{U}_3(\mathcal{I}_p^*(\mathcal{O}_f))$ for all $m \in [2, \mathsf{v}_p(f)]$. Let $m \in [2, \mathsf{v}_p(f)]$. It is sufficient to show that there are some $I, J, L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ such that $IJ = p^m L$ and $\mathcal{N}(L) = p^N$, since then $IJ\overline{L} = p^{N+m}\mathcal{O}_f$ by Proposition 3.2.5, and thus $N + m \in \mathcal{U}_3(\mathcal{I}_p^*(\mathcal{O}_f))$.

CASE 1: $p$ is inert. Observe that $N = 2\mathsf{v}_p(f)$ by Theorem 3.6. Let $m \in [2, \mathsf{v}_p(f)]$. First let $p \neq 2$. If $d \not\equiv 1 \mod 4$, then set $I = p^{2m}\mathbb{Z} + (p^m + \tau)\mathbb{Z}$ and $J = p^{2\mathsf{v}_p(f)}\mathbb{Z} + (p^{2\mathsf{v}_p(f)-m} + \tau)\mathbb{Z}$. If $d \equiv 1 \mod 4$, then set $I = p^{2m}\mathbb{Z} + (\frac{p^m - 1}{2} + \tau)\mathbb{Z}$ and $J = p^{2\mathsf{v}_p(f)}\mathbb{Z} + (\frac{p^{2\mathsf{v}_p(f)-m} - 1}{2} + \tau)\mathbb{Z}$. In any case we have $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ and $IJ = p^m L$ for some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ with $\mathcal{N}(L) = p^N$.

Next let $p = 2$. Since 2 is inert, it follows that $d \equiv 5 \mod 8$. If $m < \mathsf{v}_2(f) - 1$, then set $I = 2^{2m}\mathbb{Z} + (2^m + \tau)\mathbb{Z}$. If $m = \mathsf{v}_2(f) - 1$, then set $I = 2^{2m}\mathbb{Z} + \tau\mathbb{Z}$. Finally, if $m = \mathsf{v}_2(f)$, then set $I = 2^{2m}\mathbb{Z} + (2^{m-1} + \tau)\mathbb{Z}$. Set $J = 2^{2\mathsf{v}_2(f)}\mathbb{Z} + (2^{\mathsf{v}_2(f)-1} + \tau)\mathbb{Z}$. Observe that $I, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $IJ = 2^m L$ for some $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ with $\mathcal{N}(L) = 2^N$.

CASE 2: $p$ is ramified. It follows that $N = 2\mathsf{v}_p(f) + 1$ by Theorem 3.6. Let $m \in [2, \mathsf{v}_p(f)]$. First let $p \neq 2$. Since $p$ is ramified, we have $p \mid d$. If $d \not\equiv 1 \mod 4$, then set $I = p^{2m}\mathbb{Z} + (p^m + \tau)\mathbb{Z}$ and $J = p^{2\mathsf{v}_p(f)+1}\mathbb{Z} + (p^{\mathsf{v}_p(f)+1} + \tau)\mathbb{Z}$. If $d \equiv 1 \mod 4$, then set $I = p^{2m}\mathbb{Z} + (\frac{p^m - 1}{2} + \tau)\mathbb{Z}$ and $J = p^{2\mathsf{v}_p(f)+1}\mathbb{Z} + (\frac{p^{\mathsf{v}_p(f)+1} - 1}{2} + \tau)\mathbb{Z}$. We infer that $I, J \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ and $IJ = p^m L$ for some $L \in \mathcal{A}(\mathcal{I}_p^*(\mathcal{O}_f))$ with $\mathcal{N}(L) = p^N$ in any case.

Now let $p = 2$. Since 2 is ramified, we have $d \not\equiv 1 \mod 4$. If $d$ is even or $m < \mathsf{v}_2(f)$, then set $I = 2^{2m}\mathbb{Z} + (2^m + \tau)\mathbb{Z}$. If $d$ is odd and $m = \mathsf{v}_2(f)$, then set $I = 2^{2m}\mathbb{Z} + \tau\mathbb{Z}$. If $d$ is even, then set $J = 2^{2\mathsf{v}_2(f)+1}\mathbb{Z} + \tau\mathbb{Z}$. If $d$ is odd, then set $J = 2^{2\mathsf{v}_2(f)+1}\mathbb{Z} + (2^{\mathsf{v}_2(f)} + \tau)\mathbb{Z}$. In any case we have $I, J \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ and $IJ = 2^m L$ for some $L \in \mathcal{A}(\mathcal{I}_2^*(\mathcal{O}_f))$ with $\mathcal{N}(L) = 2^N$.

Finally, we prove the second assertion by induction on $\ell$. Let $\ell \in \mathbb{N}_{\geq 2}$ and let $H \in \{\mathcal{I}_p(\mathcal{O}_f), \mathcal{I}_p^*(\mathcal{O}_f)\}$. Without restriction we can assume that $\ell \geq 4$. We infer by the induction hypothesis that $(\mathcal{U}_{\ell-2}(H) \cap \mathbb{N}_{\geq \ell-2}) + \mathcal{U}_2(H) = [\ell - 2, \lfloor \frac{(\ell-2)N}{2} \rfloor] + [2, N] = [\ell, \lfloor \frac{\ell N}{2} \rfloor]$. Observe that $(\mathcal{U}_{\ell-2}(H) \cap \mathbb{N}_{\geq \ell-2}) + \mathcal{U}_2(H) \subset \mathcal{U}_\ell(H) \cap \mathbb{N}_{\geq \ell}$. It follows by Lemma 4.9 that $\mathcal{U}_\ell(H) \cap \mathbb{N}_{\geq \ell} \subset [\ell, \lfloor \frac{\ell N}{2} \rfloor]$, and thus $\mathcal{U}_\ell(H) \cap \mathbb{N}_{\geq \ell} = [\ell, \lfloor \frac{\ell N}{2} \rfloor]$. $\square$

**Theorem 5.2.** *Let $\mathcal{O}$ be an order in a quadratic number field $K$ with conductor $f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$.*

1. *If $f$ is divisible by a split prime, then $\mathcal{U}_k(\mathcal{I}(\mathcal{O})) = \mathcal{U}_k(\mathcal{I}^*(\mathcal{O})) = \mathbb{N}_{\geq 2}$ for all $k \in \mathbb{N}_{\geq 2}$.*
2. *Suppose that $f$ is not divisible by a split prime and set $M = \max\{\mathrm{v}_p(f) \mid p \in \mathbb{P}\}$. Then $\mathcal{U}_k(\mathcal{I}(\mathcal{O})) = \mathcal{U}_k(\mathcal{I}^*(\mathcal{O}))$ is a finite interval for all $k \in \mathbb{N}_{\geq 2}$, and for their maxima we have*
   (a) *If $\mathrm{v}_q(f) = M$ for a ramified prime $q$, then $\rho_k(\mathcal{I}(\mathcal{O})) = \rho_k(\mathcal{I}^*(\mathcal{O})) = kM + \lfloor \frac{k}{2} \rfloor$ for all $k \in \mathbb{N}_{\geq 2}$ and $\rho(\mathcal{I}(\mathcal{O})) = \rho(\mathcal{I}^*(\mathcal{O})) = M + \frac{1}{2}$.*
   (b) *If $\mathrm{v}_q(f) < M$ for all ramified primes $q$, then $\rho_k(\mathcal{I}(\mathcal{O})) = \rho_k(\mathcal{I}^*(\mathcal{O})) = kM$ for all $k \in \mathbb{N}_{\geq 2}$ and $\rho(\mathcal{I}(\mathcal{O})) = \rho(\mathcal{I}^*(\mathcal{O})) = M$.*

*Proof.* 1. Let $f$ be divisible by a split prime $p$ and let $k \in \mathbb{N}_{\geq 2}$. Since $\mathcal{I}_p^*(\mathcal{O})$ is a divisor-closed submonoid of $\mathcal{I}^*(\mathcal{O})$ and $\mathcal{I}_p(\mathcal{O})$ is a divisor-closed submonoid of $\mathcal{I}(\mathcal{O})$, it follows from Proposition 5.1.1 that $\mathcal{U}_k(\mathcal{I}(\mathcal{O})) = \mathcal{U}_k(\mathcal{I}^*(\mathcal{O})) = \mathbb{N}_{\geq 2}$.

2. Let $k \in \mathbb{N}_{\geq 2}$ and $\ell \in \mathcal{U}_k(\mathcal{I}(\mathcal{O}))$. There are $I_i \in \mathcal{A}(\mathcal{I}(\mathcal{O}))$ for each $i \in [1, k]$ and $J_j \in \mathcal{A}(\mathcal{I}(\mathcal{O}))$ for each $j \in [1, \ell]$ such that $\prod_{i=1}^{k} I_i = \prod_{j=1}^{\ell} J_j$. Note that $\sqrt{I_i}, \sqrt{J_j} \in \mathfrak{X}(\mathcal{O})$ for all $i \in [1, k]$ and $j \in [1, \ell]$. For $P \in \mathfrak{X}(\mathcal{O})$ set $k_P = |\{i \in [1, k] \mid \sqrt{I_i} = P\}|$ and $\ell_P = |\{j \in [1, \ell] \mid \sqrt{J_j} = P\}|$. If $p$ is a prime divisor of $f$, then set $k_p = k_{P_{f,p}}$ and $\ell_p = \ell_{P_{f,p}}$. Observe that $k = \sum_{P \in \mathfrak{X}(\mathcal{O})} k_P$ and $\ell = \sum_{P \in \mathfrak{X}(\mathcal{O})} \ell_P$. Recall that the $P$-primary components of $\prod_{i=1}^{k} I_i$ are uniquely determined, and thus $\ell_P \in \mathcal{U}_{k_P}(\mathcal{I}_P(\mathcal{O}))$ for all $P \in \mathfrak{X}(\mathcal{O})$. If $P \in \mathfrak{X}(\mathcal{O})$ does not contain the conductor, then $\mathcal{I}_P(\mathcal{O})$ is factorial, and hence $\ell_P = k_P$. Also note that if $P \in \mathfrak{X}(\mathcal{O})$ and $k_P \leq 1$, then $\ell_P = k_P$. If $p$ is an inert prime that divides $f$, then it follows from Proposition 5.1.2 and Theorem 3.6 that $\rho_r(\mathcal{I}_p(\mathcal{O})) = \rho_r(\mathcal{I}_p^*(\mathcal{O})) = r\mathrm{v}_p(f)$ for all $r \in \mathbb{N}_{\geq 2}$. We infer again by Proposition 5.1.2 and Theorem 3.6 that $\rho_r(\mathcal{I}_p(\mathcal{O})) = \rho_r(\mathcal{I}_p^*(\mathcal{O})) = r\mathrm{v}_p(f) + \lfloor \frac{r}{2} \rfloor$ for all ramified primes $p$ that divide $f$ and all $r \in \mathbb{N}_{\geq 2}$.

CASE 1: $\mathrm{v}_q(f) = M$ for some ramified prime $q$. If $P \in \mathfrak{X}(\mathcal{O})$, then $\ell_P \leq k_P M + \lfloor \frac{k_P}{2} \rfloor$.

Consequently, $\ell = \sum_{P \in \mathfrak{X}(\mathcal{O})} \ell_P \leq (\sum_{P \in \mathfrak{X}(\mathcal{O})} k_P)M + \sum_{P \in \mathfrak{X}(\mathcal{O})} \lfloor \frac{k_P}{2} \rfloor \leq kM + \lfloor \frac{k}{2} \rfloor$. In particular, $\rho_k(\mathcal{I}(\mathcal{O})) \leq kM + \lfloor \frac{k}{2} \rfloor = \max\{\rho_k(\mathcal{I}_p^*(\mathcal{O})) \mid p \in \mathbb{P}, p \mid f\} \leq \rho_k(\mathcal{I}^*(\mathcal{O})) \leq \rho_k(\mathcal{I}(\mathcal{O}))$. This implies that $\rho_k(\mathcal{I}(\mathcal{O})) = \rho_k(\mathcal{I}^*(\mathcal{O})) = \max\{\rho_k(\mathcal{I}_p^*(\mathcal{O})) \mid p \in \mathbb{P}, p \mid f\} = kM + \lfloor \frac{k}{2} \rfloor$.

CASE 2: $\mathrm{v}_q(f) < M$ for all ramified primes $q$. Note that $\ell_p \leq k_p \mathrm{v}_p(f) + \lfloor \frac{k_p}{2} \rfloor \leq k_p M$ for all ramified primes $p$ that divide $f$. Therefore, $\ell_P \leq k_P M$ for all $P \in \mathfrak{X}(\mathcal{O})$. This implies that $\ell = \sum_{P \in \mathfrak{X}(\mathcal{O})} \ell_P \leq (\sum_{P \in \mathfrak{X}(\mathcal{O})} k_P)M = kM$. We infer that $\rho_k(\mathcal{I}(\mathcal{O})) \leq kM = \max\{\rho_k(\mathcal{I}_p^*(\mathcal{O})) \mid p \in \mathbb{P}, p \mid f\} \leq \rho_k(\mathcal{I}^*(\mathcal{O})) \leq \rho_k(\mathcal{I}(\mathcal{O}))$, and thus $\rho_k(\mathcal{I}(\mathcal{O})) = \rho_k(\mathcal{I}^*(\mathcal{O})) = \max\{\rho_k(\mathcal{I}_p^*(\mathcal{O})) \mid p \in \mathbb{P}, p \mid f\} = kM$.

By Proposition 5.1.2, we obtain that $\mathcal{U}_k(\mathcal{I}(\mathcal{O})) \cap \mathbb{N}_{\geq k} = \mathcal{U}_k(\mathcal{I}^*(\mathcal{O})) \cap \mathbb{N}_{\geq k}$ is a finite interval. Since the last assertion holds for every $k \in \mathbb{N}_{\geq 2}$, we infer that

$\mathcal{U}_k(\mathcal{I}(\mathcal{O})) = \mathcal{U}_k(\mathcal{I}^*(\mathcal{O}))$ is a finite interval for all $k \in \mathbb{N}_{\geq 2}$. If $\mathrm{v}_q(f) = M$ for some ramified prime $q$, then

$$\rho(\mathcal{I}(\mathcal{O})) = \rho(\mathcal{I}^*(\mathcal{O})) = \lim_{k\to\infty} \frac{\rho_k(\mathcal{I}(\mathcal{O}))}{k} = \lim_{k\to\infty} M + \frac{1}{k}\left\lfloor \frac{k}{2} \right\rfloor = M + \frac{1}{2}.$$

Finally, let $\mathrm{v}_q(f) < M$ for all ramified primes $q$. Then

$$\rho(\mathcal{I}(\mathcal{O})) = \rho(\mathcal{I}^*(\mathcal{O})) = \lim_{k\to\infty} \frac{\rho_k(\mathcal{I}(\mathcal{O}))}{k} = \lim_{k\to\infty} \frac{kM}{k} = M. \qquad \square$$

In a final remark we gather what is known on further arithmetical invariants of monoids of ideals of orders in quadratic number fields.

*Remark 5.3.* Let $\mathcal{O}$ be an order in a quadratic number field $K$ with conductor $f\mathcal{O}_K$ for some $f \in \mathbb{N}_{\geq 2}$.

1. The monotone catenary degree of $\mathcal{I}^*(\mathcal{O})$ is finite by [20, Corollary 5.14]. Precise values for the monotone catenary degree are available so far only in the seminormal case [18, Theorem 5.8].

2. The tame degree of $\mathcal{I}^*(\mathcal{O})$ is finite if and only if the elasticity is finite if and only if $f$ is not divisible by a split prime. This follows from Equations. 2.3 and 2.4, Theorem 5.2, and from [16, Theorem 3.1.5]. Precise values for the tame degree are not known so far.

3. For an atomic monoid $H$, the set $\{\rho(L) \mid L \in \mathcal{L}(H)\} \subset \mathbb{Q}_{\geq 1}$ of all elasticities was first studied by Chapman et al. and then it found further attention by several authors (e.g., [4, 7], [22, Theorem 5.5], [23, 35]). We say that $H$ is *fully elastic* if for every rational number $q$ with $1 < q < \rho(H)$ there is an $L \in \mathcal{L}(H)$ with $\rho(L) = q$. Since $\mathcal{I}^*(\mathcal{O})$ is cancellative and has a prime element, it is fully elastic by [3, Lemma 2.1]. Since $\mathcal{I}^*(\mathcal{O}) \subset \mathcal{I}(\mathcal{O})$ is divisor-closed and $\rho(\mathcal{I}(\mathcal{O})) = \rho(\mathcal{I}^*(\mathcal{O}))$ by Theorem 5.2, it follows that $\mathcal{I}(\mathcal{O})$ is fully elastic.

4. For an atomic monoid $H$, let

$$\daleth^*(H) = \{\min(L \setminus \{2\}) \mid 2 \in L \in \mathcal{L}(H) \text{ with } |L| > 1\} \subset \mathbb{N}_{\geq 3}.$$

By definition, we have $\daleth^*(H) \subset 2 + \Delta(H)$ and in [11, 23] the invariant $\daleth^*(H)$ was used as a tool to study $\Delta(H)$. Proposition 4.1.4 shows that, both for $H = \mathcal{I}(\mathcal{O})$ and for $H = \mathcal{I}^*(\mathcal{O})$, we have $\max \daleth^*(H) = 2 + \max \Delta(H)$.

**Acknowledgements** This work was supported by the Austrian Science Fund FWF, Project Numbers J4023-N35 and P28864-N35. We would like to thank the referee for carefully reading the manuscript and for many suggestions and comments that improved the quality of this paper and simplified the proof of Theorem 3.6.

## References


1. Anderson, D.D., Mott, J.L.: Cohen-Kaplansky domains: integral domains with a finite number of irreducible elements. J. Algebra **148**, 17–41 (1992)
2. Baeth, N.R., Smertnig, D.: Arithmetical invariants of local quaternion orders. Acta Arith. **186**, 143–177 (2018)
3. Baginski, P., Chapman, S.T., Crutchfield, C., Kennedy, K.G., Wright, M.: Elastic properties and prime elements. Result. Math. **49**, 187–200 (2006)
4. Barron, T., O'Neill, C., Pelayo, R.: On the set of elasticities in numerical monoids. Semigroup Forum **94**, 37–50 (2017)
5. Bowles, C., Chapman, S.T., Kaplan, N., Reiser, D.: On delta sets of numerical monoids. J. Algebra Appl. **5**, 695–718 (2006)
6. Butts, H.S., Pall, G.: Ideals not prime to the conductor in quadratic orders. Acta Arith. **21**, 261–270 (1972)
7. Chapman, S.T., Holden, M., Moore, T.: Full elasticity in atomic monoids and integral domains. Rocky Mt. J. Math. **36**, 1437–1455 (2006)
8. Colton, S., Kaplan, N.: The realization problem for delta sets of numerical monoids. J. Commut. Algebra **9**, 313–339 (2017)
9. Coykendall, J., Malcolmson, P., Okoh, F.: Inert primes and factorization in extensions of quadratic orders. Houston J. Math. **43**, 61–77 (2017)
10. Dobbs, D.E., Fontana, M.: Seminormal rings generated by algebraic integers. Mathematika **34**, 141–154 (1987)
11. Fan, Y., Geroldinger, A.: Minimal relations and catenary degrees in Krull monoids. J. Commut. Algebra **11**, 29–47 (2019)
12. Fan, Y., Geroldinger, A., Kainrath, F., Tringali, S.: Arithmetic of commutative semigroups with a focus on semigroups of ideals and modules. J. Algebra Appl. **11**, 1750234 (42 pages) (2017)
13. Fan, Y., Tringali, S.: Power monoids: a bridge between factorization theory and arithmetic combinatorics. J. Algebra **512**, 252–294 (2018)
14. Gao, W., Geroldinger, A.: On products of $k$ atoms. Monatsh. Math. **156**, 141–157 (2009)
15. Geroldinger, A.: Additive group theory and non-unique factorizations. Combinatorial Number Theory and Additive Group Theory, Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, pp. 1–86 (2009)
16. Geroldinger, A., Halter-Koch, F.: Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory. Pure and Applied Mathematics, vol. 278. Chapman & Hall/CRC (2006)
17. Geroldinger, A., Halter-Koch, F., Kaczorowski, J.: Non-unique factorizations in orders of global fields. J. Reine Angew. Math. **459**, 89–118 (1995)
18. Geroldinger, A., Kainrath, F., Reinhart, A.: Arithmetic of seminormal weakly Krull monoids and domains. J. Algebra **444**, 201–245 (2015)
19. Geroldinger, A., Lettl, G.: Factorization problems in semigroups. Semigroup Forum **40**, 23–38 (1990)
20. Geroldinger, A., Reinhart, A.: The monotone catenary degree of monoids of ideals. Internat. J. Algebra Comput. **29**, 419–458 (2019)
21. Geroldinger, A., Schmid, W.A.: A realization theorem for sets of distances. J. Algebra **481**, 188–198 (2017)
22. Geroldinger, A., Schmid, W.A., Zhong, Q.: Systems of sets of lengths: transfer Krull monoids versus weakly Krull monoids. In: Rings, Polynomials, and Modules, pp. 191–235. Springer, Cham (2017)
23. Geroldinger, A., Zhong, Q.: Sets of arithmetical invariants in transfer Krull monoids. J. Pure Appl. Algebra **223**, 3889–3918 (2019)
24. Geroldinger, A., Zhong, Q.: The set of distances in seminormal weakly Krull monoids. J. Pure Appl. Algebra **220**, 3713–3732 (2016)
25. Halter-Koch, F.: Quadratic Irrationals. Pure and Applied Mathematics, vol. 306. Chapman & Hall/CRC (2013)

26. Kainrath, F.: On local half-factorial orders. In: Arithmetical Properties of Commutative Rings and Monoids. Lecture Notes in Pure and Applied Mathematics, vol. 241, pp. 316–324. Chapman & Hall/CRC (2005)
27. Klaise, J.: Orders in quadratic imaginary fields of small class number (2012). https://warwick.ac.uk/fac/cross_fac/complexity/people/students/dtc/students2013/klaise/janis_klaise_ug_report.pdf
28. O'Neill, C., Pelayo, R.: Realisable sets of catenary degrees of numerical monoids. Bull. Australian Math. Soc. **97**, 240–245 (2018)
29. Peruginelli, G., Zanardo, P.: The lattice of primary ideals of orders in quadratic number fields. Int. J. Number Theory **12**(7), 2025–2040 (2016)
30. Philipp, A.: A precise result on the arithmetic of non-principal orders in algebraic number fields, J. Algebra Appl. **11**, 1250087, 42pp
31. Ribenboim, P.: Classical theory of Algebraic Numbers. Universitext, Springer, New York (2001)
32. Schmid, W.A.: Some recent results and open problems on sets of lengths of Krull monoids with finite class group. In: Multiplicative Ideal Theory and Factorization Theory, pp. 323–352. Springer (2016)
33. Smertnig, D.: Sets of lengths in maximal orders in central simple algebras. J. Algebra **390**, 1–43 (2013)
34. Tringali, S.: Structural properties of subadditive families with applications to factorization theory. Israel J. Math. **234**, 1–35 (2019)
35. Zhong, Q.: On elasticities of v-noetherian monoids. J. Algebra **34**, 145–167 (2019)

# UMT-domains: A Survey

**Gyu Whan Chang**

**Abstract** Let $D$ be an integral domain, $X$ be an indeterminate over $D$, and $D[X]$ be the polynomial ring over $D$. A nonzero prime ideal $Q$ of $D[X]$ is called an *upper to zero* in $D[X]$ if $Q \cap D = (0)$. We say that $D$ is a UMT-domain if each upper to zero in $D[X]$ is a maximal $t$-ideal of $D[X]$. The notion of UMT-domains was introduced by Houston and Zafrullah in 1989. In this paper, we survey the results on UMT-domains with focus on uppers to zero, Nagata rings, graded integral domains, and constructions of new UMT-domains.

**Keywords** $t$-operation · Upper to zero · UMT-domain · Nagata ring · Graded integral domain

## 1 Introduction

A Prüfer domain is an integral domain whose nonzero finitely generated ideals are invertible. It is well known that Dedekind domains are Prüfer domains, and Prüfer domains are Dedekind domains if and only if it is Noetherian. Hence, the notion of Prüfer domains is a natural generalization of Dedekind domains to non-Noetherian integral domains. It is well known that an integral domain $D$ is a Prüfer domain if and only if $D_M$ is a valuation domain for all maximal ideals $M$ of $D$. However, note that $D[X]$, the polynomial ring over $D$, is a Prüfer domain if and only if $D$ is a field. When we study the ideal-theoretic properties of integral domains, the so-called $t$-operation is very useful. For example, $D$ is a Krull domain if and only if every nonzero ideal of $D$ is $t$-invertible; a Krull domain is a UFD if and only if it has a trivial divisor class group; and a Krull domain is a Dedekind domain if and only if its Krull dimension is one. A P$v$MD is an integral domain whose nonzero finitely generated ideals are $t$-invertible; equivalently, $D_P$ is a valuation domain for all maximal $t$-ideals $P$ of $D$

G. W. Chang (✉)
Department of Mathematics Education, Incheon National University,
Incheon 22012, Korea
e-mail: whan@inu.ac.kr



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_3

[42, Theorem 5]. Hence, a Krull domain and a P$v$MD are the $t$-operation analogs of Dedekind domains and Prüfer domains, respectively. Moreover, $D$ is a Krull domain (resp., P$v$MD) if and only if $D[X]$ is a Krull domain (resp., P$v$MD). Thus, the class of P$v$MDs includes Dedekind domains, Prüfer domains, Krull domains, and polynomial rings over a P$v$MD.

A quasi-Prüfer domain is an integral domain whose integral closure is a Prüfer domain [31, Corollary 6.5.14]; a UMT-domain $D$ is an integral domain such that $D_P$ has the Prüfer integral closure for all maximal $t$-ideals $P$ of $D$; and $D$ is a P$v$MD if and only if $D$ is an integrally closed UMT-domain. Hence, UMT-domains can be considered as the $t$-operation analog of quasi-Prüfer domains or non-integrally closed P$v$MDs. The notion of UMT-domains was introduced by Houston and Zafrullah [46] and studied carefully by Fontana, Gabelli, and Houston [30]. In this paper, we survey several properties of UMT-domains. Precisely, this paper consists of five sections containing the introduction. In Section 2, we review the definitions and basic results on star operations (Section 2.1), $*$-invertibility (Section 2.2), $t$-class groups (Section 2.3), and P$v$MDs, Nagata rings, and Kronecker function rings (Section 2.4). In Section 3, we give basic properties of uppers to zero, several characterizations of UMT-domains (Section 3.1) and Kaplansky type theorems for uppers to zero (Section 3.2) which lead to the study of a general theory of almost factoriality. Section 4 is devoted to the UMT-domain property of graded integral domains. In Section 4.1, we first introduce some definitions for graded integral domains. We then study the UMT-domain property of graded integral domains in Section 4.2 (general case) and Section 4.3 (when $R_H$ is a UFD). Finally, in Section 5, we introduce the technique of constructing new UMT-domains from old one via semigroup rings and pullback.

## 2 Definitions Related to the $t$-operation

Throughout $D$ denotes an integral domain with quotient field $K$, $X$ is an indeterminate over $D$, $D[X]$ is the polynomial ring over $D$, and an overring of $D$ means a subring of $K$ containing $D$.

### 2.1 Star Operations

Let $\mathbf{F}(D)$ (resp., $\mathbf{f}(D)$) be the set of nonzero (resp., nonzero finitely generated) fractional ideals of $D$. A *star operation* on $D$ is a function $*$ from $\mathbf{F}(D)$ into $\mathbf{F}(D)$ satisfying the following three properties for all $0 \neq x \in K$ and $I, J \in \mathbf{F}(D)$:

1. $(xD)_* = xD$, $(xI)_* = xI_*$,
2. $I \subseteq I_*$, and $I \subseteq J$ implies $I_* \subseteq J_*$, and
3. $(I_*)_* = I_*$.

Given a star operation $*$ on $D$, we can construct two new star operations $*_f$ and $*_w$ on $D$ as follows:

- $I_{*_f} = \bigcup\{J_* \mid J \in \mathbf{f}(D)$ and $J \subseteq I\}$ and
- $I_{*_w} = \{x \in K \mid xJ \subseteq I$ for some $J \in \mathbf{f}(D)$ with $J_* = D\}$.

Then $(*_f)_f = *_f$ and $(*_w)_f = (*_f)_w = *_w$. We say that $*$ is of *finite character* if $*_f = *$; so $*_f$ and $*_w$ are of finite character. For $I \in \mathbf{F}(D)$, let $I_d = I$. Then $d$ is the identity function of $\mathbf{F}(D)$, and hence $d$ is a star operation on $D$ with $d = d_f = d_w$. For another well-known examples of star operations, note that if we let $I^{-1} = \{x \in K \mid xI \subseteq D\}$ for $I \in \mathbf{F}(D)$, then $I^{-1} \in \mathbf{F}(D)$. Hence, the $v$-operation given by $I_v = (I^{-1})^{-1}$ for all $I \in \mathbf{F}(D)$ is a star operation. The $t$-and $w$-operations are defined by $t = v_f$ and $w = v_w$, respectively.

**Lemma 2.1.** *Let $D$ be an integral domain, $I, J \in \mathbf{F}(D)$, $\{I_\alpha\}$ be a nonempty subset of $\mathbf{F}(D)$, and $*$ be a star operation on $D$.*

1. $I \subseteq I_{*_w} \subseteq I_{*_f} \subseteq I_*$.
2. $I_v = \bigcap\{xD \mid x \in K$ *and* $I \subseteq xD\}$.
3. $I_* \subseteq I_v$, *and hence* $I \subseteq I_{*_f} \subseteq I_t$ *and* $I \subseteq I_{*_w} \subseteq I_w$.
4. $(IJ)_* = (IJ_*)_* = (I_*J_*)_*$.
5. *If* $\bigcap_\alpha I_\alpha \neq (0)$, *then* $\bigcap_\alpha (I_\alpha)_* = (\bigcap_\alpha (I_\alpha)_*)_*$.

*Proof.* (1) Clear. (2) [39, Theorem 34.1]. (3) If $x \in K$ with $I \subseteq xD$, then $I_* \subseteq (xD)_* = xD$. Thus, $I_* \subseteq I_v$ by (2). (4) and (5) [39, Proposition 32.2].

Let $*$ be a star operation on $D$. An $I \in \mathbf{F}(D)$ is called a $*$-*ideal* if $I_* = I$. A $*$-ideal of $D$ is said to be of *finite type* if $I = J_*$ for some $J \in \mathbf{f}(D)$; so a $d$-ideal of finite type is just a nonzero finitely generated ideal. A $*$-ideal is a *maximal* $*$-*ideal* if it is maximal among proper integral $*$-ideals. Let $*$-Max$(D)$ be the set of maximal $*$-ideals of $D$. Hence, $d$-Max$(D)$ := Max$(D)$ is the set of maximal ideals of $D$. It may happen that $*$-Max$(D) = \emptyset$ even though $D$ is not a field as in the case of a rank-one nondiscrete valuation domain $D$ where $v$-Max$(D) = \emptyset$. However, we have the following nice properties of star operations of finite character.

**Lemma 2.2.** *Let $D$ be an integral domain and $*$ be a star operation of finite character on $D$ (e.g., $* = d, t$ or $w$).*

1. $*$-*Max*$(D) \neq \emptyset$ *if $D$ is not a field.*
2. *Each maximal $*$-ideal of $D$ is a prime ideal.*
3. *Each proper $*$-ideal of $D$ is contained in a maximal $*$-ideal.*
4. *Each prime ideal of $D$ minimal over a $*$-ideal is a $*$-ideal; so each height-one prime ideal is a $*$-ideal.*
5. $*$-*Max*$(D) = *_w$-*Max*$(D)$.
6. $D = \bigcap_{P \in *\text{-}Max(D)} D_P$.
7. $I_{*_w} = \bigcap_{P \in *\text{-}Max(D)} ID_P$ *for all* $I \in \mathbf{F}(D)$.

*Proof.* (1), (2), and (3) This can be proved by an easy argument of Zorn's lemma.

(4) Let $I$ be a $*$-ideal of $D$ and $P$ be a minimal prime ideal of $I$. It suffices to show that $P_* \subseteq P$. Let $0 \neq x \in P_*$. Then there is a $J \in \mathbf{f}(D)$ such that $J \subseteq P$ and $x \in J_*$. Note that $P$ is minimal over $I$ and $J$ is finitely generated. Hence, there are an integer $n \geq 1$ and $s \in D \setminus P$ so that $sJ^n \subseteq I$, and thus $s(J_*)^n \subseteq (sJ^n)_* \subseteq I_* = I \subseteq P$. Thus, $x \in J_* \subseteq P$.

(5) [5, Theorem 2.16]. (6) This is an easy exercise. (7) [5, Corollary 2.10].

Let $A \subseteq B$ be an extension of integral domains. As in [29], we say that $B$ is *t-linked* over $A$ if $I^{-1} = A$ for $I \in \mathbf{f}(A)$ implies $(IB)^{-1} = B$. It is easy to see that $B$ is $t$-linked over $A$ if and only if $B = \bigcap_{P \in t\text{-Max}(A)} B_P$ [18, Lemma 3.2], if and only if either $Q \cap A = (0)$ or $Q \cap A \neq (0)$ and $(Q \cap A)_t \subsetneq A$ for all $Q \in t\text{-Max}(B)$ [7, Propositions 2.1].

**Lemma 2.3.** ([58] or [28, Lemma 2.3]) *Let $R$ be a $t$-linked overring of an integral domain $D$. For each $A \in \mathbf{F}(D)$, let*

$$A_{w_D} = \{x \in K \mid xJ \subseteq A \textit{ for some } J \in \mathbf{f}(D) \textit{ with } J_v = D\}.$$

*Then $w_D$ is a star operation of finite character on $D$.*

We mean by $*$-dim$(D) = 1$ that $*$-Max$(D) \neq \emptyset$ and each prime $*$-ideal of $D$ is a maximal $*$-ideal of $D$. Clearly, if dim$(D) = 1$ (i.e., $D$ is one-dimensional), then $t$-dim$(D) = 1 = w$-dim$(D)$. For more on basic properties of star operations, the reader can refer to [39, Sections 32 and 34].

## 2.2 $*$-Invertibility

Let $*$ be a star operation on $D$. We say that an $I \in \mathbf{F}(D)$ is $*$-*invertible* if $(II^{-1})_* = D$. Clearly, if $*_f = *$, then $I$ is $*$-invertible if and only if $II^{-1} \nsubseteq P$ for all $P \in *$-Max$(D)$. Hence, by Lemma 2.2(5), $I$ is $*_f$-invertible if and only if $I$ is $*_w$-invertible. Note that $I = I_d \subseteq I_w \subseteq I_t \subseteq I_v$ for all $I \in \mathbf{F}(D)$; so $I$ is invertible $\Rightarrow$ $I$ is $w$-invertible $\Leftrightarrow$ $I$ is $t$-invertible $\Rightarrow$ $I$ is $v$-invertible.

**Lemma 2.4.** *[48, Proposition 2.6] Let $*$ be a star operation of finite character on an integral domain $D$. Then $I \in \mathbf{F}(D)$ is $*$-invertible if and only if $I_* = J_*$ for some $J \in \mathbf{f}(D)$ and $ID_P$ is principal for all $P \in *$-Max$(D)$.*

Let $*_1$ and $*_2$ be star operations. Then $I_{*_1} \subseteq I_{*_2}$ if and only if $(I_{*_2})_{*_1} = (I_{*_1})_{*_2} = I_{*_2}$ for all $I \in \mathbf{F}(D)$. Hence, every $v$-ideal is a $*$-ideal for any star operation $*$ on $D$. The next result shows that a $*$-ideal is a $v$-ideal when it is $*$-invertible.

**Proposition 2.5.** (cf. [60, Theorem 1.1]) *Let $*_1$ and $*_2$ be star operations on an integral domain $D$ such that $I_{*_1} \subseteq I_{*_2}$ for all $I \in \mathbf{F}(D)$. Then a $*_1$-invertible $*_1$-ideal of $D$ is a $*_2$-invertible $v$-ideal.*

*Proof.* Let $I$ be a $*_1$-invertible $*_1$-ideal of $D$. Clearly, $I$ is $*_2$-invertible. Also, if $x \in I_v$, then $xI^{-1} \subseteq D$, and hence $x \in xD = x(II^{-1})_{*_1} \subseteq I_{*_1}$. Hence, $I_v \subseteq I_{*_1}$, and thus $I_v = I_{*_1} = I$.

We say that $D$ is a $*$-*Dedekind domain* if each nonzero ideal of $D$ is $*$-invertible. We also say that $D$ is a *Prüfer* $*$-*multiplication domain* (P$*$MD) if each nonzero finitely generated ideal of $D$ is $*_f$-invertible. An integral domain $D$ is a $v$-*domain* if each nonzero finitely generated ideal of $D$ is $v$-invertible. Clearly,

- $*$-Dedekind domain $\Rightarrow$ P$*$MD, and
- Dedekind domain $=$ $d$-Dedekind domain $\Rightarrow$ Prüfer domain $=$ P$d$MD $\Rightarrow$ P$*$MD $=$ P$*_f$MD $=$ P$*_w$MD $\Rightarrow$ P$v$MD $\Rightarrow$ $v$-domain.

**Proposition 2.6.** *Let $D$ be an integral domain.*

1. *$D$ is a $t$-Dedekind domain if and only if $D$ is a Krull domain.*
2. *$D$ is a $v$-Dedekind domain if and only if $D$ is completely integrally closed.*

*Proof.* (1) [49, Theorem 3.6]. (2) [39, Theorem 34.3].

A Bézout domain (resp., GCD domain) $D$ is an integral domain in which each nonzero finitely generated ideal (resp., $I_v$ for each $I \in \mathbf{f}(D)$) is principal. Hence, by Proposition 2.5,

- Bézout domain $=$ GCD domain $+$ Prüfer domain

and GCD domains are P$v$MDs.

## 2.3 *t-Class Group and Picard Group*

Let $T(D)$ (resp., $Inv(D)$, $Prin(D)$) be the group of $t$-invertible fractional $t$-ideals (resp., invertible fractional ideals, nonzero principal fractional ideals) of $D$ under the $t$-multiplication $I * J = (IJ)_t$. It is obvious that $Prin(D) \subseteq Inv(D) \subseteq T(D)$. The *$t$-class group* of $D$ is the abelian group $Cl(D) = T(D)/Prin(D)$ and the *Picard group* of $D$ is a subgroup $Pic(D) = Inv(D)/Prin(D)$ of $Cl(D)$. It is clear that if $D$ is a Krull domain, then $Cl(D)$ is the divisor class group of $D$. Also, if $D$ is a Prüfer domain or one-dimensional integral domain, then $Cl(D) = Pic(D)$.

**Proposition 2.7.** *Let $D$ be an integral domain.*

1. *If each maximal ideal of $D$ is a $t$-ideal, then $Cl(D) = Pic(D)$.*
2. *$D$ is a GCD domain if and only if $D$ is a P$v$MD with $Cl(D) = \{0\}$.*
3. *$D$ is a UFD if and only if $D$ is a Krull domain with $Cl(D) = \{0\}$.*

*Proof.* (1) Clear. (2) [13, Proposition 2]. (3) [35, Proposition 6.1].

It is well known that $D$ is a GCD domain (resp., UFD) if and only if $D[X]$, the polynomial ring over $D$, is a GCD domain (resp., UFD); so in this case, $Cl(D[X]) = Cl(D)$. The next result shows that $Cl(D)$ (resp., $Pic(D)$) is a subgroup of $Cl(D[X])$ (resp., $Pic(D[X])$).

**Lemma 2.8.** *Let $I$ be a nonzero fractional ideal of an integral domain $D$.*

1. $(ID[X])^{-1} = I^{-1}D[X]$.
2. $(ID[X])_v = I_vD[X]$.
3. $(ID[X])_t = I_tD[X]$.
4. $ID[X] \cap K = I$.

*Hence, $I$ is a (prime) $t$-ideal of $D$ (resp., invertible, $t$-invertible) if and only if $ID[X]$ is a (prime) $t$-ideal of $D[X]$ (resp., invertible, $t$-invertible). In particular, $Pic(D) \subseteq Pic(D[X])$ and $Cl(D) \subseteq Cl(D[X])$.*

*Proof.* (1), (2), and (3) [48, Proposition 2.2]. (4) Clear.

For a polynomial $f \in K[X]$, we denote by $c_D(f)$ (simply, $c(f)$) the fractional ideal of $D$ generated by the coefficients of $f$. For convenience, we mean by $c(f)_* = D$ that $f \neq 0$ and $c(f)_* = D$ for any star operation $*$ on $D$. Dedekind–Mertens lemma states that if $f, g \in K[X]$ are nonzero, then

$$c(f)^{m+1}c(g) = c(f)^m c(fg)$$

for $m = \deg(g)$ [39, Theorem 28.1]. In particular, if $c(f)$ is $*$-invertible, then $(c(f)c(g))_* = c(fg)_*$.

**Proposition 2.9.** *Let $D$ be an integral domain. Then the following statements are equivalent.*

1. *$D$ is integrally closed.*
2. $Cl(D) = Cl(D[X])$.
3. $fK[X] \cap D[X] = fc(f)^{-1}[X]$ *for all* $0 \neq f \in D[X]$.
4. $c(fg)_v = (c(f)c(g))_v$ *for all* $0 \neq f, g \in D[X]$.

*Proof.* (1) $\Leftrightarrow$ (2) [36, Theorem 3.6]. (1) $\Rightarrow$ (4) [39, Proposition 34.8]. (4) $\Rightarrow$ (3) This is true by the proof of [39, Corollary 34.9]. (3) $\Rightarrow$ (1) Let $a, b \in D$, $b \neq 0$ such that $x = \frac{a}{b}$ is integral over $D$. So if $f = bX - a$, then $Q_f := fK[X] \cap D[X] = f(a, b)^{-1}[X]$ by assumption. Thus, $x \in D$ [36, Lemma 3.5].

## 2.4 PvMDs, Nagata Rings, and Kronecker Function Rings

Let $X$ be an indeterminate over an integral domain $D$ and $D[X]$ be the polynomial ring over $D$. For a star operation $*$ on $D$, let $N_* = \{f \in D[X] \mid c(f)_* = D\}$; then $N_*$ is a saturated multiplicative set of $D[X]$ by Dedekind–Mertens lemma and $N_d \subseteq$

$N_* \subseteq N_v$. We call $D(X) := D[X]_{N_d}$ (resp., $D[X]_{N_*}$) the Nagata ring (resp., $*$-Nagata ring) of $D$.

**Proposition 2.10.** *1. $Max(D[X]_{N_*}) = \{P[X]_{N_*} \mid P \in *_f\text{-}Max(D)\}$.*
*2. $Pic(D[X]_{N_*}) = \{0\}$.*
*3. Each maximal ideal of $D[X]_{N_v}$ is a $t$-ideal, and hence*

$$Cl(D[X]_{N_v}) = Pic(D[X]_{N_v}) = \{0\}.$$

*Proof.* These results appear in Proposition 2.1, Theorem 2.14, and Proposition 2.2 of [48], respectively.

A star operation $*$ on $D$ is said to be *endlich arithmetisch brauchbar* (*e.a.b.*) if $(AB)^* \subseteq (AC)^*$ for all $A, B, C \in \mathbf{f}(D)$ implies $B^* \subseteq C^*$. It is well known that if $D$ admits an *e.a.b.* star operation, then $D$ is integrally closed [39, Corollary 32.8]. Conversely, if $D$ is integrally closed, then the star operation $b$ on $D$, defined by $I_b = \bigcap\{IV \mid V$ is a valuation overring of $D\}$, is an *e.a.b.* star operation of finite character and $b$-Max$(D) =$ Max$(D)$ [15, Lemma 3.1].

**Theorem 2.11.** ([39, Theorem 32.7]) *Let $D$ be an integral domain, $*$ be an e.a.b. star operation on $D$, $X$ be an indeterminate over $D$, and*

$$Kr(D,*) = \left\{\frac{f}{g} \mid f, g \in D[X], g \neq 0, \text{ and } c(f) \subseteq c(g)_*\right\}.$$

*1. $Kr(D,*)$ is a Bézout domain,*
*2. $Kr(D,*) \cap K = D$, and*
*3. $fKr(D,*) = c(f)Kr(D,*)$ and $fKr(D,*) \cap K = c(f)_*$ for all $0 \neq f \in D[X]$.*

*In this case, $Kr(D,*)$ is called the Kronecker function ring of $D$ with respect to $*$.*

Let $*$ be an *e.a.b.* star operation on $D$. It is clear that $D[X]_{N_*} \subseteq$ Kr$(D,*)$, and next in Corollary 2.13, we study when $D[X]_{N_*} =$ Kr$(D,*)$.

**Theorem 2.12.** *Let $*$ be a star operation on an integral domain $D$. Then the following statements are equivalent.*

*1. $D$ is a P$*$MD.*
*2. $*_w$ is an e.a.b. star operation.*
*3. $D[X]_{N_*}$ is a Prüfer domain.*
*4. Every ideal of $D[X]_{N_*}$ is extended from $D$.*
*5. $c(fg)_{*_w} = (c(f)c(g))_{*_w}$ for all $0 \neq f, g \in D[X]$.*
*6. $D_P$ is a valuation domain for all $P \in *_f\text{-}Max(D)$.*
*7. $D$ is a PvMD and $*_f = t$ on $D$.*

*Proof.* (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) [32, Theorem 3.1]. (1) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5) [15, Theorem 3.7]. (1) $\Leftrightarrow$ (6) [45, Theorem 1.1]. (1) $\Leftrightarrow$ (7) [32, Proposition 3.15].

Arnold showed that if $D$ is integrally closed, then $D$ is a Prüfer domain if and only if $\mathrm{Kr}(D, b) = D(X)$ [12, Theorem 4]. This was generalized to P$v$MDs by Gilmer as follows: If $D$ is a $v$-domain (equivalently, the $v$-operation on $D$ is $e.a.b.$), then $D$ is a P$v$MD if and only if $\mathrm{Kr}(D, v) = D[X]_{N_v}$ [38, Theorem 2.5].

**Corollary 2.13.** ([32, Theorem 3.1]) *Let $*$ be an $e.a.b$ star operation on an integral domain $D$. Then $D$ is a P$*$MD if and only if $D[X]_{N_*} = Kr(D, *)$.*

In [33], Fontana and Loper used an arbitrary star operation $*$ on an integral domain $D$ to define a Kronecker function ring $Kr(D, *)$ as follows.

**Lemma 2.14.** ([33, Theorem 5.1, Proposition 4.5(2), and Corollary 3.5]) *Let $*$ be a star operation on an integral domain D, and let $Kr(D, *) = \{\frac{f}{g} \mid f, g \in D[X], g \neq 0$, and $(c(f)c(h))_* \subseteq (c(g)c(h))_*$ for some $0 \neq h \in D[X]\}$. Then $Kr(D, *)$ is a Bézout domain with quotient field $K(X)$.*

For more on star operations, P$*$MDs, Nagata rings, and Kronecker function rings, the reader can refer to [15, 32, 34], [39, Sections 32 and 33], [48, 60].

## 3 UMT-domains

Let $D$ denote an integral domain with quotient field $K$, $\bar{D}$ be the integral closure of $D$ in $K$, $X$ be an indeterminate over $D$, $D[X]$ be the polynomial ring over $D$, and $N_v = \{f \in D[X] \mid c(f)_v = D\}$. In this section, we study several characterizations of UMT-domains (Section 3.1) and Kaplansky type theorems for uppers to zero in polynomial rings (Section 3.2).

### *3.1 UMT-domains*

Let $Q$ be a nonzero prime ideal of $D[X]$. We say that $Q$ is an *upper to zero* in $D[X]$ if $Q \cap D = (0)$. The next result gives some basic properties of uppers to zero in $D[X]$. For more on uppers to zero in polynomial rings, the reader can refer to Houston's survey article [44].

**Proposition 3.1.** *Let $Q$ be an upper to zero in $D[X]$.*

1. *$Q = fK[X] \cap D[X]$ for some nonzero irreducible polynomial $f \in K[X]$.*
2. *$htQ = 1$, and hence $Q$ is a prime $t$-ideal of $D[X]$.*
3. *The following statements are equivalent.*

   *(a)* *$Q$ is a maximal $t$-ideal of $D[X]$.*
   *(b)* *$Q$ is $t$-invertible.*
   *(c)* *$Q$ contains a nonzero polynomial $f \in D[X]$ with $c(f)_v = D$.*

4. *If $D$ is integrally closed, then $Q$ is a $v$-ideal.*

*Proof.* (1) By definition, $Q \cap D = (0)$, and hence $Q_{D\setminus\{0\}}$ is a nonzero prime ideal of $K[X]$. Note that $K[X]$ is a PID; so $Q_{D\setminus\{0\}} = fK[X]$ for some nonzero irreducible polynomial $f \in K[X]$. Thus, $Q = Q_{D\setminus\{0\}} \cap K[X] = fK[X] \cap D[X]$.

(2) $\text{ht}Q = \text{ht}(Q_{D\setminus\{0\}}) = \text{ht}(fK[X]) = 1$.

(3) [46, Theorem 1.4].

(4) By (1), $Q = fK[X] \cap D[X]$ for some $0 \neq f \in D[X]$, and since $D$ is integrally closed, $Q = fc(f)^{-1}[X]$ by Proposition 2.9. Thus, by Lemma 2.8, $Q_v = (fc(f)^{-1}[X])_v = f(c(f)^{-1})_v[X] = fc(f)^{-1}[X] = Q$.

The next corollary shows when an upper to zero in $D[X]$ is a maximal ideal, which can be proved by Proposition 3.1(2) with some other results.

**Corollary 3.2.** ([19, Corollary 5]) *Let $f = a_0 + a_1X + \cdots + a_nX^n \in D[X]$ be irreducible in $K[X]$ and $Q = fK[X] \cap D[X]$. Then $Q$ is a maximal ideal of $D[X]$ if and only if $(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}) \subseteq P$ for all nonzero prime ideals $P$ of $\bar{D}$. In this case, $fK[X] \cap \bar{D}[X] = \frac{1}{a_0}f\bar{D}[X]$.*

By Proposition 3.1, every upper to zero in $D[X]$ is a prime $t$-ideal. Following [46], we say that $D$ is a *UMT-domain* if each upper to zero in $D[X]$ is a maximal $t$-ideal of $D[X]$. (UMT stands for Upper to zero is a Maximal $T$-ideal.)

**Theorem 3.3.** ([46, Proposition 3.2]) *An integrally closed domain $D$ is a UMT-domain if and only if $D$ is a P$v$MD.*

Hence, UMT-domains can be considered as non-integrally closed P$v$MDs. A *quasi-Prüfer domain* is a UMT-domain in which every maximal ideal is a $t$-ideal; equivalently, its integral closure is a Prüfer domain [31, Chapter VI].

**Theorem 3.4.** *The following statements are equivalent for an integral domain $D$.*

1. *$D$ is a UMT-domain.*
2. *$\bar{D}_P$ is a Prüfer domain for all $P \in t$-Max$(D)$.*
3. *$\bar{D}_P$ is a Prüfer domain for all prime $t$-ideals $P$ of $D$.*
4. *$\bar{D}_P$ is a Bézout domain for all $P \in t$-Max$(D)$.*
5. *$\bar{D}_P$ is a Bézout domain for all prime $t$-ideals $P$ of $D$.*
6. *Each $t$-linked overring of $D$ is a UMT-domain.*

*Proof.* (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) [30, Theorem 1.5]. (1) $\Leftrightarrow$ (5) [16, Lemma 2.2]. (5) $\Rightarrow$ (4) $\Rightarrow$ (2) Clear. (1) $\Rightarrow$ (6) [30, Proposition 1.2]. (6) $\Rightarrow$ (1) Clear.

**Corollary 3.5.** ([30, Proposition 1.2]) *Let $D$ be a UMT-domain. Then $D_S$ is a UMT-domain for every multiplicative set $S$ of $D$.*

*Proof.* Let $I$ be a nonzero finitely generated ideal of $D$. Then $(ID_S)^{-1} = I^{-1}D_S$ [39, Theorem 4.4]. Hence, $D_S$ is $t$-linked over $D$. Thus, by Theorem 3.4, $D_S$ is a UMT-domain.

We next give some characterizations of UMT-domains via polynomial rings, Nagata rings, and Kronecker function rings.

**Theorem 3.6.** *The following statements are equivalent for an integral domain $D$.*

1. *$D$ is a UMT-domain.*
2. *$D[X]$ is a UMT-domain.*
3. *Each prime ideal of $D[X]_{N_v}$ is extended from $D$.*
4. *$D[X]_{N_v}$ is a quasi-Prüfer domain.*
5. *$\bar{D}[X]_{N_v}$ is a Prüfer domain.*
6. *$Kr(D, w) = \bar{D}[X]_{N_v}$, where $Kr(D, w)$ is as in Lemma 2.14.*
7. *Every upper to zero in $D[X]$ is $t$-invertible.*
8. *Each upper to zero in $D[X]$ contains an $0 \neq f \in D[X]$ with $c(f)_v = D$.*

*Proof.* (1) ⇔ (2) [30, Theorem 2.4]. (1) ⇔ (3) [46, Theorem 3.1]. (1) ⇔ (4) ⇔ (5) [23, Corollary 2.4 and Theorem 2.16]. (1) ⇔ (6) [17, Corollary 7]. (1) ⇔ (7) ⇔ (8) Proposition 3.1(3).

Let $D^{[w]} = \bigcap_{P \in t\text{-Max}(D)} \bar{D}_P$. Then $D^{[w]}$ is an integrally closed $t$-linked overring of $D$, $D^{[w]} = \bar{D}[X]_{N_v} \cap K$ and $D^{[w]}[X]_{N_v} = \bar{D}[X]_{N_v}$ [28, Theorem 1.3]. In particular, the $w_D$-operation on $D^{[w]}$ can be defined as in Lemma 2.3. It is easy to see that $A_{w_D} = A\bar{D}[X]_{N_v} \cap K$ for all $A \in \mathbf{F}(D^{[w]})$ [28, Lemma 2.3].

**Theorem 3.7.** *Let $D$ be an integral domain and $w_D$ be the star operation of finite character on $D^{[w]}$ as in Lemma 2.3. Then the following statements are equivalent.*

1. *$D$ is a UMT-domain.*
2. *$D^{[w]}$ is a P$w_D$MD.*
3. *$D^{[w]}$ is a PvMD and $t$-Max$(D^{[w]}) = \{Q \in Spec(D^{[w]}) \mid Q \cap D \in t\text{-}Max(D)\}$.*

*Proof.* (1) ⇔ (2) [58, Theorem 4.2]. (1) ⇔ (3) [28, Theorem 2.6].

For another characterization of UMT-domains, recall from [4] that a multiplicative subset $S$ of $D$ is a *$t$-splitting set* if for each $0 \neq d \in D, dD = (AB)_t$ for some integral ideals $A$ and $B$ of $D$, where $A_t \cap sD = sA_t$ (equivalently, $(A, s)_t = D$) for all $s \in S$ and $B_t \cap S \neq \emptyset$. It is known that $S$ is a $t$-splitting set of $D$ if and only if $dD_S \cap D$ is $t$-invertible for all $0 \neq d \in D$ [4, Corollary 2.3].

**Theorem 3.8.** ([22, Corollary 2.9]) *An integral domain $D$ is a UMT-domain if and only if $D \setminus \{0\}$ is a $t$-splitting set in $D[X]$.*

A strong Mori domain (SM domain) is an integral domain which satisfies the ascending chain condition on integral $w$-ideals. Clearly, Noetherian domains are SM domains, while SM domains need not be Noetherian (e.g., $\mathbb{Q}[\{X_\alpha\}]$ for an infinite set $\{X_\alpha\}$ of indeterminates over the field $\mathbb{Q}$ of rational numbers).

**Theorem 3.9.** ([28, Corollary 3.2]) *Let $D$ be an SM domain. Then $D$ is a UMT-domain if and only if $t$-dim$(D) = 1$.*

If $D$ is integrally closed, then each upper to zero in $D[X]$ is a $v$-ideal by Proposition 3.1(4). In [47], Houston and Zafrullah called $D$ a *UMV-domain* if each upper to zero in $D[X]$ is a maximal $v$-ideal. It is clear that if $D$ is a UMT-domain, then each upper to zero in $D[X]$ is a maximal $v$-ideal. Hence, UMT-domains are UMV-domains, while UMV-domains need not be UMT-domains (e.g., see [37, Example 3.1] for $v$-domains that are not P$v$MDs and [47, Example 3.5] for a non-integrally closed UMV-domain that is not a UMT-domain).

**Theorem 3.10.** ([47, Theorem 3.3]) *The following statements are equivalent for an integral domain $D$.*

1. *$D$ is a $v$-domain.*
2. *$D$ is an integrally closed UMV-domain.*
3. *$D$ is integrally closed and each upper to zero in $D[X]$ is $v$-invertible.*

Recall that $D$ is an *S-domain* if ht$(PD[X]) = 1$ for every prime ideal $P$ of $D$ with ht$P = 1$ [50, p. 26]. It is easy to see that a UMT-domain is an S-domain; and if $t$-dim$(D) = 1$ (e.g., dim$(D) = 1$), then $D$ is an S-domain if and only if $D$ is a UMT-domain (cf. [55, Theorem 8]). However, S-domains need not be UMT-domains. For example, if $D = \mathbb{R} + (X, Y)\mathbb{C}[\![X, Y]\!]$, where $\mathbb{C}[\![X, Y]\!]$ is the power series ring over the field $\mathbb{C}$ of complex numbers and $\mathbb{R}$ is the field of real numbers, then $D$ is a 2-dimensional local Noetherian domain [14, Theorem 4 and Corollary 9] whose maximal ideal is a $t$-ideal. Hence, $D$ is an S-domain [50, Theorem 148] but not a UMT-domain by Theorem 3.9. Moreover, it is clear that $D^{[w]} = \bar{D} = \mathbb{C}[\![X, Y]\!]$, and hence $D^{[w]}$ is a P$v$MD. Thus, in Theorem 3.7, $D^{[w]}$ being a P$v$MD does not imply that $D$ is a UMT-domain.

## 3.2 Kaplansky Type Theorems

It is well known that $D$ is a UFD if and only if every nonzero prime ideal of $D$ contains a nonzero prime element [50, Theorem 5]. Also, by Theorem 3.6 (resp., [23, Theorem 1.1]), we have

**Proposition 3.11.** *An integral domain $D$ is a UMT-domain (resp., quasi-Prüfer domain) if and only if every upper to zero in $D[X]$ contains a nonzero polynomial $f \in D[X]$ with $c(f)_v = D$ (resp., $c(f) = D$).*

In this subsection, we study this kind of theorem, called Kaplansky type theorem, for uppers to zero in $D[X]$. Note that, nonzero principal ideal ⇒ invertible ideal ⇒ $t$-invertible ideal; and prime ideal ⇒ primary ideal.

**Lemma 3.12.** *Let* $0 \neq f \in K[X]$ *and* $Q = fK[X] \cap D[X]$.

1. *Q is principal if and only if* $c(f)_v$ *is principal. In this case,* $Q = \frac{f}{a}D[X]$ *for some* $0 \neq a \in D$ *with* $c(f)_v = aD$.
2. *[57, Theorem A]* $f$ *is a prime element of* $D[X]$ *if and only if* $f$ *is irreducible over* $K$ *and* $c(f)_v = D$.

*Proof.* (1) If $Q = gD[X]$ for some $g \in D[X]$, then $fK[X] = gK[X]$, and hence $f = ag$ for some $0 \neq a \in D$ and $c(g)_v = D$ [10, Lemma 2.1]. Thus, $c(f)_v = aD$. Conversely, if $c(f)_v = bD$ for some $b \in D$, then $c(\frac{f}{b})_v = D$, and thus $Q = \frac{f}{b}D[X]$ by Dedekind–Mertens lemma.

(2) If $f$ is a prime element, then $fK[X]$ is a prime ideal and $fD[X] = fK[X] \cap D[X]$. Hence, $f$ is irreducible over $K$ and $c(f)_v = D$ by (1). The reverse implication follows directly from (1).

We next give a Kaplansky type characterization of GCD domains via uppers to zero in polynomial rings.

**Theorem 3.13.** ([57, Theorem I] and [24, Theorem 2.2]) *The following statements are equivalent for an integral domain D.*

1. *D is a GCD domain.*
2. *Each upper to zero in* $D[X]$ *contains a nonzero prime element.*
3. *Each upper to zero in* $D[X]$ *is principal.*
4. *Every* $(aX + b)K[X] \cap D[X]$ *for* $0 \neq a, b \in D$ *is principal.*

*Proof.* (1) ⇒ (3) Let $Q$ be an upper to zero in $D[X]$. Then $Q = fK[X] \cap D[X]$ for some $0 \neq f \in D[X]$, and since $c(f)_v$ is principal, $Q$ is principal by Lemma 3.12.

(2) ⇔ (3) ⇒ (4) Clear.

(4) ⇒ (1) Let $f = aX + b$. Then $f$ is irreducible in $K[X]$, and hence $fK[X] \cap D[X]$ is an upper to zero in $D[X]$. Hence, $fK[X] \cap D[X]$ is principal by assumption, and thus $(a, b)_v = c(f)_v$ is principal by Lemma 3.12. Thus, $D$ is a GCD domain.

**Corollary 3.14.** ([24, Corollary 2.3]) *An integral domain D is a Bézout domain if and only if each upper to zero in* $D[X]$ *contains a nonzero prime element* $f$ *with* $c(f) = D$.

A primary element of an integral domain $D$ is a nonzero nonunit $a \in D$ such that $a|bc$ for $b, c \in D$ implies either $a|b$ or $a|c^n$ for some integer $n \geq 1$; equivalently, $aD$ is a primary ideal. Clearly, a prime element is primary.

**Theorem 3.15.** ([10, Theorem 2.4]) *Each upper to zero in* $D[X]$ *contains a primary element if and only if D is a UMT-domain with* $Cl(D[X])$ *torsion.*

**Corollary 3.16.** ([24, Corollary 2.5]) *Each upper to zero in* $D[X]$ *contains a nonzero primary element* $f$ *with* $c(f) = D$ *if and only if D is a quasi-Prüfer domain with* $Cl(D[X])$ *torsion.*

*Proof.* (⇒) This follows directly from Proposition 3.11 and Theorem 3.15. (⇐) Note that a quasi-Prüfer domain is a UMT-domain. Hence, each upper to zero in $D[X]$ contains a primary element $f$ by Theorem 3.15. Then $c(f)_v = D$, and since each maximal ideal of $D$ is a $t$-ideal, $c(f) = D$.

We say that $D$ is an almost GCD domain (AGCD-domain) if, for each $0 \neq a, b \in D$, there is an integer $n = n(a, b) \geq 1$ such that $(a^n, b^n)_v$ is principal; equivalently, $a^n D \cap b^n D$ is principal. It is known that an integrally closed domain $D$ is an AGCD-domain if and only if $D$ is a P$v$MD with $Cl(D)$ torsion [59, Theorem 3.9].

**Corollary 3.17.** *Let D be an integrally closed domain.*

1. *[10, Corollary 2.5] Each upper to zero in $D[X]$ contains a primary element if and only if D is an AGCD-domain.*
2. *[24, Corollary 2.6] Each upper to zero in $D[X]$ contains a primary element $f$ with $c(f) = D$ if and only if D is a Prüfer domain with $Cl(D)$ torsion.*

An integral domain $D$ is called a generalized GCD domain (GGCD domain) if the intersection of two invertible ideals of $D$ is invertible [1]; equivalently, every $v$-ideal of finite type is invertible [1, Theorem 1]. Clearly, GGCD-domains are P$v$MDs because P$v$MDs are integral domains whose $v$-ideals of finite type are $t$-invertible and invertible ideals are $t$-invertible.

**Theorem 3.18.** ([6, Theorem 15]) *An integral domain D is a GGCD-domain if and only if each upper to zero in $D[X]$ is invertible.*

*Proof.* This can be proved by the fact that if $D$ is integrally closed, then $fK[X] \cap D[X] = fc(f)^{-1}[X]$ for all $0 \neq f \in D[X]$ by Proposition 2.9.

An integral domain $D$ is an almost GGCD-domain (AGGCD-domain) if for $0 \neq a, b \in D$, there is an integer $n = n(a, b) \geq 1$ such that $a^n D \cap b^n D$ (equivalently, $(a^n, b^n)_v$) is invertible. It is known that $D$ is an AGCD-domain if and only if $D$ is an AGGCD-domain with $Cl(D)$ torsion [51, Theorem 5.1].

**Theorem 3.19.** ([24, Theorem 2.8]) *Let D be an integrally closed domain.*

1. *Every upper to zero in $D[X]$ contains a $t$-invertible primary ideal if and only if D is a PvMD.*
2. *Every upper to zero in $D[X]$ contains an invertible primary ideal if and only if D is an AGGCD-domain.*

For another example of UMT-domains, recall that $D$ is called an almost P$v$MD (AP$v$MD) if, for each $0 \neq a, b \in D$, there exists an integer $n = n(a, b) \geq 1$ such that $(a^n, b^n)$ is $t$-invertible. Note that $(a^n, b^n)_v$ is $t$-invertible if and only if $(a^n, b^n)$ is $t$-invertible; so AGGCD domains are AP$v$MDs.

**Theorem 3.20.** *Let $D$ be an integral domain with integral closure $\bar{D}$.*

1. *$D$ is an AP$v$MD if and only if $D$ is a UMT-domain and $D \subseteq \bar{D}$ is a root extension, i.e., $a \in \bar{D}$ implies $a^n \in D$ for some integer $n = n(a) \geq 1$.*
2. *$D$ is an AGCD-domain if and only if $D$ is an AP$v$MD with $Cl(D)$ torison.*

*Proof.* These appear in Theorem 3.8 and Theorem 3.1 of [52], respectively.

In [56], Storch studied almost factorial domains which are Krull domains with torsion divisor class groups [35, Proposition 6.8]. Then, in [59], Zafrullah began to study a general theory of almost factoriality where he defined the notion of AGCD-domains. As we noted in this subsection, we have AGCD-domain $\Rightarrow$ AGGCD-domain $\Rightarrow$ AP$v$MD $\Rightarrow$ UMT-domain.

## 4 Graded Integral Domains Which Are UMT-domains

In this section, we study the UMT-domain property of graded integral domains. We first review the definitions related with graded integral domains.

### *4.1 Definitions of Graded Integral Domains*

Let $\Gamma$ be a nonzero torsionless grading monoid, that is, $\Gamma$ is a nonzero torsionless commutative cancellative monoid (written additively), and $\langle \Gamma \rangle = \{a - b \mid a, b \in \Gamma\}$ be the quotient group of $\Gamma$; so $\langle \Gamma \rangle$ is a torsionfree abelian group. It is well known that a cancellative monoid $\Gamma$ is torsionless if and only if $\Gamma$ can be given a total order compatible with the monoid operation [54, page 123]. By a ($\Gamma$-)graded integral domain $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$, we mean an integral domain graded by $\Gamma$. Hence, each nonzero $x \in R_\alpha$ has degree $\alpha$, i.e., $\deg(x) = \alpha$, $\deg(0) = 0$, and $R_\alpha R_\beta \subseteq R_{\alpha+\beta}$ for all $\alpha, \beta \in \Gamma$. Thus, each nonzero $f \in R$ can be written uniquely as $f = x_{\alpha_1} + \cdots + x_{\alpha_n}$ with $\deg(x_{\alpha_i}) = \alpha_i$ and $\alpha_1 < \cdots < \alpha_n$. A nonzero $x \in R_\alpha$ for every $\alpha \in \Gamma$ is said to be *homogeneous*. Let $H = \bigcup_{\alpha \in \Gamma}(R_\alpha \setminus \{0\})$; so $H$ is the saturated multiplicative set of nonzero homogeneous elements of $R$. Then $R_H$, called the *homogeneous quotient field* of $R$, is a $\langle \Gamma \rangle$-graded integral domain whose nonzero homogeneous elements are units. Hence, $R_H$ is a completely integrally closed GCD domain [3, Proposition 2.1]. For a fractional ideal $A$ of $R$ with $A \subseteq R_H$, let $A^h$ be the fractional ideal of $R$ generated by homogeneous elements in $A$; so $A^h \subseteq A$. The fractional ideal $A$ is said to be *homogeneous* if $A^h = A$. Let $C(f)$ denote the fractional ideal of $R$ generated by the homogeneous components of $f \in R_H$ and $C(A) = \sum_{f \in A} C(f)$ for a fractional ideal $A$ of $R$ with $A \subseteq R_H$. Clearly, $C(f)$ and $C(A)$ are homogeneous fractional ideals of $R$. It is known that if $f, g \in R$, then $C(f)^{m+1}C(g) = C(f)^m C(fg)$ for some integer $m \geq 1$ [54].

Examples of torsionless grading monoids include the additive monoids $\mathbb{Z}^+$ and $\mathbb{Q}^+$ of nonnegative integers and nonnegative rational numbers, respectively. Also, $\langle \mathbb{Z}^+ \rangle = \mathbb{Z}$ and $\langle \mathbb{Q}^+ \rangle = \mathbb{Q}$ are the additive groups of integers and rational numbers, respectively. It is clear that the semigroup ring $D[\Gamma]$ of $\Gamma$ over an integral domain $D$ is a $\Gamma$-graded integral domain with $\deg(aX^\alpha) = \alpha$ for $0 \neq a \in D$ and $\alpha \in \Gamma$. Also, the polynomial ring $D[X]$ and the Laurent polynomial ring $D[X, X^{-1}]$ are graded integral domains graded by $\mathbb{Z}^+$ and $\mathbb{Z}$, respectively.

Throughout this section, $\Gamma$ is always a nonzero torsionless grading monoid, $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ is a $\Gamma$-graded integral domain such that $R_\alpha \neq (0)$ for all $\alpha \in \Gamma$, $\bar{R}$ is the integral closure of $R$, $H$ is the saturated multiplicative set of nonzero homogeneous elements of $R$, and $N(H) = \{f \in R \mid f \neq 0 \text{ and } C(f)_v = R\}$; so $N(H)$ is a saturated multiplicative set of $R$.

## 4.2 General Case

Our first result shows why we are mainly interested in homogeneous maximal $t$-ideals when we study the divisibility properties (e.g., P$v$MDs and Krull domains) of graded integral domains.

**Lemma 4.1.** *Let $Q$ be a maximal $t$-ideal of $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$.*

1. *If $Q \cap H = \emptyset$, then $R_Q$ is a valuation domain. In particular, if $R_H$ is a UFD, then $R_Q$ is a rank-one DVR.*
2. *If $Q \cap H \neq \emptyset$, then $Q$ is homogeneous.*

*Hence, $\{Q \in t\text{-}Max(D) \mid Q \cap H \neq \emptyset\} = \{Q \in t\text{-}Max(D) \mid Q \text{ is homogeneous}\}$.*

*Proof.* (1) [27, Theorem 2]. (2) [9, Lemma 1.2].

The next result is a graded integral domain analog of Theorem 3.4.

**Theorem 4.2.** ([27, Corollary 7] and [43, Theorem 3.2]) *The following statements are equivalent for a graded integral domain $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$.*

1. *$R$ is a UMT-domain.*
2. *$\bar{R}_Q$ is a Prüfer domain for all homogeneous maximal $t$-ideals $Q$ of $R$.*
3. *$R_Q$ is a quasi-Prüfer domain for all homogeneous maximal $t$-ideals $Q$ of $R$.*
4. *$R_{N(H)}$ is a UMT-domain.*
5. *$R_{H \setminus Q}$ is a UMT-domain and $Q_{H \setminus Q}$ is a $t$-ideal for all homogeneous maximal $t$-ideals $Q$ of $R$.*

*Proof.* This result follows directly from Theorem 3.4, Lemma 4.1 and the fact that $Q_{N(H)}$ is a maximal $t$-ideal of $R_{N(H)}$ for all homogeneous maximal $t$-ideals $Q$ of $R$ [11, Proposition 1.3].

**Corollary 4.3.** ([25, Lemma 2.7] and [2, Theorem 6.4]) *Let $R = \bigoplus_{\alpha\in\Gamma} R_\alpha$ be a graded integral domain. Then the following statements are equivalent.*

1. *$R$ is a PvMD.*
2. *$R_Q$ is a valuation domain for all homogeneous maximal $t$-ideals $Q$ of $R$.*
3. *Every nonzero finitely generated homogeneous ideal of $R$ is $t$-invertible.*

*Proof.* (1) $\Rightarrow$ (3) Clear. (3) $\Rightarrow$ (2) This follows because $IR_Q$ is principal for all nonzero finitely generated homogeneous ideals $I$ of $R$. (2) $\Rightarrow$ (1) This is an immediate consequence of Theorem 2.12 and Lemma 4.1 (or Theorems 3.3 and 4.2).

As in [11], we say that $R$ satisfies property (#) if $C(I)_t = R$ implies $I \cap N(H) \neq \emptyset$ for all nonzero ideals $I$ of $R$; equivalently, $\mathrm{Max}(R_{N(H)}) = \{Q_{N(H)} \mid Q \in t\text{-}\mathrm{Max}(D)$ with $Q \cap H \neq \emptyset\}$ [11, Proposition 1.4]. Examples of graded integral domains with property (#) include (i) graded integral domains with a unit of nonzero degree, (ii) $D[\Gamma]$, the monoid domain of $\Gamma$ over an integral domain $D$, and (iii) $D[\{X_\alpha\}]$, the polynomial ring over $D$, [11, Example 1.6].

**Corollary 4.4.** ([27, Corollary 8]) *Let $R = \bigoplus_{\alpha\in\Gamma} R_\alpha$ be a graded integral domain with property* (#). *Then the following statements are equivalent.*

1. *$R$ is a UMT-domain.*
2. *$R_{N(H)}$ is a quasi-Prüfer domain.*
3. *$\bar{R}_{N(H)}$ is a Prüfer domain.*

Let $R = D[X, X^{-1}]$ be the Laurent polynomial ring over an integral domain $D$. Then $R$ is a $\mathbb{Z}$-graded integral domain and $R_{N(H)} = D[X]_{N_v}$. Hence, Corollary 4.4 is a natural generalization of Theorem 3.6 (1), (4), and (5).

## *4.3 When $R_H$ Is a UFD*

In this subsection, we study the UMT-domain property of graded integral domains $R = \bigoplus_{\alpha\in\Gamma} R_\alpha$ such that $R_H$ is a UFD; so throughout this subsection, we always assume that $R_H$ is a UFD. We first give some examples of graded integral domains $R$ with $R_H$ a UFD.

**Example 4.5.** Let $R = \bigoplus_{\alpha\in\Gamma} R_\alpha$ be a graded integral domain. Then $R_H$ is a UFD if one of the following conditions are satisfied:

1. [8, Proposition 3.5] $\langle\Gamma\rangle$ satisfies the ascending chain condition on its cyclic subgroups.
2. $R = D[\{X_\alpha\}]$ is the polynomial ring over an integral domain $D$.
3. [53, Section A.I.4.] $\langle\Gamma\rangle = \mathbb{Z}$ is the additive group of integers.

Let $R = D[X]$ be the polynomial ring over $D$. Then $Q$ is an upper to zero in $D[X]$ if and only if either $Q = XD[X]$ or $Q = fK[X, X^{-1}] \cap D[X]$ for some prime element $0 \neq f \in K[X]$. Also, $R_H = K[X, X^{-1}]$, and hence if $Q$ is an upper to zero in $D[X]$ with $Q \neq XD[X]$, then $Q = fR_H \cap R$. Motivated by this fact, Chang introduced the notion of graded UMT-domains. As we will see, the notions of UMT-domains and graded UMT-domains are distinct in general.

**Definition 4.6.** [21, Definition 1.4] Let $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ be a graded integral domain, and assume that $R_H$ is a UFD.

1. A nonzero prime ideal $Q$ of $R$ is an *upper to zero in* $R$ if $fR_H \cap R$ for some $f \in R_H$. (In this case, $f$ is a nonzero prime element of $R_H$.)
2. $R$ is a *graded UMT-domain* if every upper to zero in $R$ is a maximal $t$-ideal.

Clearly, $XD[X]$ is a maximal $t$-ideal of $D[X]$. Hence, $D$ is a UMT-domain if and only if $D[X]$ is a graded UMT-domain. However, if $D = \mathbb{R} + (y, z)\mathbb{C}[\![y, z]\!]$ (see the remark after Theorem 3.10), then $R = D + XK[X]$ is a graded UMT-domain with property (#) but not a UMT-domain ([20, Corollary 9] and [21, Proposition 4.2]).

**Theorem 4.7.** ([21, Proposition 1.7]) *Let $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ be a UMT-domain. Then $R$ is a graded UMT-domain.*

The next result is a graded integral domain analog of Proposition 3.1(3) which is very useful for the study of UMT-domain properties.

**Proposition 4.8.** *[21, Proposition 1.8] Let $Q$ be a prime $t$-ideal of $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ such that $Q \cap H = \emptyset$. Then the following statements are equivalent.*

*1. $C(Q)_t = R$.*
*2. $Q$ is $t$-invertible.*
*3. $Q$ is a maximal $t$-ideal.*

*In this case, ht$Q = 1$, and hence $Q$ is an upper to zero in $R$.*

Let $f \in D[X]$ be a nonzero polynomial with $c(f)_v = D$. If $A$ is an ideal of $D[X]$ with $f \in A$, then $A$ is $t$-invertible [46, Proposition 4.1] and $fD[X] = (Q_1^{e_1} \cdots Q_n^{e_n})_t$ for some uppers to zero $Q_i$ in $D[X]$ and integers $e_i \geq 1$ [41, p. 144]. The next result is an extension of these results to graded integral domains.

**Corollary 4.9.** (cf. [21, Proposition 1.12]) *Let $A$ be a nonzero ideal of $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ such that $C(A)_t = R$. Then $A_t = (Q_1^{e_1} \cdots Q_n^{e_n})_t$ for some $t$-invertible uppers to zero $Q_i$ in $R$ and integers $e_i \geq 1$. In particular, $A$ is $t$-invertible.*

*Proof.* Let $Q$ be a maximal $t$-ideal of $R$ with $A \subseteq Q$. Then $R = C(A)_t \subseteq C(Q)_t \subseteq R$ or $C(Q)_t = R$. Hence, $Q \cap H = \emptyset$ by Lemma 4.1, and thus $Q$ is an upper to zero in $R$ that is $t$-invertible by Proposition 4.8. This also implies that each prime $t$-ideal of $R$ containing $A$ is $t$-invertible. Thus, $A_t = (Q_1^{e_1} \cdots Q_n^{e_n})_t$ for some uppers to zero $Q_i$ in $R$ and integers $e_i \geq 1$ [41, Theorem 1.3] and $A$ is $t$-invertible.

**Corollary 4.10.** ([21, Corollary 1.13]) *Let* $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ *and* $0 \neq f \in R$ *with* $C(f)_v = R$. *Then* $fR = (Q_1^{e_1} \cdots Q_n^{e_n})_t$ *for some uppers to zero* $Q_i$ *in* $R$ *and integers* $e_i \geq 1$.

The next result gives a characterization of graded UMT-domains $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ with property (#). Note that if $R = D[X, X^{-1}]$, then $R$ satisfies property (#) and $R_{N(H)} = D[X]_{N_v}$; hence, the next result is an extension of Theorem 3.6 to graded integral domains with property (#).

**Theorem 4.11.** *Let* $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ *be a graded integral domain with property* (#). *Then the following statements are equivalent.*

1. *$R$ is a graded UMT-domain.*
2. *Every upper to zero in $R$ contains an $f \in R$ with $C(f)_v = R$.*
3. *Every prime ideal of $R_{N(H)}$ is extended from a homogeneous ideal of $R$.*
4. *Every upper to zero in $R$ is $t$-invertible.*

*Proof.* (1) ⇔ (2) ⇔ (3) [21, Theorem 2.2]. (2) ⇔ (4) Proposition 4.8.

We now give several characterizations of graded UMT-domains with a unit of nonzero degree, and in this case, graded UMT-domains are UMT-domains.

**Theorem 4.12.** *Let* $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ *be a graded integral domain with a unit of nonzero degree. Then the following statements are equivalent.*

1. *$R$ is a graded UMT-domain.*
2. *Every upper to zero in $R$ contains an $f \in Q$ with $C(f)_v = R$.*
3. *Every prime ideal of $R_{N(H)}$ is extended from a homogeneous ideal of $R$.*
4. *$R$ is a UMT-domain.*
5. *$\bar{R}_{N(H)}$ is a Prüfer domain.*
6. *$R_{N(H)}$ is a UMT-domain.*
7. *$R_{N(H)}$ is a quasi-Prüfer domain.*
8. *Every upper to zero in $R$ is $t$-invertible.*
9. *Let $Q$ be a nonzero prime ideal of $R$ with $C(Q)_t \subsetneq R$. Then $Q$ is a homogeneous prime $t$-ideal.*
10. *Let $Q$ be a nonzero prime ideal of $R$ such that $Q \subseteq M$ for some homogeneous maximal $t$-ideal $M$ of $R$. Then $Q$ is a homogeneous prime $t$-ideal.*

*Proof.* (1)−(7) [21, Theorem 3.5]. (1) ⇔ (8) Theorem 4.11 because graded integral domains with a unit of nonzero degree satisfy property (#). (1) ⇔ (9) ⇔ (10) [21, Corollary 3.10].

**Corollary 4.13.** ([26, Theorem 2.5]) *Let* $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ *be a graded integral domain with a unit of nonzero degree. Then $R$ is an integrally closed graded UMT-domain if and only if $R$ is a PvMD.*

Let $R = D[X]$ be the polynomial ring over $D$. Then, as we note after Definition 4.6, if $R$ is a graded UMT-domain, then $R$ is a UMT-domain even though $R$ does not contain a unit of nonzero degree. The next result explains why this phenominon happens.

**Corollary 4.14.** ([21, Corollary 3.13]) *Let $R = \bigoplus_{\alpha \in \Gamma} R_\alpha$ be a graded integral domain with a nonzero homogeneous prime element $p$ such that $ht(pR) = 1$ and $deg(p) \neq 0$. Then $R$ is a graded UMT-domain if and only if $R$ is a UMT-domain.*

*Proof.* Let $S = \{p^n \mid n \geq 1\}$. Then it is easy to see that $R$ is a (graded) UMT-domain if and only if $R_S$ is a (graded) UMT-domain. Thus, the result is an immediate consequence of Theorem 4.12.

# 5 Constructing New UMT-domains from Old Ones

In this section, we construct new UMT-domains from old UMT-domains via semigroup rings (Section 5.1) and pullbacks (Section 5.2).

## *5.1 Semigroup Rings*

Let $D$ be an integral domain, $\Gamma$ be a nonzero torsionless grading monoid, and $D[\Gamma]$ be the semigroup ring of $\Gamma$ over $R$. Then $D[\Gamma]$ is an integral domain [40, Theorem 8.1] graded by $\Gamma$ with $\deg(aX^\alpha) = \alpha$ for $0 \neq a \in D$ and $\alpha \in \Gamma$. We say that $\Gamma$ is a *valuation monoid* if either $g \in \Gamma$ or $-g \in \Gamma$ for every $g \in \langle \Gamma \rangle$. Clearly, $\mathbb{Z}^+$ and $\mathbb{Q}^+$ are valuation monoids.

**Lemma 5.1.** *Let $\Gamma$ be a torsionless grading monoid. Then the following statements are equivalent.*

1. *$\Gamma$ is a valuation monoid.*
2. *$\langle \Gamma \rangle = \Gamma \cup (-\Gamma)$.*
3. *$a + \Gamma \subseteq b + \Gamma$ or $b + \Gamma \subseteq a + \Gamma$ for every $a, b \in \Gamma$.*
4. *Every finitely generated ideal of $\Gamma$ is principal.*

*Proof.* This is an easy exercise.

Let $\bar{D}$ be the integral closure of $D$ and $\bar{\Gamma}$ be the integral closure of $\Gamma$. Then $\overline{D[\Gamma]} = \bar{D}[\bar{\Gamma}]$ [40, Theorem 12.10] and $\text{Max}(D[\Gamma]_{N(H)}) = \{P[X]_{N(H)} \mid P \in t\text{-Max}(D)\} \cup \{D[S]_{N(H)} \mid S \in t\text{-Max}(\Gamma)\}$ [11, Example 1.6].

**Theorem 5.2.** *The following statements are equivalent for $D[\Gamma]$.*

1. *$D[\Gamma]$ is a UMT-domain.*
2. *$D[\Gamma]_{N(H)}$ is a quasi-Prüfer domain.*
3. *$\overline{D}[\overline{\Gamma}]_{N(H)}$ is a Prüfer domain.*
4. *$D$ is a UMT-domain and $\bar{\Gamma}_S$ is a valuation monoid for all maximal $t$-ideals $S$ of $\Gamma$.*
5. *$D[\Gamma]_Q$ is a quasi-Prüfer domain for all maximal $t$-ideals $Q$ of $D[\Gamma]$ with $Q \cap D \neq (0)$ or $X^\alpha \in Q$ for some $\alpha \in \Gamma$.*

*Proof.* (1) ⇔ (2) ⇔ (3) ⇔ (4) [27, Theorem 17]. (1) ⇔ (5) Note that $Q$ is a homogeneous maximal $t$-ideal of $D[\Gamma]$ if and only if either $Q \cap D \neq (0)$ or $X^\alpha \in Q$ for some $\alpha \in \Gamma$. Thus, the result follows from Theorem 4.2.

**Corollary 5.3.** ([27, Corollary 18]) *Let $G$ be a torsionfree abelian group. Then $D[G]$ is a UMT-domain if and only if $D$ is a UMT-domain.*

*Proof.* Clearly, $G$ has no maximal $t$-ideal. Thus, the result follows directly from Theorem 5.2.

**Corollary 5.4.** ([27, Corollary 18]) *Let $\Gamma$ be a numerical semigroup. Then $D[\Gamma]$ is a UMT-domain if and only if $D$ is a UMT-domain.*

*Proof.* Clearly, $\bar{\Gamma} = \mathbb{Z}^+$ is a valuation monoid. Thus, the result follows directly from Theorem 5.2.

**Corollary 5.5.** ([30, Theorems 2.4 and 2.5] and [21, Corollary 3.14]) *Let $\{X_\alpha\}$ be a nonempty set of indeterminates over $D$ and $N_v = \{f \in D[\{X_\alpha\}] \mid c(f)_v = D\}$. Then the following statements are equivalent.*

1. *$D$ is a UMT-domain.*
2. *$D[\{X_\alpha\}]$ is a UMT-domain.*
3. *$D[\{X_\alpha, X_\alpha^{-1}\}]$ is a UMT-domain.*
4. *$D[\{X_\alpha\}]_{N_v}$ is a UMT-domain.*
5. *$D[\{X_\alpha\}]_{N_v}$ is a quasi-Prüfer domain.*

*Proof.* For each $\alpha$, let $\mathbb{Z}_\alpha = \mathbb{Z}$ be the additive group of integers; so if $G = \bigoplus_\alpha \mathbb{Z}_\alpha$, then $G$ is a torsionfree abelian group and the group ring $D[G]$ of $G$ over $D$ is isomorphic to $D[\{X_\alpha, X_\alpha^{-1}\}]$. Hence, the result follows from Theorem 5.2.

## 5.2 Pullbacks

Let $T$ be an integral domain, $M$ be a maximal ideal of $T$, $k = T/M$, $D$ be a subring of $k$, $\varphi : T \to k$ be the canonical homomorphism, and $R = \varphi^{-1}(D)$ be the pullback of the following diagram:

$$\begin{array}{ccc} R = \varphi^{-1}(D) & \longrightarrow & D \\ \downarrow & & \downarrow \\ T & \xrightarrow{\ \varphi\ } & k = T/M. \end{array}$$

Then $T$ is a $t$-linked overring of $R$ [30, Proposition 3.1] and $M$ is a prime $t$-ideal of $R$. Hence, by Theorem 3.4, if $R$ is a UMT-domain, then $T$ is a UMT-domain. We call $R$ a pullback of type $(\star)$. For example, if $T$ is a valuation domain with maximal ideal $M$ such that $T = k + M$ (e.g., $T = k[\![X]\!]$ is the power series ring over $k$), then $R = D + M$.

**Theorem 5.6.** ([30, Theorem 3.7]) *Let $R$ be a pullback of type ($\star$). Then $R$ is a UMT-domain if and only if $D$ and $T$ are UMT-domains, $M$ is a maximal $t$-ideal of $T$, and $k$ is algebraic over the quotient field of $D$.*

**Corollary 5.7.** *Let $D$ be an integral domain with quotient field $K$, $k$ be an algebraic extension field of $K$, and $X$ be an indeterminate over $k$. Then the following statements are equivalent.*

1. *$D$ is a UMT-domain.*
2. *$D + X^n k[X]$ is a UMT-domain for all integers $n \geq 1$.*
3. *$D + X^n k[\![X]\!]$ is a UMT-domain for all integers $n \geq 1$.*

*Proof.* (1) $\Leftrightarrow$ (2) Clearly, $k[X]$ is a UMT-domain, and hence $k[S]$ for $S = \{0, n, n+1, \dots\}$ is a UMT-domain (by Corollary 5.4) and $X^n k[X]$ is a maximal $t$-ideal of $k[S]$. Thus, the results follow from Theorem 5.6.

(1) $\Leftrightarrow$ (3) Let $T = k[\![X^n, X^{n+1}, \cdots]\!]$. Then $\bar{T} = k[\![X]\!]$ is a rank-one DVR. Hence, $T$ is a quasi-Prüfer domain and $X^n k[\![X]\!]$ is a maximal $t$-ideal of $T$. Thus, by Theorem 5.6, $D$ is a UMT-domain if and only if $D + X^n k[\![X]\!]$ is a UMT-domain.

**Corollary 5.8.** *Let $D$ be an integral domain with quotient field $K$, $k$ be an algebraic extension field of $K$, $k[\mathbb{Q}^+]$ be the semigroup ring of $\mathbb{Q}^+$ over $k$, and $M = \{g \in k[\mathbb{Q}^+] \mid g(0) = 0\}$. Then $D$ is a UMT-domain if and only if $D + M$ is a UMT-domain.*

*Proof.* Note that $k[\mathbb{Q}^+]$ is a P$v$MD by Corollary 4.3 and $M$ is a maximal $t$-ideal of $k[\mathbb{Q}^+]$ (cf. Lemma 4.1). Thus, the result follows directly from Theorem 5.6.

**Acknowledgements** This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2017R1D1A1B06029867).

## References

1. Anderson, D.D., Anderson, D.F.: Generalized GCD domains. Comment. Math. Univ. St. Pauli **28**, 215–221 (1979)
2. Anderson, D.D., Anderson, D.F.: Divisorial ideals and invertible ideals in a graded integral domain. J. Algebra **76**, 549–569 (1982)
3. Anderson, D.D., Anderson, D.F.: Divisibility properties of graded domains. Canad. J. Math. **34**, 196–215 (1982)
4. Anderson, D.D., Anderson, D.F., Zafrullah M.: The ring $D + XD_S[X]$ and $t$-splitting sets, Commutative Algebra. Arab. J. Sci. Eng. Sect. C (26), 3–16 (2001)
5. Anderson, D.D., Cook, S.J.: Two star-operations and their induced lattices. Comm. Algebra **28**, 2461–2475 (2000)
6. Anderson, D.D., Dumitrescu, T., Zafrullah, M.: Quasi-Schreier domains, II. Comm. Algebra **35**, 2096–2104 (2007)

7. Anderson, D.D., Houston, E., Zafrullah, M.: $t$-linked extensions, the t-class group, and Nagata's theorem. J. Pure Appl. Algebra **86**, 109–124 (1993)
8. Anderson, D.F.: Graded Krull domains. Comm. Algebra **7**, 79–106 (1979)
9. Anderson, D.F., Chang, G.W.: Homogeneous splitting sets of a graded integral domain. J. Algebra **288**, 527–544 (2005)
10. Anderson, D.F., Chang, G.W.: Almost splitting sets in integral domains, II. J. Pure Appl. Algebra **208**, 351–359 (2007)
11. Anderson, D.F., Chang, G.W.: Graded integral domains and Nagata rings. J. Algebra **387**, 169–184 (2013)
12. Arnold, J.T.: On the ideal theory of the Kronecker function ring and the domain $D(X)$. Canad. J. Math. **21**, 558–563 (1969)
13. Bouvier, A.: Le groupe des classes d'un anneaux integre, 107 eme Congres des Societes Savantes, Brest fasc. IV 85–92 (1982)
14. Brewer, J., Rutter, E.: $D + M$ constructions with general overrings. Michigan Math. J. **23**, 33–42 (1976)
15. Chang, G.W.: Prüfer $*$-multiplication domains, Nagata rings, and Kronecker function rings. J. Algebra **319**, 309–319 (2008)
16. Chang, G.W.: Locally pseudo-valuation domains of the form $D[X]_{N_v}$. J. Korean Math. Soc. **45**, 1405–1416 (2008)
17. Chang, G.W.: Kronecker function rings and Prüfer-like domains. Korean J. Math. **20**, 371–379 (2012)
18. Chang, G.W.: The $A + XB[X]$ construction from Prüfer $v$-multiplication domains. J. Algebra **439**, 417–437 (2015)
19. Chang, G.W.: Uppers to zero in polynomial rings which are maximal ideals. Bull. Korean Math. Soc. **52**, 525–530 (2015)
20. Chang, G.W.: Graded integral domains and Nagata rings II. Korean J. Math. **25**, 215–227 (2017)
21. Chang, G.W.: Graded integral domains and Prüfer-like domains. J. Korean Math. Soc. **54**, 1733–1757 (2017)
22. Chang, G.W., Dumitrescu, T., Zafrullah, M.: $t$-Splitting sets in integral domains. J. Pure Appl. Algebra **187**, 71–86 (2004)
23. Chang, G.W., Fontana, M.: Uppers to zero in polynomial rings and Prüfer-like domains. Comm. Algebra **37**, 164–192 (2009)
24. Chang, G.W., Kim, H.: Kaplansky-type theorems II. Kyungpook Math. J. **51**, 339–344 (2011)
25. Chang, G.W., Kang, B.G., Lim, J.W.: Prüfer $v$-multiplication domains and related domains of the form $D + D_S[\Gamma^*]$. J. Algebra **323**, 3124–3133 (2010)
26. Chang, G.W., Kim, H., Oh, D.Y.: Kaplansky-type theorems in graded integral domains. Bull. Korean Math. Soc. **52**, 1253–1268 (2015)
27. Chang, G.W., Sahandi, P.: Graded integral domains which are UMT-domains. Comm. Algebra **46**, 2742–2752 (2018)
28. Chang, G.W., Zafrullah, M.: The $w$-integral closure of integral domains. J. Algebra **295**, 195–210 (2006)
29. Dobbs, D., Houston, E., Lucas, T., Zafrullah, M.: $t$-linked overrings and PVMDs. Comm. Algebra **17**, 2835–2852 (1989)
30. Fontana, M., Gabelli, S., Houston, E.: UMT-domains and domains with Prüfer integral closure. Comm. Algebra **25**, 1017–1039 (1998)
31. Fontana, M., Huckaba, J., Papick, I.: Prüfer Domains. Marcel Dekker, New York (1997)
32. Fontana, M., Jara, P., Santos, E.: Prüfer $*$-multiplication domains and semistar operations. J. Algebra Appl. **2**, 1–30 (2003)
33. Fontana, M., Loper, K.A.: Kronecker function rings: a general approach. In: Ideal Theoretic Methods in Commutative Algebra, Lecture Notes in Pure and Applied Mathematics vol. 220, pp. 189-205. Marcel Dekker (2001)

34. Fontana, M., Loper, K.A.: A historical overview of Kronecker function rings, Nagata rings, and related star and semistar operations. In: Brewer, J.W., Glaz, S., Heinzer, W.J., Olberding, B.M. (eds.) Multiplicative Ideal Theory in Commutative Algebra, pp. 169–187. Springer, A Tribute to the Work of Robert Gilmer (2006)
35. Fossum, R.: The Divisor Class Group of a Krull Domain. Springer, New York/Berlin (1973)
36. Gabelli, S.: On divisorial ideals in polynomial rings over Mori domains. Comm. Algebra **15**, 2349–2370 (1987)
37. Gabelli, S., Roitman, M.: Maximal divisorial ideals and $t$-maximal ideals. JPJ. Algebra Number Theory Appl. **4**, 323–336 (2004)
38. Gilmer, R.: An embedding theorem for HCF-rings. Proc. Cambridge Philos. Soc. **68**, 583–587 (1970)
39. Gilmer, R.: Multiplicative Ideal Theory. Marcel Dekker, New York (1972)
40. Gilmer, R.: Commutative Semigroup Rings. Univ. of Chicago Press, Chicago (1984)
41. Gilmer, R., Mott, J., Zafrullah, M.: $t$-invertibility and comparability. In: Commutative Ring Theory. Lecture Notes in Pure and Applied Mathematics, vol. 153, pp. 141–150. Marcel Dekker, New York (1994)
42. Griffin, M.: Some results on $v$-multiplication rings. Canad. J. Math. **19**, 7l0–722 (1967)
43. Hamdi, H., Sahandi, P.: Uppers to zero in polynomial rings over graded domains and UM$t$-domains. Bull. Korean Math. Soc. **55**, 187–204 (2018)
44. Houston, E.: Uppers to zero in polynomial rings. In: Brewer, J.W., Glaz, S., Heinzer, W.J., Olberding, B.M. (eds.) Multiplicative Ideal Theory in Commutative Algebra, pp. 243–261. Springer, A Tribute to the Work of Robert Gilmer (2006)
45. Houston, E., Malik, S., Mott, J.: Characterizations of $*$-multiplication domains. Canad. Math. Bull. **27**, 48–52 (1984)
46. Houston, E., Zafrullah, M.: On $t$-invertibility II. Comm. Algebra **17**, 1955–1969 (1989)
47. Houston, E., Zafrullah, M.: UMV-domains. In: Arithmetical Properties of Commutative Rings and Monoids, Lecture Notes in Pure and Applied Mathematics, vol. 241, pp. 304-315. Chapman & Hall/CRC, New York (2005)
48. Kang, B.G.: Prüfer $v$-multiplication domains and the ring $R[X]_{N_v}$. J. Algebra **123**, 151–170 (1989)
49. Kang, B.G.: On the converse of a well-known fact about Krull domains. J. Algebra **124**, 284–299 (1989)
50. Kaplansky, I.: Commutative Rings, revised edn. University of Chicago, Chicago (1974)
51. Lewin, R.L.: Almost generalized GCD-domains, In: Andeson, D.D. (eds.) Factorization in Integral Domains. Lecture Notes in Pure and Applied Mathematics, vol. 189, New York, Basel, pp. 371–382. Marcel Dekker, Hong Kong (1997)
52. Li, Q.: On almost Prüfer $v$-multiplication domains. Algebra Colloq. **19**, 493–500 (2012)
53. Năstăsescu, C., Van Oystaeyen, F.: Graded Ring Theory, Library of Math, vol. 28. North Holland, Amsterdam (1982)
54. Northcott, D.G.: Lessons on Rings, Modules, and Multiplicities. Cambridge University Press, Cambridge (1968)
55. Seidenberg, A.: A note on the dimension theory of rings. Pacific J. Math. **3**, 505–512 (1953)
56. Storch, U.: Fastfaktorielle ringe, Schriftenreihe Math. Inst. Univ. Münster, Heft 36 (1967)
57. Tang, H.T.: Gauss' lemma. Proc. Amer. Math. Soc. **35**, 372–376 (1972)
58. Wang, F.: On induced operations and UMT-domains. Sichuan Shifan Daxue Xuebao Ziran Kexue Ban **27**, 1–9 (2004)
59. Zafrullah, M.: A general theory of almost factoriality. Manuscripta Math. **51**, 29–62 (1985)
60. Zafrullah, M.: Putting $t$-invertibility to use, Non-Noetherian commutative ring theory, vol. 520, pp. 429–457, Math. Appl., Kluwer Academic Publishers, Dordrecht (2000)

# The Apéry Set of a Good Semigroup

**Marco D'Anna, Lorenzo Guerrieri, and Vincenzo Micale**

**Abstract** We study the Apéry Set of good subsemigroups of $\mathbb{N}^2$, a class of semigroups containing the value semigroups of curve singularities with two branches. Even if this set in infinite, we show that, for the Apéry Set of such semigroups, we can define a partition in "levels" that allows to generalize many properties of the Apéry Set of numerical semigroups, i.e., value semigroups of one-branch singularities.

**Keywords** Value semigroups · Algebroid curves · Gorenstein rings · Symmetric semigroups · Apéry Set

**MSC** 13A18 · 14H99 · 13H99 · 20M25

## 1 Introduction

The concept of *good semigroup* was formally defined in [1] in order to study value semigroups of Noetherian analytically unramified one-dimensional semilocal reduced rings, e.g., the local rings arising from curve singularities (and from their blowups), possibly with more than one branch; the properties of these semigroups were already considered in [3, 5, 6, 9, 13–15], but it was in [1] that their structure was systematically studied. Similarly to the one-branch case, when the value semigroup is a numerical semigroup, the properties of the rings can be translated and studied at semigroup level. For example, the celebrated result by Kunz (see [18]) that a one-dimensional analytically irreducible local domain is Gorenstein if and only if

M. D'Anna (✉) · L. Guerrieri · V. Micale
Università di Catania, Viale Andrea Doria 6, 95125 Catania, Italy
e-mail: mdanna@dmi.unict.it

L. Guerrieri
e-mail: guelor@guelan.com

V. Micale
e-mail: vmicale@dmi.unict.it



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_4

its value semigroup is symmetric can be generalized to analytically unramified rings (see [14] and also [6]); in the same way, the numerical characterization of the canonical module in the analytically irreducible case (see [16]) can be given also in the more general case (see [9]).

However good semigroups present some problems that make difficult their study; first of all they are not finitely generated as monoid (even if they can be completely determined by a finite set of elements (see [7, 10, 15])) and they are not closed under finite intersections. Secondly, the behavior of the good ideals of good semigroups (e.g., the ideals arising as values of ideals of the corresponding ring) is not good at all, in the sense that the class of good ideals is not closed under sums and differences (see, e.g., [1, 17]).

Hence, unlike what happens for numerical semigroups (in analogy to analytically irreducible domains), it is not clear how to define the concept of complete intersection good semigroups and also the concepts of embedding dimension and type for these semigroups.

Moreover, in the same paper [1], it is shown that the class of good semigroups is larger than the class of value semigroups and, at the moment, no characterization of value good semigroups is known (while, for the numerical semigroup case, it is easily seen that any such semigroup is the value semigroup of the ring of the corresponding monomial curve). This means that to prove a property for good semigroups it is not possible to take advantage of the nature of value semigroups and it is necessary to work only at semigroup level.

Despite this bad facts, there is a concept quite natural to define that seems very promising in order to study good semigroups and to translate at numerical level other ring concepts: the *Apéry Set*. In general, given any monoid $S$ and any element $s \in S$, the $\mathbf{Ap}(S, s)$ is defined as the set $\{t \in S : \ t - s \notin S\}$ (where the $-$ is taken in the group generated by $S$). For studying numerical semigroups, this concept reveals to be very useful and it is also a bridge between semigroup and ring properties, since many important ring properties are stable under quotients with respect to principal ideals generated by a nonzero divisor $(x)$ and the values of the nonzero elements in $R/(x)$ are exactly the elements of $\mathbf{Ap}(S, v(x))$. This strategy was used, e.g., in [4, 8, 11, 12] taking $(x)$ to be a minimal reduction of the maximal ideal that, in this situation, corresponds to an element of minimal nonzero value.

For good semigroups, the notion of $\mathbf{Ap}(S, s)$ was used in [2], in order to obtain an algorithmic characterization of those good semigroups that are value semigroups of a plane singularity with two branches. In that paper, using deeply the structure of the rings associated to plane singularities, it is proved that $\mathbf{Ap}(S, \boldsymbol{e})$ (where $\boldsymbol{e} = (e_1, e_2)$ is the minimal nonzero element in $S \subset \mathbb{N}^2$) can be divided in $e = e_1 + e_2$ subsets, where the integer $e$ corresponds to the multiplicity of the ring.

In this paper we want to investigate the Apéry Set of a good semigroup. Again the problem is that we have to deal with an infinite set; so, first of all, we want to understand if there is a natural partition of it in $e$ subsets, where $e$ is the sum of the components of the minimal nonzero element of $S$ and, in case $S$ is a value semigroup, it represents also the multiplicity of the corresponding ring; to answer to this question we decided to restrict to the good subsemigroups of $\mathbb{N}^2$, otherwise the technicalities would increase too much. After finding a possible partition $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$, we prove that, if $S$ is the value semigroup of a ring $(R, \mathfrak{m}, k)$, it is possible to choose $e$ elements $\boldsymbol{\alpha}_i$ in the Apéry Set, one for each $A_i$, so that, taking any element $f_i \in R$ of valuation $v(f_i) = \boldsymbol{\alpha}_i$, the classes $\bar{f_i}$ are a basis of the $e$-dimensional $k$-vector space $R/(x)$ (where $x$ is a minimal reduction of $\mathfrak{m}$). This fact make us confident that the definition of the partition is the one we where looking for.

At this point it is natural to investigate if it is possible to generalize the well-known characterization of symmetric numerical semigroups given via their Apéry Set. It turns out that also good symmetric semigroups have $\mathbf{Ap}(S, \boldsymbol{e})$ whose partition satisfies a duality property similar to the duality that holds for the numerical case.

The structure of the paper is the following: after recalling in Section 2 all the preliminary definitions and results needed for the rest of the paper, in Section 3 we define the partition of the Apéry Set of $S$ and we prove that this partition produces exactly $e_1 + e_2$ levels (Theorem 3); successively we deepen the study of the structure of Apéry Set (Theorem 5) and we prove that, in the case of value semigroups, the partition allows to find a basis for $R/(x)$ as explained above (Theorem 6).

In Section 4 we study the properties of the Apéry Set of symmetric good semigroups with particular attention to duality properties of its elements (Proposition 7 and Theorem 8) and in Section 5 we use these results to prove a duality for the levels, characterizing the symmetric semigroups, in analogy to the duality of Apéry Set in the numerical semigroup case (Theorem 9). Finally we deepen this duality showing that we can find sequences of elements, one for each level, that have the same duality properties of the Apéry Set of the numerical semigroups (Theorem 10).

## 2 Preliminaries

Let $\mathbb{N}$ be the set of nonnegative integers. As usual, $\leq$ stands for the natural partial ordering in $\mathbb{N}^2$: set $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$, $\boldsymbol{\beta} = (\beta_1, \beta_2)$, then $\boldsymbol{\alpha} \leq \boldsymbol{\beta}$ if $\alpha_1 \leq \beta_1$ and $\alpha_2 \leq \beta_2$. Trough this paper, if not differently specified, when referring to minimal or maximal elements of a subset of $\mathbb{N}^2$, we refer to minimal or maximal elements with respect to $\leq$. Given $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^2$, the infimum of the set $\{\boldsymbol{\alpha}, \boldsymbol{\beta}\}$ (with respect to $\leq$) will be denoted by $\boldsymbol{\alpha} \wedge \boldsymbol{\beta}$. Hence

$$\boldsymbol{\alpha} \wedge \boldsymbol{\beta} = (\min(\alpha_1, \beta_1), \min(\alpha_2, \beta_2)).$$

Let $S$ be a submonoid of $(\mathbb{N}^2, +)$. We say that $S$ is a *good semigroup* if

(G1) for all $\boldsymbol{\alpha}, \boldsymbol{\beta} \in S$, $\boldsymbol{\alpha} \wedge \boldsymbol{\beta} \in S$;
(G2) if $\boldsymbol{\alpha}, \boldsymbol{\beta} \in S$ and $\alpha_i = \beta_i$ for some $i \in \{1, 2\}$, then there exists $\boldsymbol{\delta} \in S$ such that $\delta_i > \alpha_i = \beta_i$, $\delta_j \geq \min\{\alpha_j, \beta_j\}$ for $j \in \{1, 2\} \setminus \{i\}$ and $\delta_j = \min\{\alpha_j, \beta_j\}$ if $\alpha_j \neq \beta_j$;
(G3) there exists $\boldsymbol{c} \in S$ such that $\boldsymbol{c} + \mathbb{N}^2 \subseteq S$.

A good subsemigroup of $\mathbb{N}^2$ is said to be *local* if $\mathbf{0} = (0, 0)$ is its only element with a zero component. In the following we will work only with local good semigroups hence we will omit the word local.

Notice that, from condition (G1), if $\boldsymbol{c}$ and $\boldsymbol{d}$ fulfill (G3), then so does $\boldsymbol{c} \wedge \boldsymbol{d}$. So there exists a minimum $\boldsymbol{c} \in \mathbb{N}^2$ for which condition (G3) holds. Therefore we will say that

$$\boldsymbol{c} := \min\{\boldsymbol{\alpha} \in \mathbb{Z}^2 \mid \boldsymbol{\alpha} + \mathbb{N}^2 \subseteq S\}$$

is the *conductor* of $S$. We denote $\boldsymbol{\gamma} := \boldsymbol{c} - \mathbf{1}$.

In light of [1, Proposition 2.1], value semigroups of Noetherian, analytically unramified, residually rational, one-dimensional, reduced semilocal rings with two minimal primes are good subsemigroups of $\mathbb{N}^2$ and $R$ is local if and only it its value semigroup is local; in the rest of this paper, we will always assume these hypotheses on the rings $R$ unless differently stated.

We give the following technical definitions that are commonly used in the literature about good semigroups:

(1) $\Delta_i(\boldsymbol{\alpha}) := \{\boldsymbol{\beta} \in \mathbb{Z}^2 \mid \alpha_i = \beta_i \text{ and } \alpha_j < \beta_j \text{ for } j \neq i\}$,
(2) $\Delta_i^S(\boldsymbol{\alpha}) := \Delta_i(\boldsymbol{\alpha}) \cap S$,
(3) $\Delta(\boldsymbol{\alpha}) := \Delta_1(\boldsymbol{\alpha}) \cup \Delta_2(\boldsymbol{\alpha})$,
(4) $\Delta^S(\boldsymbol{\alpha}) := \Delta(\boldsymbol{\alpha}) \cap S$.

An element $\boldsymbol{\alpha} \in S$ is said to be *absolute* if $\Delta^S(\boldsymbol{\alpha}) = \emptyset$. By definition of conductor we immediately get $\Delta^S(\boldsymbol{\gamma}) = \emptyset$. Given $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^2$, we say that $\boldsymbol{\beta}$ is *above* $\boldsymbol{\alpha}$ if $\boldsymbol{\beta} \in \Delta_1(\boldsymbol{\alpha})$ and that $\boldsymbol{\beta}$ is *on the right* of $\boldsymbol{\alpha}$ if $\boldsymbol{\beta} \in \Delta_2(\boldsymbol{\alpha})$.

*Remark 1.* Let $\boldsymbol{c} = (c_1, c_2)$ be the conductor of $S$. By properties (G1) and (G2), we have that if $\boldsymbol{\alpha} = (\alpha_1, c_2) \in S$, then $\Delta_1(\boldsymbol{\alpha}) = \Delta_1^S(\boldsymbol{\alpha})$ (that is, each point $\boldsymbol{\beta} \in \mathbb{N}^2$, above $\boldsymbol{\alpha}$, is in $S$). Similarly, if $\boldsymbol{\alpha} = (c_1, \alpha_2) \in S$, then $\Delta_2(\boldsymbol{\alpha}) = \Delta_2^S(\boldsymbol{\alpha})$ (that is, each point $\boldsymbol{\beta} \in \mathbb{N}^2$, on the right of $\boldsymbol{\alpha}$, is in $S$).

The Apéry Set of $S$ with respect to $\boldsymbol{\beta} \in S$ is defined as the set

$$\mathbf{Ap}(S, \boldsymbol{\beta}) = \{\boldsymbol{\alpha} \in S | \boldsymbol{\alpha} - \boldsymbol{\beta} \notin S\}.$$

Property (G1) implies that for a local good semigroup there exists a smallest nonzero element that we will denote by $\boldsymbol{e} = (e_1, e_2)$. We will usually consider the Apéry Set of $S$ with respect to $\boldsymbol{e}$ and, in this case, we will simply write $\mathbf{Ap}(S)$ (see Fig. 1).

*Remark 2.* By definitions of conductor of $S$ and of $\mathbf{Ap}(S)$, we have

$$\{\boldsymbol{\alpha} \in \mathbb{N}^2 \mid \boldsymbol{\alpha} \geq \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}\} \cap \mathbf{Ap}(S) = \emptyset.$$

Let $A$ be a subset of $\mathbb{N}^2$ and let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in A$, we say that $\boldsymbol{\beta}$ is a consecutive point of $\boldsymbol{\alpha}$ in $A$ if, for every $\boldsymbol{\mu} \in \mathbb{N}^2$ with $\boldsymbol{\alpha} < \boldsymbol{\mu} < \boldsymbol{\beta}$, we necessary have $\boldsymbol{\mu} \notin A$.

*Remark 3.* Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbf{Ap}(S)$. If $\boldsymbol{\beta}$ is a consecutive point of $\boldsymbol{\alpha}$ in $S$, then $\boldsymbol{\beta}$ is a consecutive point of $\boldsymbol{\alpha}$ in $\mathbf{Ap}(S)$. The converse it is not true.

Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in A$. The chain of points in $A$, $\{\boldsymbol{\alpha} = \boldsymbol{\alpha}_1 < \cdots < \boldsymbol{\alpha}_h < \cdots < \boldsymbol{\alpha}_n = \boldsymbol{\beta}\}$, with $\boldsymbol{\alpha}_{h+1}$ consecutive of $\boldsymbol{\alpha}_h$, is called *saturated* of length $n$. In this case $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are called the initial point and the final point, respectively, of the chain.

A *relative ideal* of a good semigroup $S$ is a subset $\emptyset \neq E \subseteq \mathbb{Z}^2$ such that $E + S \subseteq E$ and $\boldsymbol{\alpha} + E \subseteq S$ for some $\boldsymbol{\alpha} \in S$. A relative ideal $E$ contained in $S$ is simply called an *ideal*. If $E$ satisfies (G1) and (G2), then we say that $E$ is a *good ideal* of $S$ (condition (G3) follows from the definition of good relative ideal).

**Proposition 1** ([9, 17]) *All the saturated chains in a good ideal $E$ of $S$ with fixed initial and final points have the same length.*

If $\boldsymbol{\alpha}, \boldsymbol{\beta} \in E$, we denote by $d_E(\boldsymbol{\alpha}, \boldsymbol{\beta})$ the common length of all the saturated chains in the good ideal $E$ with initial point $\boldsymbol{\alpha}$ and final point $\boldsymbol{\beta}$. Moreover, if $E \supseteq F$ are two good ideals, considering $\boldsymbol{m}_E$ and $\boldsymbol{m}_F$ the minimal elements, respectively, of $E$ and $F$ and taking $\boldsymbol{\alpha} \geq \boldsymbol{c}_F$ where $\boldsymbol{c}_F$ is the conductor of $F$, it is possible to define the following distance function $d(E \setminus F) = d_E(\boldsymbol{m}_E, \boldsymbol{\alpha}) - d_F(\boldsymbol{m}_F, \boldsymbol{\alpha})$ (cf [9, 17] to see that it is a well defined distance). This distance funtion allows to translate many ring properties at semigroup level, since, if $I \supseteq J$ are two fractional ideals of $R$, it is proved, in the same papers, that the length $\lambda_R(I/J)$ equals $d_{v(R)}(v(I) \setminus v(J))$.

*Remark 4.* In the numerical semigroup case, that is $S = v(R)$ with $(R, \mathfrak{m})$ a one-dimensional, Noetherian, analitically irreducible, residually rational, local domain, it is well known that, if we denote by $x$ a minimal reduction of $\mathfrak{m}$ (i.e., an element of minimal value $e$), then $\overline{y} \neq 0$ in $R/(x)$ if and only if $v(y) \in \mathbf{Ap}(S) = \{\omega_0, \ldots, \omega_{e-1}\}$. Moreover, if $\omega_i = v(y_i)$, then $\left\{\overline{y}_0, \ldots \overline{y}_{e-1}\right\}$ are linear independent in the $R/\mathfrak{m}$-vector space $R/(x)$ and so they form a basis for it.

The first part of this remark can be easily generalized as follows, while we will be able to generalize the second part using all the results of the next section (see Theorem 6).

**Proposition 2** *Let $y \in R$; then $\overline{y} \neq 0$ in $R/(x)$ if and only if $v(y) \in \mathbf{Ap}(S)$.*

*Proof.* By definition $\overline{y} \neq 0$ in $R/(x)$ if and only if $y \notin (x)$ that is equivalent to say that $yx^{-1} \notin R$. Since $v(yx^{-1}) = v(y) - v(x)$, if $v(y) \in \mathbf{Ap}(S)$ we immediately get that $yx^{-1} \notin R$, i.e., $\overline{y} \neq 0$ in $R/(x)$. Conversely, assume that $v(y) \notin \mathbf{Ap}(S)$, i.e., $v(yx^{-1}) = v(y) - v(x) = v(r)$, for some $r \in R$. Since $R$ and both its projections on the two minimal primes are residually rational, it follows that there exists an invertible $u$ in $R$ such that $v(yx^{-1} - ur) > v(r)$; moreover, we can choose $u$ in order to increase the first or the second component, as we prefer. Hence, applying repeatedly this argument we obtain, after a finite number of steps, that $v(yx^{-1} - u'r') \geq c$, that implies $yx^{-1} - u'r' \in (R : \overline{R}) \subset R$; therefore $y \in (x)$, a contradiction. □

*Remark 5.* When $S$ is the value semigroup of a ring $(R, \mathfrak{m})$, it is not difficult to see that an element $x$ is a minimal reduction of $\mathfrak{m}$ if and only if $v(x) = \boldsymbol{e}$; hence, the integer $e = e_1 + e_2$ coincides with the multiplicity of $R$: in fact $e(R) = \lambda_R(R/(x)) = \dim_{R/\mathfrak{m}}(R/(x))$ (where $\lambda_R$ denotes the length of an $R$ module); now, using the computation of lengths explained above, it is not difficult to check that $\lambda_R(R/(x)) = d(S \setminus \boldsymbol{e} + S) = e_1 + e_2$.

It is useful to remark, at this point, that $S \setminus \boldsymbol{e} + S = \mathbf{Ap}(S)$. Hence, our first goal is, starting form a good semigroup $S \subseteq \mathbb{N}^2$, to get a partition $\mathbf{Ap}(S)$ in $e_1 + e_2 = e$ levels that should correspond to the $e$ elements of the Apéry Set of a numerical semigroup. After that we would like to find $e$ elements $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_e$ of the Apéry set of $S$, one in each class of the partition, with the property that, if $S = v(R)$ and $f_i \in R$ are such that $v(f_i) = \boldsymbol{\alpha}_i$, then $\overline{f}_1, \ldots, \overline{f}_e$ are linear independent in the $R/\mathfrak{m}$-vector space $R/(x)$ and so they form a basis for it.

We notice again that, given a good semigroups, it is not known a procedure to see if it is a value semigroup of a ring or not; so we are forced to use semigroup arguments without the possible help of ring techniques.

As in the numerical semigroup case, a symmetric good semigroup has a duality property. Indeed in [14], a good semigroup $S$ is said to be *symmetric* if

$$\boldsymbol{\alpha} \in S \iff \Delta^S(\boldsymbol{\gamma} - \boldsymbol{\alpha}) = \emptyset.$$

Moreover, in the numerical semigroup case, the symmetry of the semigroup $S$ can be characterized by a symmetry of its the Apéry Set: if we order its elements in increasing order $\mathbf{Ap}(S) = \{w_1, \ldots w_e\}$, then $S$ is symmetric if and only if $w_i + w_{e-i+1} = w_e$ for every $i = 1, \ldots, e$.

In this paper we also look for an analogue property for $\mathbf{Ap}(S)$ when $S$ is a symmetric good subsemigroup of $\mathbb{N}^2$.

## 3 Apéry Set of Good Semigroups in $\mathbb{N}^2$

In order to get the partition of the Apéry Set of $S$ we are looking for, we need to introduce a new relation on $\mathbb{N}^2$ (as it is done in [1]): we say that $(\alpha_1, \alpha_2) \leq\leq (\beta_1, \beta_2)$ if an only if $(\alpha_1, \alpha_2) = (\beta_1, \beta_2)$ or $(\alpha_1, \alpha_2) \neq (\beta_1, \beta_2)$ and $(\alpha_1, \alpha_2) \ll (\beta_1, \beta_2)$, where the last means $\alpha_1 < \beta_1$ and $\alpha_2 < \beta_2$.

We define the following subsets of $\mathbf{Ap}(S)$:

$$B^{(1)} = \{\boldsymbol{\alpha} \in \mathbf{Ap}(S) : \boldsymbol{\alpha} \text{ is maximal with respect to } \leq\leq\},$$

$$C^{(1)} := \{\boldsymbol{\alpha} \in B^{(1)} : \boldsymbol{\alpha} = \boldsymbol{\beta}_1 \wedge \boldsymbol{\beta}_2 \text{ for some } \boldsymbol{\beta}_1, \boldsymbol{\beta}_2 \in B^{(1)} \setminus \{\boldsymbol{\alpha}\}\} \text{ and } D^{(1)} = B^{(1)} \setminus C^{(1)}.$$

Assume $i > 1$ and that $D^{(1)}, \ldots, D^{(i-1)}$ have been defined; we set

$$B^{(i)} = \{\boldsymbol{\alpha} \in \mathbf{Ap}(S) \setminus (\bigcup_{j<i} D^{(j)}) : \boldsymbol{\alpha} \text{ is maximal with respect to } \leq\leq\},$$

$$C^{(i)} := \{\boldsymbol{\alpha} \in B^{(i)} : \boldsymbol{\alpha} = \boldsymbol{\beta}_1 \wedge \boldsymbol{\beta}_2 \text{ for some } \boldsymbol{\beta}_1, \boldsymbol{\beta}_2 \in B^{(i)} \setminus \{\boldsymbol{\alpha}\}\} \text{ and } D^{(i)} = B^{(i)} \setminus C^{(i)}.$$

Clearly, for some $N \in \mathbb{N}_+$, we have $\mathbf{Ap}(S) = \bigcup_{i=1}^{N} D^{(i)}$ and $D^{(i)} \cap D^{(j)} = \emptyset$, for any $i \neq j$. For simplicity we prefer to number the set of the partition in increasing order, so we set $A_i = D^{(N+1-i)}$. Hence

$$\mathbf{Ap}(S) = \bigcup_{i=1}^{N} A_i$$

We want to prove that $N = e_1 + e_2$. We will call the sets $A_i$ *levels* of the Apéry Set (see Fig. 2).

*Remark 6.* It is straightforward to see that $A_N = \Delta(\boldsymbol{\gamma} + \boldsymbol{e}) = \Delta^S(\boldsymbol{\gamma} + \boldsymbol{e})$ and that $A_1 = \{\mathbf{0}\}$. Moreover, if $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbf{Ap}(S)$, $\boldsymbol{\alpha} \ll \boldsymbol{\beta}$ and $\boldsymbol{\alpha} \in A_i$, then $\boldsymbol{\beta} \in A_j$ for some $j > i$.

**Lemma 1.** *The sets $A_i$ satisfy the following properties:*

*(1) for any $\boldsymbol{\alpha} \in A_i$ there exists $\boldsymbol{\beta} \in A_{i+1}$ such that $\boldsymbol{\alpha} \ll \boldsymbol{\beta}$ or $\boldsymbol{\alpha} = \boldsymbol{\beta}_1 \wedge \boldsymbol{\beta}_2$ with $\boldsymbol{\beta}_1, \boldsymbol{\beta}_2 \in A_{i+1}$ (both cases can happen at the same time);*
*(2) for every $\boldsymbol{\alpha} \in A_i$ and $\boldsymbol{\beta} \in A_j$, with $j \geq i$, $\boldsymbol{\beta} \not\ll \boldsymbol{\alpha}$;*
*(3) if $\boldsymbol{\alpha} \in A_i$, $\boldsymbol{\beta} \in \mathbf{Ap}(S)$ and $\boldsymbol{\beta} \geq \boldsymbol{\alpha}$, then $\boldsymbol{\beta} \in A_i \cup \cdots \cup A_N$;*
*(4) if $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$, $\boldsymbol{\beta} = (\alpha_1, \beta_2) \in A_i$, with $\alpha_2 < \beta_2$, then for any $\boldsymbol{\delta} = (\delta_1, \delta_2) \in \mathbf{Ap}(S)$ such that $\delta_1 > \alpha_1$ and $\delta_2 \geq \alpha_2$, we get $\boldsymbol{\delta} \in A_{i+1} \cup \cdots \cup A_N$; an analogous statement holds switching the components;*
*(5) if $\boldsymbol{\alpha} \ll \boldsymbol{\beta} \in \mathbf{Ap}(S)$ and they are consecutive in $S$, then there exists $i > 0$ such that $\boldsymbol{\alpha} \in A_i$ and $\boldsymbol{\beta} \in A_{i+1}$; if $\boldsymbol{\alpha} < \boldsymbol{\beta} \in \mathbf{Ap}(S)$, they share a component and they are consecutive in $S$, then there exists $i > 0$ such that either $\boldsymbol{\alpha} \in A_i$ and $\boldsymbol{\beta} \in A_{i+1}$ or $\boldsymbol{\alpha}, \boldsymbol{\beta} \in A_i$;*
*(6) let $\boldsymbol{\alpha} \in A_i$ and let be $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_j$ all the elements of $\mathbf{Ap}(S)$, $\boldsymbol{\alpha} < \boldsymbol{\beta}_r$ and consecutive to $\boldsymbol{\alpha}$ in $\mathbf{Ap}(S)$. Then at least one of them belongs to $A_{i+1}$;*
*(7) $\boldsymbol{\alpha} = (\alpha_1, \gamma_2 + e_2 + 1) \in A_i \Leftrightarrow (\alpha_1, n) \in A_i$ for some $n \geq \gamma_2 + e_2 + 1 \Leftrightarrow (\alpha_1, n) \in A_i$ for all $n \geq \gamma_2 + e_2 + 1$; an analogous statement holds switching the components;*
*(8) if $\boldsymbol{\alpha} = (\alpha_1, \gamma_2 + e_2 + 1) \in A_i$ and $\boldsymbol{\beta} = (\beta_1, \gamma_2 + e_2 + 1) \in \mathbf{Ap}(S)$, with $\beta_1 < \alpha_1$ and such that for every $a$, $\beta_1 < a < \alpha_1$, the point $(a, \gamma_2 + e_2 + 1) \notin \mathbf{Ap}(S)$, then $\boldsymbol{\beta} \in A_{i-1}$; an analogous statement holds switching the components. (We could state this property saying that, definitively, consecutive vertical lines (respectively, horizontal lines) of the Apéry Set belong to consecutive levels.)*

*Proof.* Properties (1), (2), and (3) follow immediately by definition.
(4) If $\delta_2 > \alpha_2$, then $\boldsymbol{\alpha} \ll \boldsymbol{\delta}$ and the assertion follows by definition of levels. If $\delta_2 = \alpha_2$, by property (3), $\boldsymbol{\delta} \in A_i \cup \cdots \cup A_N$; if $\boldsymbol{\delta} \in A_i$ we get a contradiction by the definition of levels, since $\boldsymbol{\alpha} = \boldsymbol{\beta} \wedge \boldsymbol{\delta}$.
(5) Let $i$ be such that $\boldsymbol{\alpha} \in A_i$. If $\boldsymbol{\alpha} = (\alpha_1, \alpha_2) \ll \boldsymbol{\beta} = (\beta_1, \beta_2)$ and they are consecutive in $S$, then there are no elements $(a, b)$ of $S$ such that $\alpha_1 \leq a < \beta_1$ and $\alpha_2 < b$ or $\alpha_1 < a$ and $\alpha_2 \leq b < \beta_2$, since $(a, b) \wedge \boldsymbol{\beta}$ would be a point of $S$ between $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$; in particular $\boldsymbol{\alpha}$ cannot be obtained as infimum of points of $S$. Moreover $\boldsymbol{\beta} \in A_j$,

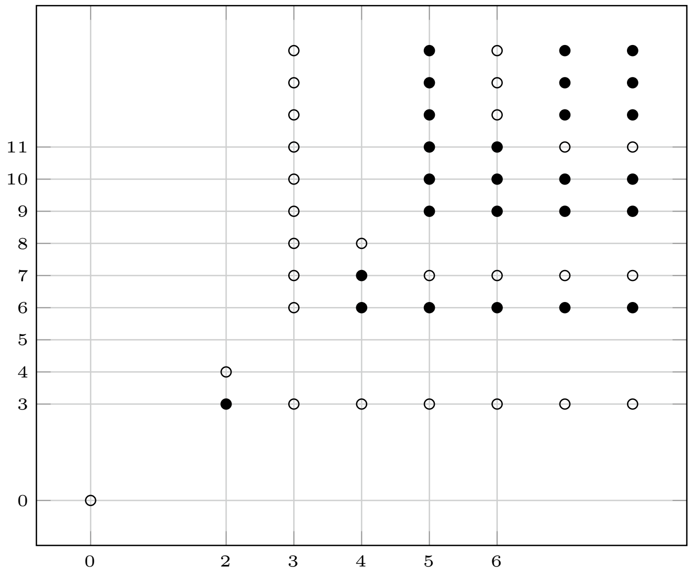



**Fig. 1** The value semigroup of $k[[X, Y, Z]]/(X^3 - Z^2) \cap (X^3 - Y^4)$. The elements of the Apéry Set are indicated with $\circ$

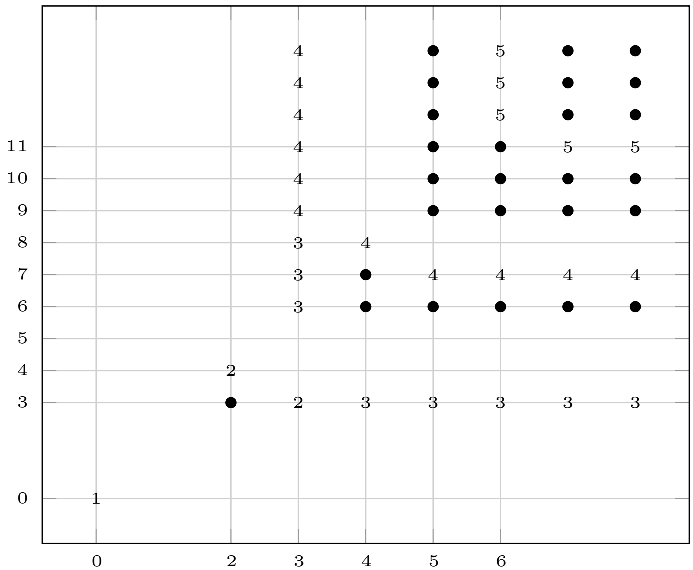



**Fig. 2** The Apéry Set of the semigroup in Fig. 1. We mark the elements of the set $A_i$ with the number $i$.

with $j > i$. By property (3) all the points of $\mathbf{Ap}(S)$ bigger than or equal to $\boldsymbol{\beta}$ belong to $A_h$, with $h \geq j$; hence, $\boldsymbol{\alpha}$ is maximal in $\mathbf{Ap}(S) \setminus (\bigcup_{h \geq j} A_h)$ with respect to $\leq\leq$ and, by definition of levels, this implies that $j = i + 1$.

Assume now that $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ share a component (e.g., $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$, $\boldsymbol{\beta} = (\alpha_1, \beta_2)$). Since they are consecutive in $S$, there are no elements $(a, b)$ of $S$ such that $\alpha_1 \leq a$ and $\alpha_2 < b < \beta_2$. Let $i$ be such that $\boldsymbol{\alpha} \in A_i$; by property (3) $\boldsymbol{\beta} \in A_j$ with $j \geq i$ and all the points of $\mathbf{Ap}(S)$ bigger than or equal to $\boldsymbol{\beta}$ belong to $A_h$, with $h \geq j$; by definition of levels, $\boldsymbol{\beta}$ is maximal in $\mathbf{Ap}(S) \setminus (\bigcup_{h>j} A_h)$ with respect to $\leq\leq$ and therefore also $\boldsymbol{\alpha}$ is maximal in the same set; hence either $j = i$ or $j = i + 1$.
(6) Assume by way of contradiction that for all $r$, $\boldsymbol{\beta}_r \in A_{h_r}$ with $h_r > i + 1$, set $h = \min\{h_r : r = 1, \ldots, j\}$. Hence $\boldsymbol{\alpha}$ is maximal in $\mathbf{Ap}(S) \setminus (\bigcup_{s \geq h} A_s)$ with respect to $\leq\leq$. In order to have $\boldsymbol{\alpha} \in A_i$, either $h = i + 1$ (that is the thesis) or $h = i + 2$ and $\boldsymbol{\alpha}$ is obtained as infimum of two elements $\boldsymbol{\delta}_1, \boldsymbol{\delta}_2 \in A_{i+1}$. But also in the second case, both $\boldsymbol{\delta}_i$ have to be consecutive to $\boldsymbol{\alpha}$ (otherwise they would be bigger than some elements $\boldsymbol{\beta}_r$, so they could not belong to $A_{i+1}$); hence, we get a contradiction by the assumption that $h = i + 2$. If, on the other hand, there exists $\boldsymbol{\beta}_r \in A_i$, it necessarily shares a component with $\boldsymbol{\alpha}$. Hence, by property (4) all the other $\boldsymbol{\beta}_s$ belong to $A_{i+1} \cup \cdots \cup A_N$. Now, applying the same argument as above, one of them has to be in $A_{i+1}$.
(7) Any element $\boldsymbol{\alpha} = (\alpha_1, \alpha_2)$ with $\alpha_2 > \gamma_2$ (respectively, $\alpha_1 > \gamma_1$) belongs to $S$ if and only if $(\alpha_1, \gamma_2 + 1) \in S$ (respectively, $((\gamma_1 + 1, \alpha_2) \in S)$. Hence it is clear that $\boldsymbol{\alpha} = (\alpha_1, \gamma_2 + e_2 + 1) \in \mathbf{Ap}(S)$ if and only if $(\alpha_1, n) \in \mathbf{Ap}(S)$ for some $n \geq \gamma_2 + e_2 + 1$ if and only if $(\alpha_1, n) \in \mathbf{Ap}(S)$ for all $(\alpha_1, n)$ (and the analogous statement holds switching the components).

So we have only to prove that these elements belongs to the same level (we will prove this fact for vertical lines and the corresponding statement for horizontal line is analogous). If not, by property (5), there exist two elements $\boldsymbol{\alpha}_1 = (\alpha_1, \alpha_2) \in A_i$ and $\boldsymbol{\alpha}_2 = (\alpha_1, \alpha_2 + 1) \in A_{i+1}$ consecutive in $\mathbf{Ap}(S)$. Now let $\beta_1 > \alpha_1$ be the smallest integer such that $\boldsymbol{\beta} = (\beta_1, \alpha_2) \in \mathbf{Ap}(S)$; since $\boldsymbol{\alpha}_1 = \boldsymbol{\alpha}_2 \wedge \boldsymbol{\beta}$ and there are no elements $(a, \alpha_2)$ of $\mathbf{Ap}(S)$, with $\alpha_1 < a < \beta_1$, it is clear that either $\boldsymbol{\beta} \in A_i$ or $\boldsymbol{\beta} \in A_{i+1}$; moreover $\boldsymbol{\alpha}_2 \ll (\beta_1, \alpha_2 + 2)$, hence, the last belongs to $A_j$ with $j > i + 1$. Hence, also in the vertical line corresponding to $\beta_1$ there are elements on different levels. Iterating the argument we get that the same happens for $\Delta_1(\boldsymbol{\gamma} + \boldsymbol{e}) \subseteq A_N$; a contradiction.
(8) By property (6), alle the elements of $S$ above $\boldsymbol{\alpha}$ are in $A_i$. Hence $\boldsymbol{\beta} \ll (\alpha_1, \gamma_2 + e_2 + 2)$ and therefore it belongs to $A_j$ with $j < i$. Moreover the hypothesis implies that $\boldsymbol{\beta}$ is maximal in $\mathbf{Ap}(S) \setminus (\bigcup_{h \geq i} A_h)$ with respect to $\leq\leq$ and cannot be obtained as infimum of two other elements maximal in the same set. The thesis follows immediately. □

Next lemma describes global properties of the elements of a good semigroup $S$ and of its Apéry Set.

**Lemma 2.** *The following assertions hold:*

*(1) Let* $\boldsymbol{\alpha} \in \mathbb{N}^2$ *and assume there is a finite positive number of elements in* $\Delta_1^S(\boldsymbol{\alpha}) \cap (\boldsymbol{e} + S)$. *Call* $\boldsymbol{\delta}$ *the maximum of them. Hence* $\Delta^S(\boldsymbol{\delta}) \subseteq \mathbf{Ap}(S)$*;*

*(2) Let $\boldsymbol{\alpha} \in \mathbf{Ap}(S)$. If there exists $\boldsymbol{\beta} \in (\boldsymbol{e} + S) \cap \Delta_1(\boldsymbol{\alpha})$, then $\Delta_2^S(\boldsymbol{\alpha}) \subseteq \mathbf{Ap}(S)$;*
*(3) Let $\boldsymbol{\alpha} = (a_1, a_2) \in A_i$ and suppose there exists $b_2 < a_2$ such that $\boldsymbol{\delta} = (a_1, b_2) \in S$ and $\Delta_2^S(\boldsymbol{\delta}) \subseteq \mathbf{Ap}(S)$. Then the minimal element $\boldsymbol{\beta} = (b_1, b_2)$ of $\Delta_2^S(\boldsymbol{\delta})$ is in $A_j$ for some $j \leq i$. In particular, if $\Delta^S(\boldsymbol{\delta}) \subseteq \mathbf{Ap}(S)$ and $\boldsymbol{\alpha}$ is the minimal element of $\Delta_1^S(\boldsymbol{\delta})$, $\boldsymbol{\beta} \in A_i$.*
*(4) Let $\boldsymbol{\alpha} = (a_1, a_2) \in A_i$ and suppose there exists $\boldsymbol{\delta} \in (\boldsymbol{e} + S) \cap \Delta_1(\boldsymbol{\alpha})$. Then $\Delta_2^S(\boldsymbol{\alpha}) \subseteq \mathbf{Ap}(S)$ and the minimal element $\boldsymbol{\beta}=(b_1, a_2)$ of $\Delta_2^S(\boldsymbol{\alpha})$ is also in $A_i$.*
*(5) Let $\boldsymbol{\alpha} \in A_i$ and assume $\Delta_1^S(\boldsymbol{\alpha}) \subseteq \mathbf{Ap}(S)$. Assume also that there exists $\boldsymbol{\beta} \in \Delta_1^S(\boldsymbol{\alpha}) \cap A_{i+1}$. Then there exists $\boldsymbol{\theta} \in (\Delta_1^S(\boldsymbol{\alpha}) \cap A_i) \cup \{\boldsymbol{\alpha}\}$ such that $\boldsymbol{\theta} < \boldsymbol{\beta}$ and $\Delta^S(\boldsymbol{\theta}) \subseteq \mathbf{Ap}(S)$.*
*The analogous assertions hold switching the components.*

*Proof.* (1) Since $\boldsymbol{\delta}$ is the maximum of $\Delta_1^S(\boldsymbol{\alpha}) \cap (\boldsymbol{e} + S)$, we have $\Delta_1^S(\boldsymbol{\delta}) \subseteq \mathbf{Ap}(S)$. Now, since $(\boldsymbol{e} + S)$ is a good ideal of $S$, by property (G2), also $\Delta_2^S(\boldsymbol{\delta}) \subseteq \mathbf{Ap}(S)$.
(2) Assume that there exists $\boldsymbol{\delta} \in \Delta_2(\boldsymbol{\alpha}) \cap (\boldsymbol{e} + S)$. Then again, since $(\boldsymbol{e} + S)$ is a good ideal, by property (G1), $\boldsymbol{\alpha} = \boldsymbol{\beta} \wedge \boldsymbol{\delta} \in (\boldsymbol{e} + S)$ and this is a contradiction.
(3) First we notice that $\Delta_2^S(\boldsymbol{\delta})$ is non-empty since also $\Delta_1^S(\boldsymbol{\delta})$ is non-empty (by axiom (G2)). Now, if $i = N$, the thesis easily follows by Remark 6. For $i < N$, we use the following argument: by definition of $\mathbf{Ap}(S)$ we can always find an element $\boldsymbol{\theta} = (g_1, g_2) \in A_{i+1}$ with $g_1 > a_1$ and $g_2 \geq a_2$. Hence, the fact that $\boldsymbol{\beta}$ is the minimal element of $\Delta_2^S(\boldsymbol{\delta})$ implies that $g_1 \geq b_1$ and this implies $\boldsymbol{\beta} \in A_j$ for $j \leq i + 1$.

If we assume by way of contradiction $\boldsymbol{\beta} \in A_{i+1}$, we would have $g_1 = b_1$ and hence, by axiom (G2), there exists an element $\boldsymbol{\omega} = (h_1, b_2)$ with $h_1 > b_1$. Since $\Delta_2^S(\boldsymbol{\delta}) \subseteq \mathbf{Ap}(S)$, we have $\boldsymbol{\omega} \in \mathbf{Ap}(S)$ and we may assume $\boldsymbol{\omega}$ minimal in $\Delta_2^S(\boldsymbol{\beta})$. Thus, if $\boldsymbol{\omega} \in A_{i+1}$ we have $\boldsymbol{\beta} = \boldsymbol{\theta} \wedge \boldsymbol{\omega} \in A_i$, otherwise we should have $\boldsymbol{\omega} \in A_j$ for some $j > i + 1$. But now we are in the same situation of the hypothesis of the lemma with $\boldsymbol{\theta}, \boldsymbol{\beta}, \boldsymbol{\omega}$ playing the role of $\boldsymbol{\alpha}, \boldsymbol{\delta}, \boldsymbol{\beta}$. In this way, iterating the process, we can create an infinite sequence of elements $\boldsymbol{\omega}^k \in \Delta_2(\boldsymbol{\delta}) \cap A_{i+k}$ and this is a contradiction because the levels of $\mathbf{Ap}(S)$ are in a finite number. The last sentence of the statement follows since, having also $\Delta_1^S(\boldsymbol{\delta}) \subseteq \mathbf{Ap}(S)$, we apply the same result and get the level of $\boldsymbol{\alpha}$ less or equal than the level of $\boldsymbol{\beta}$.
(4) If $i = N$, the thesis is clear by Remark 6. For $i < N$, clearly $\Delta_2^S(\boldsymbol{\alpha})$ is non-empty and it is contained in $\mathbf{Ap}(S)$ by (2). First assume that there exists $\boldsymbol{\theta} = (g_1, g_2) \in A_{i+1}$ such that $\boldsymbol{\theta} \gg \boldsymbol{\alpha}$. Since $\boldsymbol{\beta}$ is the minimal element of $\Delta_2^S(\boldsymbol{\alpha})$, we have $g_1 \geq b_1$. But now, if $g_1 > b_1$, then $\boldsymbol{\theta} \gg \boldsymbol{\beta}$ and hence $\boldsymbol{\beta} \in A_i$. Instead if $g_1 = b_1$ we can find a minimal element $\boldsymbol{\omega} \in \Delta_2(\boldsymbol{\beta}) \cap \mathbf{Ap}(S)$ and $\boldsymbol{\beta} = \boldsymbol{\theta} \wedge \boldsymbol{\omega}$. By (3), $\boldsymbol{\omega} \in A_j$ with $j \leq i + 1$ and thus $\boldsymbol{\beta} \in A_i$.

Now assume that there is no element of $A_{i+1}$ dominating $\boldsymbol{\alpha}$. It follows that $\boldsymbol{\alpha} = \boldsymbol{\theta} \wedge \boldsymbol{\beta}$ with $\boldsymbol{\theta}, \boldsymbol{\beta} \in A_{i+1}$. We can assume by way of contradiction both of these elements to be minimal, otherwise we would have the minimal $\boldsymbol{\beta} \in A_i$. If $\boldsymbol{\theta} \in \Delta_1(\boldsymbol{\alpha})$ is still such that $\boldsymbol{\theta} < \boldsymbol{\delta}$, we have $\Delta_2^S(\boldsymbol{\theta}) \subseteq \mathbf{Ap}(S)$ and we can find in it a minimal element $\boldsymbol{\omega} \in \Delta_2^S(\boldsymbol{\theta})$ which has to be in $A_{i+2}$ by Lemma 1(5) (otherwise we would have an element of $A_{i+1}$ dominating $\boldsymbol{\alpha}$).

Suppose there exists $\boldsymbol{\omega}^1 \in A_{i+2}$ such that $\boldsymbol{\omega}^1 \gg \boldsymbol{\theta}$. Clearly we cannot have neither $\boldsymbol{\omega}^1 \gg \boldsymbol{\omega}$ nor $\boldsymbol{\omega}^1 \in \Delta_1(\boldsymbol{\omega})$ because this would contradict (3). Hence there exists $\boldsymbol{\omega}^1 \wedge \boldsymbol{\omega} \in \Delta_2^S(\boldsymbol{\theta})$ and this is a contradiction since $\boldsymbol{\omega}$ is minimal in $\Delta_2^S(\boldsymbol{\theta})$.

Hence, we can assume that there are not elements of $A_{i+2}$ dominating $\boldsymbol{\theta}$. This means that $\boldsymbol{\theta}$ is the minimum of two elements $\boldsymbol{\omega}^1, \boldsymbol{\eta}^2 \in A_{i+2}$ and we can iterate the process replacing the elements $\boldsymbol{\theta}, \boldsymbol{\alpha}, \boldsymbol{\beta}$ with $\boldsymbol{\omega}^1, \boldsymbol{\theta}, \boldsymbol{\eta}^2$. If $\Delta_1(\boldsymbol{\alpha})$ is eventually contained in $\boldsymbol{e} + S$, after a finite number of iteration we will find an element $\boldsymbol{\omega}^k$ which is maximal in $\Delta_1(\boldsymbol{\alpha}) \cap \mathbf{Ap}(S)$ and it is dominated by some element of a greater level of $\mathbf{Ap}(S)$ (notice that in this case the elements in $\Delta_1(\boldsymbol{\alpha})$ are dominated by elements in $A_N$). This would lead to a contradiction like in the previous paragraph. If $\Delta_1(\boldsymbol{\alpha}) \cap (\boldsymbol{e} + S)$ has a maximum $\boldsymbol{\delta}$, then $\Delta^S(\boldsymbol{\delta}) \subseteq \mathbf{Ap}(S)$ by (1) and our iterative process will end, by replacing the name of the elements and of the levels, in a situation with $\boldsymbol{\alpha} = \boldsymbol{\theta} \wedge \boldsymbol{\beta}$ with $\boldsymbol{\theta}, \boldsymbol{\beta} \in A_{i+1}$ and $\boldsymbol{\theta} > \boldsymbol{\delta} > \boldsymbol{\alpha}$. In this setting, we can find a minimal element $\boldsymbol{\omega} \in \Delta_2(\boldsymbol{\delta}) \cap \mathbf{Ap}(S)$. By (3), $\boldsymbol{\omega} \in A_j$ with $j \leq i + 1$ and this again contradicts the assumption since $\boldsymbol{\omega} \gg \boldsymbol{\alpha}$.
(5) Assume $\Delta_2^S(\boldsymbol{\alpha}) \nsubseteq \mathbf{Ap}(S)$. Hence by (4), we have that the minimal element $\boldsymbol{\omega}$ of $\Delta_1^S(\boldsymbol{\alpha})$ is also in $A_i$. Hence $\boldsymbol{\omega} < \boldsymbol{\beta}$. If again $\Delta_2^S(\boldsymbol{\omega}) \nsubseteq \mathbf{Ap}(S)$ we find an element $\boldsymbol{\omega}^1 \in \Delta_1^S(\boldsymbol{\alpha}) \cap A_i$ and $\boldsymbol{\omega}^1 < \boldsymbol{\beta}$. Since there is a finite number of elements in $\Delta_1^S(\boldsymbol{\alpha})$ between $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, the process must stop to an element $\boldsymbol{\theta} \in \Delta_1^S(\boldsymbol{\alpha}) \cap A_i$ such that $\boldsymbol{\theta} < \boldsymbol{\beta}$ and $\Delta^S(\boldsymbol{\theta}) \subseteq \mathbf{Ap}(S)$. □

**Theorem 3.** *Let $S \subseteq \mathbb{N}^2$ be a good semigroup and let $\boldsymbol{e} = (e_1, e_2)$ be its minimal nonzero element. Let $\mathbf{Ap}(S) = \bigcup_{i=1}^{N} A_i$ where the sets $A_i$ are defined as above. Then $N = e_1 + e_2$.*

*Proof.* We have that $\mathbf{Ap}(S) = S \setminus (\boldsymbol{e} + S)$. Moreover both $S$ and $\boldsymbol{e} + S$ are good ideals so we can compute the distance function $d(S \setminus \boldsymbol{e} + S)$ as $d_S(\mathbf{0}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) - d_{\boldsymbol{e}+S}(\boldsymbol{e}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1})$; on the other hand we know that $d(S \setminus \boldsymbol{e} + S) = e_1 + e_2$.

Hence, to prove that $N \geq e_1 + e_2$ we show that there exists a saturated chain in $S$, between $\mathbf{0}$ and $\boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}$ that contains exactly one element of every level $A_i$: if we do not consider the $N$ elements of $\mathbf{Ap}(S)$ in this chain we get a chain (not necessarily saturated) in $\boldsymbol{e} + S$; hence, $d_S(\mathbf{0}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) - N \leq d_{\boldsymbol{e}+S}(\boldsymbol{e}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1})$, that means

$$e_1 + e_2 = d_S(\mathbf{0}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) - d_{\boldsymbol{e}+S}(\boldsymbol{e}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) \leq N.$$

To construct such a chain we start from $\mathbf{0} \in S \cap \mathbf{Ap}(S)$ and then we choose $N$ elements, one for each level $A_i$ using property (6) of Lemma 1: given $\boldsymbol{\alpha}_i \in A_i$ we choose $\boldsymbol{\alpha}_{i+1} \in A_{i+1}$ consecutive to $\boldsymbol{\alpha}_i$ in $\mathbf{Ap}(S)$; so we get a chain of $N$ elements in $\mathbf{Ap}(S)$, each one consecutive to the previous in $\mathbf{Ap}(S)$. Hence when we saturate this chain in $S$, we add only elements in $S \setminus \mathbf{Ap}(S) = \boldsymbol{e} + S$, and we obtain the desired chain.

In order to prove that $N \leq e_1 + e_2$ we want to construct a saturated chain in $\boldsymbol{e} + S$ between $\boldsymbol{e}$ and $\boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}$ such that, when we saturate it in $S$, as a chain between $\mathbf{0}$ and $\boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}$, we use at least one element for every level $A_i$ (it is clear that we can only add elements of $\mathbf{Ap}(S) = S \setminus (\boldsymbol{e} + S)$: in fact, if we add $n \geq N$ elements in $\mathbf{Ap}(S)$, this would imply $d_S(\mathbf{0}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) = d_{\boldsymbol{e}+S}(\boldsymbol{e}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) + n \geq d_{\boldsymbol{e}+S}(\boldsymbol{e}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) + N$, that is $N \leq d_S(\mathbf{0}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) - d_{\boldsymbol{e}+S}(\boldsymbol{e}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) = e_1 + e_2$.

To construct such a chain we start with $\mathbf{0} \ll \boldsymbol{e}$, that is a saturated chain in $S$; hence, we can assume that we have constructed a saturated chain in $S$, say $\boldsymbol{\alpha}_0 = \mathbf{0} < \boldsymbol{\alpha}_1 < \cdots < \boldsymbol{\alpha}_h$, such that, $\boldsymbol{\alpha}_h \leq \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}$, if we delete the elements $\boldsymbol{\alpha}_i \in \mathbf{Ap}(S)$ we get a saturated chain in $\boldsymbol{e} + S$ and every level $A_1, \ldots, A_j$ has at least one representative in it. To apply a recursive argument we need either to stretch the chain adding one or more new elements, the first consecutive to $\boldsymbol{\alpha}_h$ in $S$ and any of the others consecutive to the previous one, or to produce a new chain with the same properties (replacing the last elements of the constructed chain) for which all the levels $A_1, \ldots, A_{j+1}$ have at least one representative in it. The process will end, since the length of a saturated chain is bounded by $d_S(\mathbf{0}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1})$ (and at the last step we have to touch $A_N$) and the number of levels is bounded by $N$. We explain now how to add a new element to the chain in all the different possible cases. Before starting, we observe that if we have $\boldsymbol{\gamma} + \boldsymbol{e} + 1 \in \Delta^S(\boldsymbol{\alpha}_h)$ we complete the chain adding all the elements between $\boldsymbol{\alpha}_h$ and $\boldsymbol{\gamma} + \boldsymbol{e} + 1$ sharing a coordinate with them (they are all on the same horizontal or on the same vertical line). By Lemma 1(7 and 8) this chain will touch exactly once all the levels of $\mathbf{Ap}(S)$ between $j + 1$ and $N$.

Hence we consider now all the cases in which $\boldsymbol{\alpha}_h \ll \boldsymbol{\gamma} + \boldsymbol{e} + 1$. We can start from one of the following two cases: either (case A) $\boldsymbol{\alpha}_h \in \boldsymbol{e} + S$ or (case B) $\boldsymbol{\alpha}_h \in A_j$ (notice that at the beginning of the chain we have $\mathbf{0} \ll \boldsymbol{e}$, so we start from case A).

In both cases if $\boldsymbol{\alpha}_h$ has only one consecutive element $\boldsymbol{\beta}$ in $S$, necessarily (by axiom (G2)) we have $\boldsymbol{\alpha}_h \ll \boldsymbol{\beta}$ and we should be forced to choose $\boldsymbol{\alpha}_{h+1} = \boldsymbol{\beta}$. If $\boldsymbol{\beta} \in \boldsymbol{e} + S$, the new chain obviously satisfies the requested properties; moreover it has one element more and now we are in case A. On the other hand, assume $\boldsymbol{\beta} \in \mathbf{Ap}(S)$; the condition $\boldsymbol{\alpha}_h \ll \boldsymbol{\beta}$ implies that $\boldsymbol{\alpha}_i \ll \boldsymbol{\beta}$, for all $i = 0, \ldots, h$; in particular, let $\boldsymbol{\alpha}_r \in A_j$ be the last element of the Apéry Set in the chain. Hence, by Remark 6 we know that $\boldsymbol{\beta} \in A_{j+1} \cup \cdots \cup A_N$; if it is in $A_{j+1}$, we simply add $\boldsymbol{\beta}$ to the chain and proceed in case B. Otherwise, if $\boldsymbol{\beta}$ it is not in $A_{j+1}$, by Lemma 1(6) there exists another element $\boldsymbol{\delta}$ consecutive in $\mathbf{Ap}(S)$ to $\boldsymbol{\alpha}_r$, such that $\boldsymbol{\delta} \in A_{j+1}$ (notice that, by Lemma 1(5), this situation can happen only in case A). Now $\boldsymbol{\delta}$ has to share a component with one of the elements $\boldsymbol{\alpha}_r, \ldots, \boldsymbol{\alpha}_h$ otherwise, taking infimums, it would create a new point that makes the original chain non-saturated; more precisely, if it is above (respectively, on the right) of some $\boldsymbol{\alpha}_l$ for $r \leq l \leq h$, then $\boldsymbol{\alpha}_{l+1}$ has to be either above or on the right of $\boldsymbol{\alpha}_l$. Now we change the chain substituting $\boldsymbol{\alpha}_m$ with $\boldsymbol{\delta} \wedge \boldsymbol{\alpha}_m$, for every $m \geq l + 1$; successively we add to the chain $\boldsymbol{\delta} \wedge \boldsymbol{\beta}$ and all the other elements of $S$ on the vertical (respectively, horizontal) line until we reach $\boldsymbol{\delta}$ (notice that we may have $\boldsymbol{\delta} \wedge \boldsymbol{\alpha}_m = \boldsymbol{\delta}$ for some $m$ and in that case we simply stop to $\boldsymbol{\delta}$ because we have reached it). We show an example of the preceding process in the first picture of Figure 3.

Hence we created a new chain with the requested properties, such that every level $A_1, \ldots, A_{j+1}$ has at least one representative in it and now we are in case B.

It remains to study what happens if $\boldsymbol{\alpha}_h = \boldsymbol{\beta}_1 \wedge \boldsymbol{\beta}_2$ (where both $\boldsymbol{\beta}_i$ are consecutive to $\boldsymbol{\alpha}_h$ in $S$).

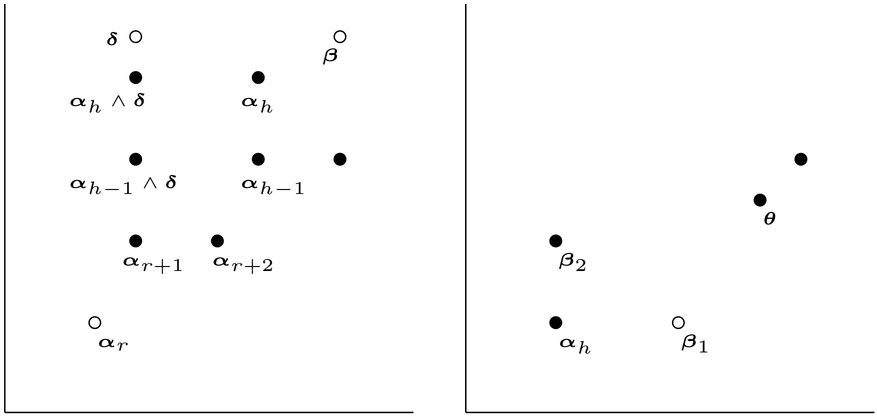



**Fig. 3** Explanation of parts of the proof

• Case A. In this case let $\boldsymbol{\alpha}_r \in A_j$ be the last element of the Apéry Set in the chain. The following situations can occur:

(A.1) both $\boldsymbol{\beta}_i \in \mathbf{Ap}(S)$: if at least one $\boldsymbol{\beta}_i$ belongs to $A_{j+1}$, we set $\boldsymbol{\alpha}_{h+1} := \boldsymbol{\beta}_i$ and we switch to case B. Otherwise, since $\boldsymbol{\alpha}_r \ll \boldsymbol{\beta}_i$, for at least one $i = 1, 2$, we have, for the same $i$, $\boldsymbol{\beta}_i \in A_{j+2} \cup \cdots \cup A_N$. By Lemma 1(6), there exists another element $\boldsymbol{\delta}$ consecutive in $\mathbf{Ap}(S)$ to $\boldsymbol{\alpha}_r$, such that $\boldsymbol{\delta} \in A_{j+1}$. Using the same argument as above, i.e., replacing the last part of the chain with $\boldsymbol{\delta} \wedge \boldsymbol{\alpha}_m$ (for $r < m \leq h$) and then proceeding on a single line until reaching $\boldsymbol{\delta}$, we obtain the desired result and we switch to case B;
(A.2) both $\boldsymbol{\beta}_i \in \boldsymbol{e} + S$: we can move to any one of them indifferently and proceed in case A;
(A.3) $\boldsymbol{\beta}_1 \in \mathbf{Ap}(S)$ and $\boldsymbol{\beta}_2 \in \boldsymbol{e} + S$: if $\boldsymbol{\beta}_1 \in A_j$ (this can happen only if the last element of the Apéry Set in the chain $\boldsymbol{\alpha}_r$ shares a component with both $\boldsymbol{\alpha}_h$ and $\boldsymbol{\beta}_1$), we set $\boldsymbol{\alpha}_{h+1} = \boldsymbol{\beta}_2$ and we proceed in case A; if $\boldsymbol{\beta}_1 \in A_{j+2}$, we take again $\boldsymbol{\delta}$ consecutive in $\mathbf{Ap}(S)$ to $\boldsymbol{\alpha}_r$ such that $\boldsymbol{\delta} \in A_{j+1}$ and, replacing the last part of the chain with $\boldsymbol{\delta} \wedge \boldsymbol{\alpha}_m$ (the elements $\boldsymbol{\alpha}_m$ are defined as in A.1), we obtain the desired result and we switch to case B.

It remains the hardest situation, i.e., $\boldsymbol{\beta}_1 \in A_{j+1}$; in this case, we have to show that both $\boldsymbol{\beta}_1$ and $\boldsymbol{\beta}_2$ do not have the same element as unique consecutive in $S$; if this was the case and if $\boldsymbol{\beta}_1$ was the only consecutive of $\boldsymbol{\alpha}_r$ in $\mathbf{Ap}(S)$ belonging to $A_{j+1}$, it would be impossible to proceed, because either we would skip the level $A_{j+1}$ or we would create a chain such that, if we delete the elements of $\mathbf{Ap}(S)$, we do not get a saturated chain in $\boldsymbol{e} + S$ (for this situation, see the second picture of Figure 3, in which we denote by $\boldsymbol{\theta}$ the unique consecutive element in $S$ of both $\boldsymbol{\beta}_1$ and $\boldsymbol{\beta}_2$ and we consider the two possible chains between $\boldsymbol{\alpha}_h$ and $\boldsymbol{\theta}$).

Let assume that $\boldsymbol{\alpha}_h$ and $\boldsymbol{\beta}_2$ share the first component (the other case is symmetric): So $\boldsymbol{\alpha}_h = (a_1, a_2)$ and $\boldsymbol{\beta}_2 = (a_1, b_2)$, with $b_2 > a_2$. They do not belong to $\mathbf{Ap}(S)$ hence both $\boldsymbol{\alpha}_h - \boldsymbol{e}$ and $\boldsymbol{\beta}_2 - \boldsymbol{e}$ belong to $S$. Hence, by Property (G2), there must be an element $(c_1, a_2 - e_2) \in S$ and so we have also another point of $S$, $\boldsymbol{\delta} = (c_1 + e_1, a_2) \in \boldsymbol{e} + S$, on the right of $\boldsymbol{\alpha}_h$. Since $\boldsymbol{\beta}_1$ is also on the right of $\boldsymbol{\alpha}_h$ and it is consecutive to it in $S$, we have three points in the same horizontal line: $\boldsymbol{\alpha}_h < \boldsymbol{\beta}_1 < \boldsymbol{\delta}$. Now, choosing $\boldsymbol{\delta}$ minimal, we are sure that it is consecutive to $\boldsymbol{\alpha}_h$ in $\boldsymbol{e} + S$. Moreover, we are sure that moving from $\boldsymbol{\beta}_1$ to $\boldsymbol{\delta}$ on the horizontal line, if we meet points of $\mathbf{Ap}(S)$, by Lemma 1(5) we do not skip any level and by Lemma 2(4) and Lemma 1(4) we do not repeat twice the same level. Hence we can stretch the chain up to $\boldsymbol{\delta}$ and proceed in case A.

• Case B. We notice that, in this case, if $\boldsymbol{\beta}_i \in \mathbf{Ap}(S)$ it has to belong either to $A_j$ or to $A_{j+1}$, since they are consecutive in $S$ to $\boldsymbol{\alpha}_h \in \mathbf{Ap}(S)$ (again by Lemma 1(5)).

The following situations can occur:

(B.1) both $\boldsymbol{\beta}_i \in A_{j+1}$: we can move to any one of them indifferently and proceed in case B;
(B.2) both $\boldsymbol{\beta}_i \in \boldsymbol{e} + S$: this cannot happen by Lemma 2(2);
(B.3) $\boldsymbol{\beta}_1 \in A_j$ and $\boldsymbol{\beta}_2 \in A_{j+1}$: we move to $\boldsymbol{\beta}_2$ and proceed in case B;
(B.4) $\boldsymbol{\beta}_1 \in A_j$ and $\boldsymbol{\beta}_2 \in \boldsymbol{e} + S$: we move to $\boldsymbol{\beta}_2$ and switch to case A;
(B.5) $\boldsymbol{\beta}_1 \in A_{j+1}$ and $\boldsymbol{\beta}_2 \in \boldsymbol{e} + S$: we can assume that $\boldsymbol{\beta}_1$ is on the right of $\boldsymbol{\alpha}_h$ and $\boldsymbol{\beta}_2$ is above it; in this case either there is another element $\boldsymbol{\beta}' \in A_{j+1}$ such that $\boldsymbol{\alpha} = \boldsymbol{\beta}_1 \wedge \boldsymbol{\beta}'$ and $\boldsymbol{\alpha} < \boldsymbol{\beta}_2 < \boldsymbol{\beta}'$ share the first component; we choose $\boldsymbol{\beta}'$ minimal with this property and we move to $\boldsymbol{\beta}_2$ and then to $\boldsymbol{\beta}'$ (considering all possible elements between them, that have to belong to $\boldsymbol{e} + S$) or there exists $\boldsymbol{\beta}'' \in A_{j+1}$ above $\boldsymbol{\beta}_1$ and consecutive to both $\boldsymbol{\beta}_i$; so we move to $\boldsymbol{\beta}_2$ and then to $\boldsymbol{\beta}''$. In both cases we proceed in case B.

The proof is complete. □

From now on we are going to denote the number of levels of the Apéry Set by $e = e(S) = e_1 + e_2$ that, as we noticed in the previous section, coincides with the multiplicity of the ring $R$, in case $S = v(R)$.

We derive from the proof of the preceding theorem, a sort of converse of property (1) of Lemma 1. We are going to make use of this next result in the last section of this article, while proving a duality property for the levels of the Apéry Set of a symmetric good semigroup.

**Proposition 4** *Let $S \subseteq \mathbb{N}^2$ be a good semigroup and let $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ be its Apéry Set. Let $\boldsymbol{\alpha} \in A_i$ for $i \geq 2$. Then, there exists $\boldsymbol{\beta} \in A_{i-1}$ such that $\boldsymbol{\beta} \leq \boldsymbol{\alpha}$.*

*Proof.* Since $A_1 = \{\mathbf{0}\}$, and $\boldsymbol{\alpha} \geq \mathbf{0}$ for every $\boldsymbol{\alpha} \in S$, the thesis is true for $i = 2$ and hence, by induction, we can assume it true for every $j < i$. Assume by way of contradiction that there exists $\boldsymbol{\alpha} \in A_i$ such that $\boldsymbol{\theta} \not\leq \boldsymbol{\alpha}$ for every $\boldsymbol{\theta} \in A_{i-1}$. We can further assume that also $\boldsymbol{\delta} \not\leq \boldsymbol{\alpha}$ for every $\boldsymbol{\delta} \in A_i$, otherwise we can simply replace $\boldsymbol{\alpha}$ with some element $\boldsymbol{\delta} \leq \boldsymbol{\alpha}$ and minimal in $A_i$ with respect to "$\leq$".

Take $\boldsymbol{\omega} \in \mathbf{Ap}(S)$ such that $\boldsymbol{\omega} \leq \boldsymbol{\alpha}$ and they are consecutive in $\mathbf{Ap}(S)$, hence, $\boldsymbol{\omega} \in A_j$ with $j < i - 1$. We may assume $j$ to be the maximal level of an element of $\mathbf{Ap}(S)$ having $\boldsymbol{\alpha}$ as a consecutive element in $\mathbf{Ap}(S)$. Assume there exists an element $\boldsymbol{\omega}' \in A_j$ such that $\boldsymbol{\omega} \in \Delta^S(\boldsymbol{\omega}')$. Hence, we can find a saturated chain in $S$ between $\boldsymbol{\omega}'$ and $\boldsymbol{\alpha}$ that does not contain any other elements of $\mathbf{Ap}(S)$. Indeed, we can find

$\boldsymbol{\beta} \in S$ such that $\boldsymbol{\omega}' \leq \boldsymbol{\beta} \leq \boldsymbol{\alpha}$, $\boldsymbol{\beta} \in \Delta^S(\boldsymbol{\omega}')$ and it is incomparable with $\boldsymbol{\omega}$ (i.e., either $\boldsymbol{\beta} \in \Delta_2^S(\boldsymbol{\omega}')$ and $\boldsymbol{\omega} \in \Delta_1^S(\boldsymbol{\omega}')$ or the converse). If $\boldsymbol{\beta} \in \mathbf{Ap}(S)$, then it has to be in $A_j$, but this is impossible since $\boldsymbol{\omega}' = \boldsymbol{\omega} \wedge \boldsymbol{\beta}$ would be the minimum of two elements of $A_j$, and therefore not in $A_j$.

It follows that we can choose an element $\tilde{\boldsymbol{\omega}} \leq \boldsymbol{\omega}$ minimal with respect to the property of being in $A_j$ (this element could be $\boldsymbol{\omega}$ itself) and find a saturated chain in $S$ between $\tilde{\boldsymbol{\omega}}$ and $\boldsymbol{\alpha}$ not containing any other elements of $\mathbf{Ap}(S)$. By inductive hypothesis, $\tilde{\boldsymbol{\omega}} \geq \boldsymbol{\delta} \in A_{j-1}$, and hence we can iterate the preceding process and construct a saturated chain in $S$ between $\mathbf{0}$ and $\boldsymbol{\alpha}$, containing only one element for every level of $\mathbf{Ap}(S)$ between 1 and $j$ and not containing any element in the levels strictly between $j$ and $i$. As in the first part of the proof of Theorem 3, we can extend this chain adding a chain in $S$ from $\boldsymbol{\alpha}$ to $\boldsymbol{\gamma} - \boldsymbol{e} + \mathbf{1}$ including only one element for each level of $\mathbf{Ap}(S)$ greater than $i$. The obtained chain going between $\mathbf{0}$ and $\boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}$ contains $h := e - (i - j) + 1$ elements of $\mathbf{Ap}(S)$, thus, removing those elements, we can find a chain in $\boldsymbol{e} + S$ between $\boldsymbol{e}$ and $\boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}$ of length

$$d_S(\mathbf{0}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) - h = d_{\boldsymbol{e}+S}(\boldsymbol{e}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1}) + e - h.$$

Since $j < i - 1$, this length is strictly bigger than $d_{\boldsymbol{e}+S}(\boldsymbol{e}, \boldsymbol{\gamma} + \boldsymbol{e} + \mathbf{1})$ and this is a contradiction. □

As we can observe in all the preceding examples of good semigroups, the first levels of $\mathbf{Ap}(S)$ are finite while the others contain either one or two infinite lines of elements. After formalizing the concept of infinite lines of elements in two definitions, we describe precisely this behavior in the next theorem (Figure 4).

**Definition 1.** Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a good semigroup. Given an element $s_1 \in S_1$, we say that $\Delta_1(s_1, r)$ is an *infinite line* of $S$ if there exists $r \in S_2$ such that $\Delta_1(s_1, r) \subseteq S$. If $\Delta_1(s_1, r) \subseteq \mathbf{Ap}(S)$, we say that $\Delta_1(s_1, r)$ is an infinite line of $\mathbf{Ap}(S)$.

Analogously, given an element $s_2 \in S_2$, $\Delta_2(q, s_2)$ is an *infinite line* of $S$ (resp. $\mathbf{Ap}(S)$) if there exists $q \in S_1$ such that $\Delta_2(q, s_2) \subseteq S$ (resp. $\mathbf{Ap}(S)$). If an infinite line of $S$ is not an infinite line of $\mathbf{Ap}(S)$, then it is an infinite line of $\boldsymbol{e} + S$.

**Definition 2.** Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a good semigroup and let $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ be its Apéry Set. For $i = 1, \ldots, e$, we say that

1. $A_i$ contains two infinite lines if there exist two elements $s_1 \in S_1$ and $s_2 \in S_2$, such that, for some $q \in S_1$, $r \in S_2$, $\Delta_1(s_1, r)$, $\Delta_2(q, s_2)$ are infinite lines of $\mathbf{Ap}(S)$ and they are contained in $A_i$.
2. $A_i$ contains only one infinite line if only one of the previous conditions hold.
3. $A_i$ is finite if it contains a finite number of elements.

**Theorem 5.** *Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a good semigroup, let $\boldsymbol{e} = (e_1, e_2)$ be its minimal nonzero element. Let $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ be the Apéry Set of $S$. Assume $e_1 \geq e_2$. Then,*

*(1) The levels $A_e, A_{e-1}, \ldots, A_{e-e_2+1}$ contain two infinite lines.*

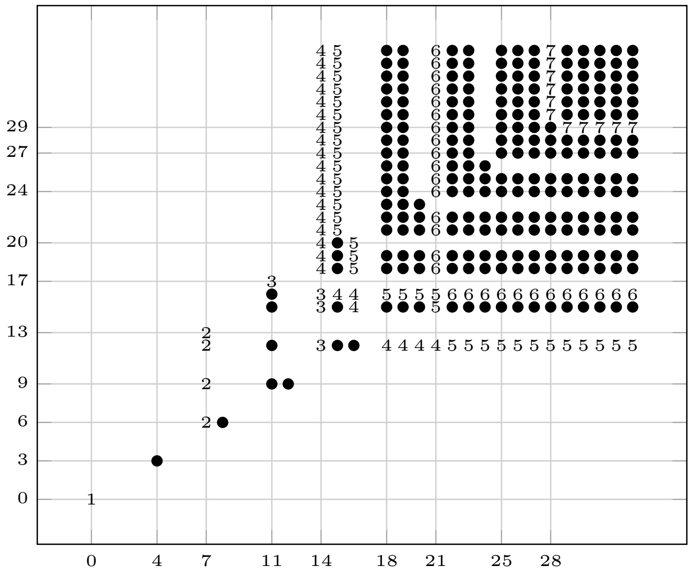



**Fig. 4** This is an example of a good semigroup that is not the value semigroup of any ring, see [1, Example 2.16, p. 8]

*(2) The levels $A_{e-e_2}, \ldots, A_{e-e_1+1}$ contain only one infinite line of the form $\Delta_1(s_1, r)$ corresponding to some element $s_1 \in S_1$.*

*(3) The levels $A_{e-e_1}, \ldots, A_2, A_1$ are finite.*

*If $e_1 \leq e_2$ the correspondent analogous conditions hold.*

*Proof.* First we show that in the projection $S_1$ of $S$ there are exactly $e_1$ elements $s_1, \ldots, s_{e_1}$ such that $\Delta_1(s_i, r)$ is an infinite line of $\mathbf{Ap}(S)$ (for some $r \in S_2$). Let $\boldsymbol{c} = (c_1, c_2)$ be the conductor of $S$. Following the preceding definitions, we have that for every $n \geq c_1$ and sufficiently large $r \in S_2$, $\Delta_1(n, r)$ is an infinite line of $S$. Moreover, $\Delta_1(n, r) \subseteq \boldsymbol{e} + S$ if and only if also $\Delta_1(n - e_1, r)$ is an infinite line of $S$, and conversely $\Delta_1(n, r) \subseteq \mathbf{Ap}(S)$ if $\Delta_1(n - e_1, r)$ is not an infinite line of $S$ for any $r \in S_2$. It follows that for every $n$ there exists a unique $m \equiv n \bmod e_1$ such that $\Delta_1(m, r)$ is an infinite line of $\mathbf{Ap}(S)$. With the same argument it can be shown that the analogous situation happens on $S_2$ and therefore there are $e_2$ infinite lines of $\mathbf{Ap}(S)$ of the form $\Delta_2(q, t_i)$ corresponding to some elements $t_1, \ldots, t_{e_2} \in S_2$. Now, notice that, by Lemma 1(7), if an infinite line is contained in $\mathbf{Ap}(S)$, then its elements must be contained eventually in a level $A_i$. Moreover, by Lemma 1(8), $A_i$ cannot contain more than two infinite lines and, if it contains two of them, they must be one of the form $\Delta_1(s_1, r)$ and the other of the form $\Delta_2(q, s_2)$. Applying inductively the definition of the levels $A_i$, it follows that the levels $A_e, A_{e-1}, \ldots, A_{e-e_j+1}$ contain the $e_j$ infinite lines contained in $\mathbf{Ap}(S)$ and corresponding to the elements of $S_j$. $\square$

We conclude this section by proving a generalization of Remark 4 holding for good semigroups. We show that if $(R, \mathfrak{m}, k)$ is an analytically unramified one-dimensional local reduced ring, its quotient ring $R/(x)$, where $x$ is a nonzero element having minimal value in the value semigroup $S = v(R)$, can be generate as a $k$-vector space by a set of $e$ elements having values in all the different levels of the Apéry Set of $S$.

**Theorem 6.** *Let $(R, \mathfrak{m}, k)$ be an analytically unramified one-dimensional local reduced ring, having value semigroup $S = v(R)$ and let $x \in R$ such that $v(x) = \boldsymbol{e} = \min(S \setminus \{\mathbf{0}\})$. Let $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ be the Apéry Set of $S$. It is possible to construct a chain*

$$\boldsymbol{\alpha}_1 < \boldsymbol{\alpha}_2 < \ldots < \boldsymbol{\alpha}_e \in S$$

*such that $\alpha_i \in A_i$ and, for every collection of $f_i \in R$ having $v(f_i) = \alpha_i$,*

$$\frac{R}{(x)} = \langle \overline{f_1}, \overline{f_2}, \ldots, \overline{f_e} \rangle_k.$$

*Proof.* By Remark 5, the dimension over $k$ of $R/(x)$ is $e$, hence, we only need to show that, for $i = 1, \ldots, e$, we can find elements $\boldsymbol{\alpha}_i$ such that the correspondent $f_i$ are linearly independent over $k$.

We set $\boldsymbol{\alpha}_1 = \mathbf{0}$ and then we define the other elements $\boldsymbol{\alpha}_i$ using the following procedure: in case $\boldsymbol{\alpha}_i \ll \boldsymbol{\beta}$ for some $\boldsymbol{\beta} \in A_{i+1}$, we may simply set $\boldsymbol{\alpha}_{i+1} := \boldsymbol{\beta}$. Otherwise, if $\boldsymbol{\alpha}_i = \boldsymbol{\beta} \wedge \boldsymbol{\delta}$ with $\boldsymbol{\beta} \in \Delta_1^S(\boldsymbol{\alpha}_i) \cap A_{i+1}$ and $\boldsymbol{\delta} \in \Delta_2^S(\boldsymbol{\alpha}_i) \cap A_{i+1}$, by Lemma 2(2), we have $\Delta_h^S(\boldsymbol{\alpha}_i) \subseteq \mathbf{Ap}(S)$ and then we set $\boldsymbol{\alpha}_{i+1} := \boldsymbol{\beta}$ if $h = 2$ and $\boldsymbol{\alpha}_{i+1} := \boldsymbol{\delta}$ if $h = 1$ (if $\Delta^S(\boldsymbol{\alpha}_i) \subseteq \mathbf{Ap}(S)$ we can take indifferently one of them).

Now, taking $f_i \in R$ such that $v(f_i) = \boldsymbol{\alpha}_i \in \mathbf{Ap}(S)$, we clearly get by Proposition 2 that $\overline{f_i}$ is nonzero in $R/(x)$. Then we consider $v(\sum_{i=1}^{e} \lambda_i f_i)$ for $\lambda_i \in k$. Let $j$ be the minimal index such that $\lambda_j \neq 0$. If $\boldsymbol{\alpha}_j \ll \boldsymbol{\alpha}_{j+1}$, we obtain

$$v(\sum_{i=1}^{e} \lambda_i f_i) = v(\lambda_j f_j) = \boldsymbol{\alpha}_j \in \mathbf{Ap}(S)$$

and therefore $\sum_{i=1}^{e} \lambda_i \overline{f_i}$ is nonzero in $R/(x)$. Otherwise, we may assume $\boldsymbol{\alpha}_{j+1} \in \Delta_1^S(\boldsymbol{\alpha}_j)$, and hence, our procedure used to define the $\boldsymbol{\alpha}_i$ implies now that $\Delta_2^S(\boldsymbol{\alpha}_j) \subseteq \mathbf{Ap}(S)$. It follows that

$$v(\sum_{i=1}^{e} \lambda_i f_i) \in \Delta_2^S(\boldsymbol{\alpha}_j) \cup \{\boldsymbol{\alpha}_j\} \subseteq \mathbf{Ap}(S)$$

and thus $\sum_{i=1}^{e} \lambda_i \overline{f_i}$ is nonzero in $R/(x)$. □

## 4 Symmetric Good Semigroups

In this section we describe more properties of the Apéry Set of a good semigroup in the symmetric case.

**Definition 3.** A good semigroup $S$ is *symmetric* if, for every $\boldsymbol{\alpha} \in \mathbb{N}^2$, $\boldsymbol{\alpha} \in S$ if and only if $\Delta^S(\boldsymbol{\gamma} - \boldsymbol{\alpha}) = \emptyset$.

Symmetry is an interesting concept because, in the value semigroup case, it is equivalent to the Gorensteiness of the associated ring. Indeed, an analytically unramified one-dimensional local reduced ring is Gorenstein if and only if its value semigroup is symmetric. But more in general, a symmetric good semigroup has other nice properties, that we list in next proposition. Some of them have been already proved in [2, Proposition 3.2]. An interesting fact that we are proving is that it is possible to know the number of absolute elements of a symmetric good semigroup only looking at one of its (numerical) projections (Figure 5).

*Remark 7.* The projections of a symmetric good semigroup may fail to be symmetric numerical semigroups, as one can see for instance in Figure 6.

**Proposition 7** *Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a symmetric good semigroup, let $\boldsymbol{e} = (e_1, e_2)$, $\boldsymbol{\gamma} = (\gamma_1, \gamma_2)$ and* $\mathbf{Ap}(S)$ *be defined as previously.*

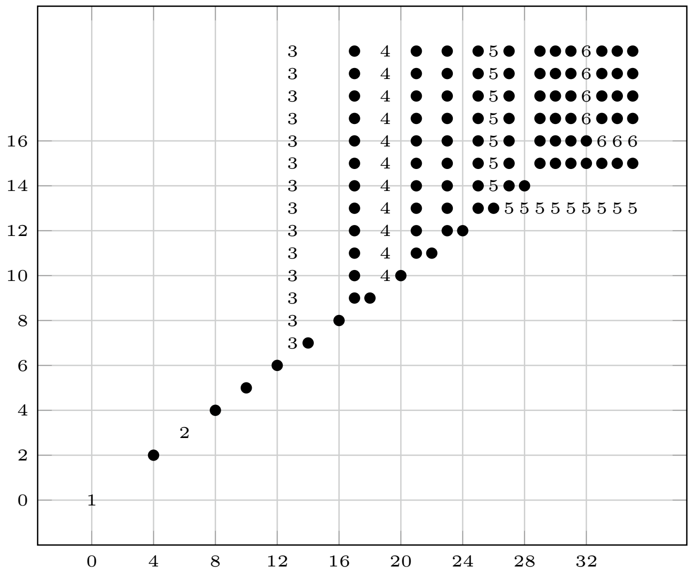



**Fig. 5** The symmetric value semigroup of $k[[X, Y]]/(Y^4 - 2X^3Y^2 - 4X^5Y + X^6 - X^7)(Y^2 - X^3)$, see [2, p. 8]. It is possible to observe that the number of absolute elements of this semigroup is $13 = 21 - 8 = 14 - 1$ as predicted by the formula in Proposition 7(2)

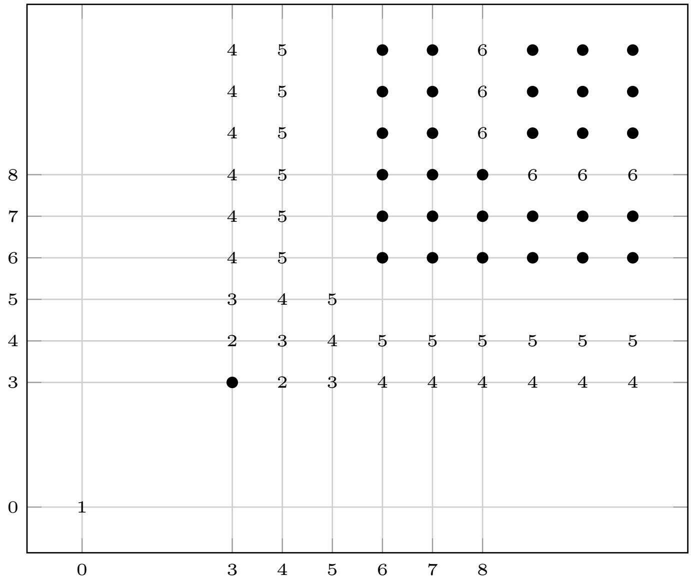


**Fig. 6** An example of a symmetric good semigroup whose projections are not symmetric numerical semigroups. It is a good example to check the duality property stated in Theorem 9

*(1) If $\boldsymbol{\alpha} \in S$ is a absolute element, then also $\boldsymbol{\gamma} - \boldsymbol{\alpha} \in S$ and it is a absolute element.*
*(2) The number of the absolute elements of $S$ is $n(S_1) - b(S_1) = n(S_2) - b(S_2)$, where $n(S_i) = |S_i \cap \{0, 1, \ldots, \gamma_i\}|$ and $b(S_i) = |\mathbb{N} \setminus S_i|$.*
*(3) For $\boldsymbol{\alpha} \in S$, $\boldsymbol{\alpha} \in \mathbf{Ap}(S)$ if and only if $\Delta^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) \neq \emptyset$.*
*(4) If $\boldsymbol{\alpha} \in \mathbf{Ap}(S)$, then $\Delta^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) \subseteq \mathbf{Ap}(S)$.*
*(5) Let $\boldsymbol{\alpha} \in \mathbb{N}^2$. If $\Delta^S(\boldsymbol{\alpha}) \subseteq \mathbf{Ap}(S)$ (possibly it is empty), then $\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha} \in S$.*
*(6) Let $\boldsymbol{\alpha} \in \mathbf{Ap}(S)$. Then for $i = 1, 2$; $\Delta_i^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) = \emptyset$ if and only if $\Delta_i^S(\boldsymbol{\alpha}) \nsubseteq \mathbf{Ap}(S)$.*

*Proof.* (1) Follows by the definitions of symmetric semigroup and absolute element.
(2) By definition of symmetric good semigroup, we have that $n \notin S_1$ if and only if $\Delta_1^S(n, 0) = \emptyset$, and if and only if $(\gamma_1 - n, \gamma_2 + m) \in S$ for every $m \geq 0$. It follows that the number of elements $s \in S_1$ such that $\Delta_1(s_1, r)$ is an infinite line of $S$ (for some $r \in S_2$) is exactly $b(S_1)$. Call $M$ the number of absolute elements of $S$. Hence,

$$\gamma_1 = M + 2b(S_1),$$

and, since $\gamma_1 = n(S_1) + b(S_1)$, we obtain $M = n(S_1) - b(S_1)$. In the same way, we can show $M = n(S_2) - b(S_2)$.
(3) An element $\boldsymbol{\alpha} \in S$ is in $\mathbf{Ap}(S)$ if and only if $\boldsymbol{\alpha} - \boldsymbol{e} \notin S$, and this happens by Definition 3 if and only if $\Delta^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) \neq \emptyset$.
(4) Since $\boldsymbol{\alpha} \in \mathbf{Ap}(S)$, $\Delta^S(\boldsymbol{\gamma} - \boldsymbol{\alpha}) = \emptyset$. It follows that $\Delta^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) \subseteq \mathbf{Ap}(S)$.

(5) If $\Delta^S(\boldsymbol{\alpha}) \subseteq \mathbf{Ap}(S)$, then by definition $\Delta^S(\boldsymbol{\alpha} - \boldsymbol{e}) = \emptyset$. and therefore $\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha} \in S$.
(6) We prove the result for $i = 1$. By (3) and (4), we have that $\Delta^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha})$ is not empty and contained in $\mathbf{Ap}(S)$. Assuming $\Delta_1^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) = \emptyset$, by axiom (G2) we get $\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha} \notin S$ and $\Delta_2^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) \neq \emptyset$. By (5), it follows that $\Delta^S(\boldsymbol{\alpha}) \nsubseteq \mathbf{Ap}(S)$ and moreover, since there exists $\boldsymbol{\omega} \in \Delta_2^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) \subseteq \mathbf{Ap}(S)$, we get by (4) $\Delta_2^S(\boldsymbol{\alpha}) \subseteq \Delta_2^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\omega}) \subseteq \mathbf{Ap}(S)$. Hence $\Delta_1^S(\boldsymbol{\alpha}) \nsubseteq \mathbf{Ap}(S)$.

Conversely, if $\Delta_1^S(\boldsymbol{\alpha}) \nsubseteq \mathbf{Ap}(S)$, there exists $\boldsymbol{\theta} \in \Delta_1^S(\boldsymbol{\alpha}) \cap (\boldsymbol{e} + S)$ and therefore, again by (3) $\Delta_1^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}) \subseteq \Delta_1^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\theta}) = \emptyset$. □

Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a good semigroup. We describe now, in the symmetric case, the absolute elements and the infinite lines of $\mathbf{Ap}(S)$ and of $\boldsymbol{e} + S$ in terms of the elements of a single projection, say $S_1$. For $n \in \mathbb{N}$, we consider the set

$$\Delta_1^S(n, 0) = \{(n, m) \in S \mid m \geq 0\}.$$

This set can be empty, finite or infinite. It is infinite if and only if $\Delta_1^S(n, r)$ is an infinite line of $S$ for some $r \in S_2$; it is finite if and only if $\Delta_1^S(n, 0)$ contains a absolute element of $S$; it is empty if and only if $n \notin S_1$. The analogous situation holds for the other projection $S_2$.

**Lemma 3.** *The set $\Delta_1^S(n, 0) \subseteq \mathbf{Ap}(S)$ if and only if $n \in \mathbf{Ap}(S_1)$.*

*Proof.* We have $n \in \mathbf{Ap}(S_1)$ if and only if $n - e_1 \notin S_1$ if and only if $\Delta_1^S(n - e_1, 0) = \emptyset$. The result now follows from the definition of $\mathbf{Ap}(S)$. □

**Theorem 8.** *Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a symmetric good semigroup, let $\boldsymbol{e} = (e_1, e_2)$ be its minimal nonzero element. Let $n \in \mathbb{N}$ and define $n' = \gamma_1 + e_1 - n$.*

*(1) $\Delta_1^S(n, 0) = \emptyset$ if and only if $\Delta_1^S(n', 0)$ is infinite and eventually contained in $\boldsymbol{e} + S$.*
*(2) $\Delta_1^S(n, 0)$ is finite with maximal element in $\boldsymbol{e} + S$ if and only if $\Delta_1^S(n', 0)$ is finite with maximal element in $\boldsymbol{e} + S$.*
*(3) $\Delta_1^S(n, 0) \nsubseteq \mathbf{Ap}(S)$ and it is finite with maximal element in $\mathbf{Ap}(S)$ if and only if $\Delta_1^S(n', 0) \nsubseteq \mathbf{Ap}(S)$ and it is finite with maximal element in $\mathbf{Ap}(S)$.*
*(4) $\Delta_1^S(n, 0) \subseteq \mathbf{Ap}(S)$ and it is finite if and only if $\Delta_1^S(n', 0)$ is infinite and eventually contained in $\mathbf{Ap}(S)$ but it contains some element of $\boldsymbol{e} + S$.*
*(5) $\Delta_1^S(n, 0) \subseteq \mathbf{Ap}(S)$ and it is infinite if and only if $\Delta_1^S(n', 0) \subseteq \mathbf{Ap}(S)$ and it is infinite.*

*All the correspondent statements hold replacing $S_1$ with $S_2$.*

*Proof.* (1) Observe that $\Delta_1^S(n, 0) = \emptyset$ if and only if $\Delta^S(n, -m) = \emptyset$ for all $m \geq 0$. This is equivalent by Definition 3 to say that $(\gamma_1 - n, \gamma_2 + m) \in S$. Hence $\Delta_1^S(n, 0) = \emptyset$ if and only if $\Delta_1^S(\gamma_1 - n, 0)$ is infinite, which is equivalent to say that $\Delta_1^S(\gamma_1 + e_1 - n, 0) = \Delta_1^S(n', 0)$ is infinite and contained in $\boldsymbol{e} + S$.
(2) Let $\boldsymbol{\alpha} \in \boldsymbol{e} + S$ be the maximal element of $S$ belonging to $\Delta_1^S(n, 0)$. Hence $\boldsymbol{\alpha}$ is an absolute element and, by Proposition 7(1) $\boldsymbol{\gamma} - \boldsymbol{\alpha}$ is also an absolute element of $S$. It

follows that $\boldsymbol{\alpha}' = \boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha} \in \boldsymbol{e} + S$. Moreover, since $\boldsymbol{\alpha} \in \boldsymbol{e} + S$, $\Delta^S(\boldsymbol{\alpha}') = \emptyset$ by Proposition 7(3). Thus $\boldsymbol{\alpha}'$ is a absolute element and $\Delta_1^S(n', 0)$ is finite with maximal element in $\boldsymbol{e} + S$. The converse is tautological.
(3) Let $\Delta_1^S(n, 0) \nsubseteq \mathbf{Ap}(S)$ and it is finite with maximal element $\boldsymbol{\alpha} = (n, m) \in \mathbf{Ap}(S)$. As in (2), we have that $\boldsymbol{\alpha}' = \boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha} \in \boldsymbol{e} + S$. But, by exclusion, (1) and (2) imply that $\Delta_1^S(n', 0)$ neither is infinite and eventually contained $\boldsymbol{e} + S$ nor has a maximal in $\boldsymbol{e} + S$. Hence there must exist $\boldsymbol{\beta} = (n', r) \in \mathbf{Ap}(S)$ with $r > m' := \gamma_2 + e_2 - m$. We conclude saying that, since $\Delta_1^S(n, 0) \nsubseteq \mathbf{Ap}(S)$, there must exist an element $\boldsymbol{\delta} = (n, d) \in \boldsymbol{e} + S$ with $d < m$ and hence $\Delta^S(\boldsymbol{\delta}') = \emptyset$. Thus there are only finite elements $(n', q) \in S$ with $q > m'$ and they are all in $\mathbf{Ap}(S)$ by Proposition 7(4), since they are elements of $\Delta^S(\boldsymbol{\alpha}')$. Since there exists at least one of such elements, namely $\boldsymbol{\beta}$, the thesis follows.
(4) Assume that $\Delta_1^S(n, 0) \subseteq \mathbf{Ap}(S)$ and it is finite. Again by (1) and (2) we exclude that $\Delta_1^S(n', 0)$ is infinite and eventually contained $\boldsymbol{e} + S$ or has a maximal in $\boldsymbol{e} + S$. Let $\boldsymbol{\alpha} = (n, m) \in \mathbf{Ap}(S)$ be the maximal element in $\Delta_1^S(n, 0)$. We proceed like in the proof of (3) to say that $\boldsymbol{\alpha}' = \boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha} \in \boldsymbol{e} + S$. If by way of contradiction $\Delta_1^S(n', 0)$ contains a maximal element $\boldsymbol{\theta} \in \mathbf{Ap}(S)$, it would follow by Proposition 7(3 and 5) that $\boldsymbol{\theta}' \in \Delta_1^S(n, 0) \cap (\boldsymbol{e} + S)$ and this is a contradiction.

Conversely, assume $\Delta_1^S(n', 0)$ is infinite and eventually contained in $\mathbf{Ap}(S)$ but it contains some element $\boldsymbol{\theta} \in \boldsymbol{e} + S$. Since $\Delta^S(\boldsymbol{\theta}') = \emptyset$ (by Proposition 7(3)), $\Delta_1^S(n, 0)$ must be finite. We conclude by exclusion, since we characterized in (2) and (3) the other possible cases of a finite $\Delta_1^S(n, 0)$.
(5) It follows since we excluded all the other possible cases in (1),(2),(3), and (4). □

**Corollary 1.** *Assume the same notations of Theorem 8. Hence,* $n \in \mathbf{Ap}(S_1)$ *if and only if* $\Delta_1^S(n', 0)$ *is infinite and eventually contained in* $\mathbf{Ap}(S)$.

## 5 Duality of the Apéry Set of Symmetric Good Semigroups

The symmetry of a numerical semigroup $S$ can be characterized by the symmetry of its Apéry Set with respect to its largest element: if we order the elements of $\mathbf{Ap}(S)$ in increasing order $\mathbf{Ap}(S) = \{w_1, \dots, w_e\}$, then $S$ is symmetric if and only if $w_i + w_{e-i+1} = w_e$.

Hence, there is a duality relation associating to each element $w_i$, the element $w_{e-i+1}$. In the case of a symmetric good semigroup we do not have this relation by choosing arbitrary elements, one from each level $A_i$ of $\mathbf{Ap}(S)$; but we find a more general duality relation associating the level $A_i$ to the level $A_{e-i+1}$, and involving both the elements of $\boldsymbol{\alpha} \in A_i$ and the sets $\Delta^S(\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha})$. After two preparatory lemmas, we define and prove this duality in Theorem 9.

In this Section, we denote as before $\boldsymbol{\alpha}' := \boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}$.

**Lemma 4.** *Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a symmetric good semigroup. Let* $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ *be the Apéry Set of S. If $\boldsymbol{\alpha} \in A_{e-i+1}$, then for every $j < i$,*

$$\Delta^S(\boldsymbol{\alpha}') \cap A_j = \emptyset.$$

*Proof.* We use induction on $i$. For $i = 1$, the result is clear. Let $\boldsymbol{\alpha} \in A_{e-i+1}$. We separate the proof in two cases:

**Case 1**: Assume $\boldsymbol{\alpha} \ll \boldsymbol{\theta}$ for some $\boldsymbol{\theta} \in A_{e-i+2}$. By inductive hypothesis $\Delta^S(\boldsymbol{\theta}') \cap A_j = \emptyset$ for every $j < i - 1$. Since $\boldsymbol{\alpha} \ll \boldsymbol{\theta}$, it follows that $\boldsymbol{\theta}' \ll \boldsymbol{\alpha}'$ and hence for every $\boldsymbol{\delta} \in \Delta^S(\boldsymbol{\alpha}')$ there exists $\boldsymbol{\beta} \in \Delta^S(\boldsymbol{\theta}')$ such that either $\boldsymbol{\beta} \ll \boldsymbol{\delta}$ or there exists $\boldsymbol{\omega} = \boldsymbol{\delta} \wedge \boldsymbol{\beta} \in \Delta^S(\boldsymbol{\theta}') \subseteq \mathbf{Ap}(S)$. In the first case the level of $\boldsymbol{\beta}$ in $\mathbf{Ap}(S)$ is smaller than the level of $\boldsymbol{\delta}$. In the second case, as a consequence of Lemma 2(3), the element $\boldsymbol{\omega}$ is in a level of $\mathbf{Ap}(S)$ smaller than the level of $\boldsymbol{\delta}$. Hence we can find elements in $\Delta^S(\boldsymbol{\theta}')$ in some level smaller than the level of any element of $\Delta^S(\boldsymbol{\alpha}')$. It follows that $\Delta^S(\boldsymbol{\alpha}') \subseteq \bigcup_{j \geq i} A_j$ and hence the thesis.

**Case 2**: Now assume $\boldsymbol{\alpha} = \boldsymbol{\theta} \wedge \boldsymbol{\delta}$ with $\boldsymbol{\theta} \in \Delta_1^S(\boldsymbol{\alpha}) \cap A_{e-i+2}$ and $\boldsymbol{\delta} \in \Delta_2^S(\boldsymbol{\alpha}) \cap A_{e-i+2}$. Hence $\boldsymbol{\alpha}' \in \Delta_1(\boldsymbol{\theta}') \cap \Delta_2(\boldsymbol{\delta}')$. Assuming $\Delta_1^S(\boldsymbol{\alpha}') \neq \emptyset$ and taking $\boldsymbol{\omega} \in \Delta_1^S(\boldsymbol{\alpha}')$, we can find an element $\boldsymbol{\beta} \in \Delta^S(\boldsymbol{\delta}')$ such that either $\boldsymbol{\beta} \ll \boldsymbol{\omega}$ or there exists $\boldsymbol{\beta}^1 = \boldsymbol{\omega} \wedge \boldsymbol{\beta} \in \Delta^S(\boldsymbol{\delta}') \subseteq \mathbf{Ap}(S)$ (it is possible to have $\boldsymbol{\beta}^1 = \boldsymbol{\alpha}'$). Using the same argument of Case 1, we show that one element among $\boldsymbol{\beta}$ and $\boldsymbol{\beta}^1$ is in a level of $\mathbf{Ap}(S)$ smaller than the level of $\boldsymbol{\omega}$ and therefore we get the same thesis of Case 1. In case $\Delta_2^S(\boldsymbol{\alpha}') \neq \emptyset$ we can use the same argument to find the needed elements in $\Delta^S(\boldsymbol{\theta}')$. □

**Lemma 5.** *Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a symmetric good semigroup. Let* $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ *be the Apéry Set of S. If $\boldsymbol{\alpha} \in A_i$, then*

$$\Delta^S(\boldsymbol{\alpha}') \cap A_{e-i+1} \neq \emptyset.$$

*Proof.* Again we use induction on $i$. For $i = 1$, the result follows since $A_1 = \{\mathbf{0}\}$ and $\Delta^S(\mathbf{0}') = \Delta^S(\boldsymbol{\gamma} + \boldsymbol{e}) = A_e$. Let $\boldsymbol{\alpha} \in A_i$. By Lemma 4, we have that $\Delta^S(\boldsymbol{\alpha}') \subseteq \bigcup_{j \geq e-i+1} A_j$. By Proposition 4 we have that $\boldsymbol{\alpha} \geq \boldsymbol{\theta}$ for some $\boldsymbol{\theta} \in A_{i-1}$. We separate the proof in two cases:

**Case 1**: Assume $\boldsymbol{\alpha} \gg \boldsymbol{\theta}$. By inductive hypothesis, we know that there exists $\boldsymbol{\beta} \in \Delta^S(\boldsymbol{\theta}') \cap A_{e-i+2}$. Using the argument of the proof of Lemma 4 (Case 1) we can show that there exists some element $\boldsymbol{\omega} \in \Delta^S(\boldsymbol{\alpha}')$ which is in a level of $\mathbf{Ap}(S)$ smaller than $A_{e-i+2}$. Thus we must have $\boldsymbol{\omega} \in A_{e-i+1}$.

**Case 2**: Now assume $\boldsymbol{\alpha} \in \Delta^S(\boldsymbol{\theta})$. Without loss of generality, we say that $\boldsymbol{\alpha} \in \Delta_1^S(\boldsymbol{\theta})$. Now, if $\Delta_1^S(\boldsymbol{\theta}) \nsubseteq \mathbf{Ap}(S)$, by Proposition 7(6) we have $\Delta_1^S(\boldsymbol{\theta}') = \emptyset$ and therefore $\Delta_2^S(\boldsymbol{\theta}') \neq \emptyset$. Otherwise, if $\Delta_1^S(\boldsymbol{\theta}) \subseteq \mathbf{Ap}(S)$, applying Lemma 2(5) we find an element $\boldsymbol{\omega} \in (\Delta_1^S(\boldsymbol{\theta}) \cap A_{i-1}) \cup \{\boldsymbol{\theta}\}$ such that $\Delta_2^S(\boldsymbol{\omega}) \subseteq \mathbf{Ap}(S)$ and hence again by Proposition 7(6), $\Delta_2^S(\boldsymbol{\omega}') \neq \emptyset$. In both cases we have found an element $\boldsymbol{\omega} \in A_{i-1}$ such that $\boldsymbol{\alpha} \in \Delta_1^S(\boldsymbol{\omega})$ and $\Delta_2^S(\boldsymbol{\omega}') \neq \emptyset$. Proceeding like in Case 2 of Lemma 4 and using the inductive hypothesis, we find an element $\boldsymbol{\beta} \in \Delta^S(\boldsymbol{\alpha}')$ which is in a level of $\mathbf{Ap}(S)$ smaller than $A_{e-i+2}$. Thus we must have $\boldsymbol{\beta} \in A_{e-i+1}$ as in Case 1. □

**Theorem 9.** *Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a good semigroup. Let $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ be the Apéry Set of $S$. Denote*

$$A'_i = \left( \bigcup_{\boldsymbol{\omega} \in A_i} \Delta^S(\boldsymbol{\omega}') \right) \setminus \left( \bigcup_{\boldsymbol{\omega} \in A_j,\ j<i} \Delta^S(\boldsymbol{\omega}') \right).$$

*The following assertions are equivalent:*

1. *$S$ is symmetric.*
2. *$A'_i = A_{e-i+1}$ for every $i = 1, \ldots, e$.*

*Proof.* (1) → (2): Assume $S$ to be symmetric and notice that in this case by Proposition 7(4), $A'_i \subseteq \mathbf{Ap}(S)$. As a consequence of the definition of the levels, $A'_e = A_1$ and $A'_1 = A_e$, thus we can assume by induction $A'_j = A_{e-j+1}$ for $j < i$ and $A_j = A'_{e-j+1}$ for $j > e - i + 1$.

We first show $A'_i \subseteq A_{e-i+1}$. Let $\boldsymbol{\delta} \in A'_i$, hence $\boldsymbol{\delta} \in \Delta^S(\boldsymbol{\omega}')$ for some $\boldsymbol{\omega} \in A_i$ and $\boldsymbol{\delta} \notin \bigcup_{\boldsymbol{\theta} \in A_j,\ j<i} \Delta^S(\boldsymbol{\theta}')$. Since $\boldsymbol{\omega} \in A_i$, by Lemma 4, $\boldsymbol{\delta} \notin A_j$ for $j < e - i + 1$. By way of contradiction assume $\boldsymbol{\delta} \in A_j$ for some $j > e - i + 1$. Thus, by inductive hypothesis $A_j = A'_{e-j+1}$ and $e - j + 1 < i$. Hence $\boldsymbol{\delta} \in \Delta^S(\boldsymbol{\theta}')$ for some $\boldsymbol{\theta} \in A_{e-j+1}$, but this is a contradiction since $\boldsymbol{\delta} \in A'_i$ and $e - j + 1 < i$.

Now we show the other containment $A_{e-i+1} \subseteq A'_i$. Let $\boldsymbol{\omega} \in A_{e-i+1}$ and take $\boldsymbol{\delta} \in \Delta^S(\boldsymbol{\omega}') \cap A_i$ which does exist by Lemma 5. Hence $\boldsymbol{\omega} \in \Delta^S(\boldsymbol{\delta}')$. We need to prove that $\boldsymbol{\omega} \notin \Delta^S(\boldsymbol{\theta}')$ for every $\boldsymbol{\theta} \in A_j$ with $j < i$. If by way of contradiction, we assume $\boldsymbol{\omega} \in \Delta^S(\boldsymbol{\theta}')$ for some $\boldsymbol{\theta} \in A_j$ with $j < i$, we can take a minimal $j$ such that this happens, and hence by definition of $A'_j$ and by inductive hypothesis, we get $\boldsymbol{\omega} \in A'_j = A_{e-j+1} = A_h$ with $h > e - i + 1$. But this is impossible since the levels of $\mathbf{Ap}(S)$ are disjoint. With the same proof it is possible to show that $A_i = A'_{e-i+1}$ and continue with the induction to prove (2).

(2) → (1): We argue by way of contradiction. Assuming that $S$ is not symmetric, we can find $\boldsymbol{\alpha} \notin S$ such that $\Delta^S(\boldsymbol{\gamma} - \boldsymbol{\alpha}) = \emptyset$. Since there exists a minimal $k \in \mathbb{N}$ such that $\boldsymbol{\alpha} + k\boldsymbol{e} \in S$ and for every $k$, also $\Delta^S(\boldsymbol{\gamma} - \boldsymbol{\alpha} - k\boldsymbol{e}) = \emptyset$, we may assume, replacing $\boldsymbol{\alpha}$ by $\boldsymbol{\alpha} + k\boldsymbol{e}$, that $\boldsymbol{\alpha} + \boldsymbol{e} \in \mathbf{Ap}(S)$. Assuming $\boldsymbol{\alpha} + \boldsymbol{e} \in A_i$, we show that $\boldsymbol{\alpha} + \boldsymbol{e} \notin A'_j$ for every $j$, and therefore $A_i \neq A'_{e-i+1}$. Indeed,

$$\emptyset = \Delta^S(\boldsymbol{\gamma} - \boldsymbol{\alpha}) = \Delta^S(\boldsymbol{\gamma} + \boldsymbol{e} - (\boldsymbol{\alpha} + \boldsymbol{e}))$$

and, if $\boldsymbol{\alpha} + \boldsymbol{e} \in \Delta^S(\boldsymbol{\beta}')$ for some $\boldsymbol{\beta} \in \mathbf{Ap}(S)$, we would have $\boldsymbol{\beta} \in \Delta^S(\boldsymbol{\gamma} + \boldsymbol{e} - (\boldsymbol{\alpha} + \boldsymbol{e}))$ and this is a contradiction. □

**Corollary 2.** *Let $S \subseteq \mathbb{N}^2$ be a symmetric good semigroup and let $\boldsymbol{\alpha} \in A_{e-i+1}$. The minimal elements of $\Delta^S(\boldsymbol{\alpha}')$ with respect to $\leq$ are in $A_i$.*

*Proof.* By Lemma 4, for every $j < i$, $\Delta^S(\boldsymbol{\alpha}') \cap A_j = \emptyset$, while by Lemma 5, $\Delta^S(\boldsymbol{\alpha}') \cap A_i \neq \emptyset$. Hence there exists a minimal element $\boldsymbol{\beta}$ of $\Delta^S(\boldsymbol{\alpha}')$ in $A_i$. If $\boldsymbol{\theta}$ is another minimal element of $\Delta^S(\boldsymbol{\alpha}')$, we clearly have $\boldsymbol{\alpha}' = \boldsymbol{\beta} \wedge \boldsymbol{\theta} \in S$, and hence $\boldsymbol{\theta} \in A_i$ by Lemma 2(3). □

In the next theorem, we provide a specific sequence of elements of a good semigroup $S$, taken one from each level $A_i$, behaving like the elements of the Apéry Set of a numerical semigroup with respect to sums. Notice that this sequence may not be the unique having the required property, but we give here a canonical way to construct one.

**Theorem 10.** *Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a symmetric good semigroup and let $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ be the Apéry Set of $S$. Assume $e_1 \geq e_2$.*

*1. If $e$ is even, there exists a sequence of elements $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_e$ such that*

$$\boldsymbol{\alpha}_i \in A_i$$

*and*

$$\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_{e-i+1} = \boldsymbol{\alpha}_e.$$

*2. If $e$ is odd, set $e = 2d - 1$. Then, there exists a sequence of elements $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_e, \boldsymbol{\beta}$ such that*

$$\boldsymbol{\alpha}_i \in A_i, \; \boldsymbol{\beta} \in A_d$$

*and*

$$\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_{e-i+1} = \boldsymbol{\alpha}_e$$

*for $i \neq d$, and moreover*

$$\boldsymbol{\alpha}_d + \boldsymbol{\beta} = \boldsymbol{\alpha}_e$$

*Proof.* Let $\mathbf{Ap}(S_1) = \{\omega_1 = 0, \omega_2, \ldots, \omega_{e_1}\}$ be the Apéry Set of $S_1$ with elements listed in increasing order. For $i = 1, \ldots, e_1$ set

$$\boldsymbol{\alpha}_i := \min \Delta_1^S(\omega_i, 0).$$

We observe that, defined in this way, $\boldsymbol{\alpha}_i \in A_i$, since, by Corollary 1, the set $\Delta_1^S(\omega_i', 0)$ is eventually contained in $\mathbf{Ap}(S)$ and in particular, by Theorem 5 it is eventually contained in $A_{e-i+1}$. Hence, we get $\boldsymbol{\alpha}_i \in A_i$ by Corollary 2. Moreover, there exists a minimal $h_i \geq 0$ such that $\boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}_i + (0, h_i) \in A_{e-i+1}$.

Call $H := \max\{h_i\}$ and define again for $i = 1, \ldots, e_1$,

$$\boldsymbol{\alpha}_{e-i+1} := \boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}_i + (0, H).$$

It follows that $\boldsymbol{\alpha}_{e-i+1} \in A_{e-i+1}$ and that $\boldsymbol{\alpha}_i + \boldsymbol{\alpha}_{e-i+1} = \boldsymbol{\gamma} + \boldsymbol{e} + (0, H) = \boldsymbol{\alpha}_e$. The second assertion is proved in the same way by defining $\boldsymbol{\beta} := \boldsymbol{\gamma} + \boldsymbol{e} - \boldsymbol{\alpha}_d + (0, H)$. □

We conclude giving a quite surprising result about symmetric good semigroup with large conductor.

**Proposition 11** *Let $S \subseteq S_1 \times S_2 \subseteq \mathbb{N}^2$ be a symmetric good semigroup and let $\mathbf{Ap}(S) = \bigcup_{i=1}^{e} A_i$ be the Apéry Set of $S$. Assume $e_1 \geq e_2$ and*

$$\gamma_1 > 2f(S_1) + e_1$$

*where $f(S_1)$ denotes the Frobenius number of $S_1$. Then, $e_1 = e_2$.*

*Proof.* Set $\mathbf{Ap}(S_1) = \{\omega_1 = 0, \omega_2, \dots, \omega_{e_1}\}$ with elements listed in increasing order. In the proof of Theorem 10 is shown that $\boldsymbol{\alpha}_i = \min \Delta_1^S(\omega_i, 0) \in A_i$ and moreover by Theorem 9, any element $\boldsymbol{\theta} = (\gamma_1 + e_1 - \omega_i, t_2)$, with $t_2 \geq \gamma_2 + e_2$, is in $A_{e-i+1}$ that is an infinite level by Corollary 1. Since by assumption,

$$\omega_{e_1} = f(S_1) + e_1 < \gamma_1 + e_1 - (f(S_1) + e_1) = \omega'_{e_1},$$

we get $\boldsymbol{\alpha}_{e_1} \ll \boldsymbol{\theta} \in A_{e-e_1+1}$ and therefore $e_1 < e - e_1 + 1 = e_2 + 1$, since by Theorem 3, $e = e_1 + e_2$. It follows that $e_1 = e_2$. □

## References


1. Barucci, V., D'Anna, M., Fröberg, R.: Analytically unramified one-dimensional semilocal rings and their value semigroups. J. Pure Appl. Alg. **147**, 215–254 (2000)
2. Barucci, V., D'Annae, M., Fröberg, R.: The Apéry algorithm for a plane singularity with two branches. Beitrage zur Algebra und Geometrie **46**(1) (2005)
3. Barucci, V., D'Anna, M., Fröberg, R.: The semigroup of values of a one-dimensional local ring with two minimal primes. Comm. Algebra **28**(8), 3607–3633 (2000)
4. Bryant, L.: Goto numbers of a numerical semigroup ring and the gorensteinness of associated graded rings. Comm. Alg. **38**(6), 2092–2128 (2010)
5. Campillo, A., Delgado, F., Gusein-Zade, S.M.: On generators of the semigroup of a plane curve singularity. J. London Math. Soc. **60**(2), 420–430 (1999)
6. Campillo, A., Delgado, F., Kiyek, K.: Gorenstein properties and symmetry for one-dimensional local Cohen-Macaulay rings. Manuscripta Math. **83**, 405–423 (1994)
7. Carvalho, E., Hernandes, M.E.: The semiring of values of an algebroid curve (2017). arXiv:1704.04948v1
8. Cortadellas, T., Jafari, R., Zarzuela, S.: On the Apery sets of monomial curves. Semigroup Forum **86**(2), 289–320 (2013)
9. D'Anna, M.: The canonical module of a one-dimensional reduced local ring. Comm. Algebra **25**, 2939–2965 (1997)
10. D'Anna, M., Garcia Sanchez, P., Micale, V., Tozzo, L.: Good semigroups of $N^n$. Int. J. Algebra Comput. **28**, 179–206 (2018)
11. D'Anna, M., Jafari, R., Strazzanti, F.: Tangent cones of monomial curves obtained by numerical duplication (2018). arXiv:1803.08302
12. D'Anna, M., Micale, V., Sammartano, A.: When the associated graded ring of a semigroup ring is Complete Intersection. J. Pure Appl. Algebra **217**, 1007–1017 (2013)

13. Delgado, F.: The semigroup of values of a curve singularity with several branches. Manuscripta Math. **59**, 347–374 (1987)
14. Delgado, F.: Gorenstein curves and symmetry of the semigroup of value, Manuscripta Math. **61**, 285–296. Springer, Perspectives (1988)
15. García, A.: Semigroups associated to singular points of plane curves. J. Reine Angew. Math. **336**, 165–184 (1982)
16. Jäger, J.: Längenberechnung und kanonische Ideale in eindimensionalen Ringen. Arch. Math. (Basel) **29**(5), 504–512 (1977)
17. Korell, P., Schulze, M., Tozzo, L.: Duality on value semigroups. arXiv:1510.04072
18. Kunz, E.: The value-semigroup of a one-dimensional Gorenstein ring. Proc. Amer. Math. Soc. **25**, 748–751 (1970)

# On Syzygies for Rings of Invariants of Abelian Groups

**M. Domokos**

**Abstract** It is well known that results on zero-sum sequences over a finitely generated abelian group can be translated to statements on generators of rings of invariants of the dual group. Here the direction of the transfer of information between zero-sum theory and invariant theory is reversed. First it is shown how a presentation by generators and relations of the ring of invariants of an abelian group acting linearly on a finite-dimensional vector space can be obtained from a presentation of the ring of invariants for the corresponding multiplicity free representation. This combined with a known degree bound for syzygies of rings of invariants yields bounds on the presentation of a block monoid associated to a finite sequence of elements in an abelian group. The results have an equivalent formulation in terms of binomial ideals, but here the language of monoid congruences and the notion of catenary degree is used.

**Keywords** Affine monoid · Ring of invariants · Catenary degree · Syzygies · Toric variety

## 1 Introduction

Let $G$ be an abelian group (written multiplicatively) and $G_0 \subseteq G$ a finite subset. Consider the additive monoid $\mathbb{N}_0^{G_0}$ (maps from $G_0$ into the set of non-negative integers, with pointwise addition). It contains the submonoid

$$\mathcal{B}(G_0) := \{\alpha \in \mathbb{N}_0^{G_0} \mid \prod_{g \in G_0} g^{\alpha(g)} = 1 \in G\} \tag{1}$$

This research was partially supported by National Research, Development and Innovation Office, NKFIH K 119934.

M. Domokos (✉)
Rényi Institute, Budapest, Hungary
e-mail: domokos.matyas@renyi.hu



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_5

called the *block monoid of* $G_0$ or the *monoid of product-one sequences over* $G_0$, see [14, Definition 3.4.1]. It causes no loss of generality in the construction of $\mathcal{B}(G_0)$ if we assume that the group $G$ is generated by $G_0$. We note that in most of the related literature the group is written additively, and therefore the terminology of *zero-sum sequences* is used. $\mathcal{B}(G_0)$ is a reduced affine monoid (see for example [14, Theorem 3.4.2.1]), write $\mathcal{A}(\mathcal{B}(G_0))$ for the finite set of its atoms.

Our focus is on a similar but more general construction. Fix an $m$-tuple $\underline{g} = (g_1, \dots, g_m) \in G^m$ of elements of the abelian group $G$, and set

$$\mathcal{B}(\underline{g}) = \{\alpha \in \mathbb{N}_0^m \mid \prod_{i=1}^{m} g_i^{\alpha_i} = 1 \in G\}. \tag{2}$$

This is a finitely generated submonoid of the additive monoid $\mathbb{N}_0^m$. Write $\mathrm{supp}(\underline{g})$ for the subset $\{g_1, \dots, g_m\}$ of $G$. In the special case when $g_1, \dots, g_m$ are distinct, the monoid $\mathcal{B}(\underline{g})$ can be identified with $\mathcal{B}(\mathrm{supp}(\underline{g}))$. In general (i.e., when $g_1, \dots, g_m$ are not all distinct) the monoid $\mathcal{B}(\underline{g})$ is different from $\mathcal{B}(\mathrm{supp}(\underline{g}))$. So the construction (2) is indeed a generalization of (1) (however, see Remark 6 in Section 4).

Interest in the monoids $\mathcal{B}(G_0)$ and $\mathcal{B}(\underline{g})$ and their semigroup rings comes from several mathematical topics: factorization theory in monoids, multiplicative ideal theory, zero-sum theory, invariant theory, toric varieties, binomial or toric ideals. For example, it has been long known that results on the atoms in monoids of the form $\mathcal{B}(\underline{g})$ can be reformulated in terms of generators or degree bounds for rings of invariants of abelian groups (see, e.g., [9] for some details and references).

In this paper we shall study presentations of reduced affine monoids, with a particular attention on the monoids $\mathcal{B}(\underline{g})$. By a *monoid* we mean a commutative cancellative semigroup with an identity element. A monoid is *affine* if it is a finitely generated submonoid of a finitely generated free abelian group. We say that a monoid is *reduced* if the identity element is its only unit (invertible element). Recall that by Grillet's theorem, reduced affine monoids are exactly the monoids that are isomorphic to a finitely generated submonoid of the additive monoid $\mathbb{N}_0^k$ for some $k$ (see for example [3, Proposition 2.16]).

Let $S$ be a reduced affine monoid (written multiplicatively) and $\mathcal{A}(S)$ the set of atoms in $S$. Then $\mathcal{A}(S)$ is finite, and it is a minimal generating set of $S$, see for example Proposition 1.1.7 in [14]. Denote by $\mathbb{N}_0^{\mathcal{A}(S)}$ the additive monoid of functions from $\mathcal{A}(S)$ into the additive monoid $\mathbb{N}_0$ of non-negative integers; this is a free monoid generated by $|\mathcal{A}(S)|$ elements. Take commuting indeterminates $\{x_a \mid a \in \mathcal{A}(S)\}$, and let $M$ denote the free monoid generated by them (written multiplicatively):

$$M = \{x^\alpha = \prod_{a \in \mathcal{A}(S)} x_a^{\alpha(a)} \mid \alpha \in \mathbb{N}_0^{\mathcal{A}(S)}\}$$

with multiplication $x^\alpha x^\gamma = x^{\alpha+\gamma}$. Consider the unique semigroup homomorphism

$$\pi : M \to S \text{ given by } x_a \mapsto a, \quad a \in \mathcal{A}(S)$$

(called *factorization homomorphism* in [1]). Denote by $\sim_S$ the congruence on $M$ defined by

$$x^\alpha \sim_S x^\gamma \iff \pi(x^\alpha) = \pi(x^\gamma) \in S,$$

and call it the *defining congruence of S* (it is called *the monoid of relations of S* in [1]). The semigroup homomorphism $\pi$ factors through a monoid isomorphism

$$M/\sim_S \stackrel{\cong}{\longrightarrow} S.$$

Formally the congruence $\sim_S$ will be viewed as a subset of $M \times M$. The congruence $\sim_S$ is finitely generated by [25]. By a *presentation* of $S$ we mean a finite subset of $M \times M$ generating the conguence $\sim_S$ (see for example [16, Section I.4] for basic notions related to semigroup congruences).

Now let us summarize the content of the present paper. Our Theorem 1 tells in particular how a presentation of $\mathcal{B}(\underline{g})$ can be derived from a presentation of $\mathcal{B}(\mathrm{supp}(\underline{g}))$. It turns out that in most cases the catenary degree (cf. Definition 1) of $\mathcal{B}(\underline{g})$ coincides with the catenary degree of $\mathcal{B}(\mathrm{supp}(\underline{g}))$ (see Corollary 3). Combining Theorem 1 with a degree bound of Derksen [10] for the defining relations of the ring of invariants of a linearly reductive group, we derive in Theorem 4 degree bounds for a presentation of $\mathcal{B}(\underline{g})$. In order to formulate this result, we introduce the notion of graded catenary degree of a graded monoid (see Definition 2), which is a refinement of (and an upper bound for) the ordinary catenary degree. These results on presentations of monoids have an equivalent formulation in terms of generators of (binomial) ideals of relations of semigroup rings of monoids, this is pointed out in Section 2. A Gröbner basis version of Theorem 1 is given in Theorem 2. Since the semigroup rings of the form $\mathbb{C}[\mathcal{B}(G)]$ are exactly the rings of invariants of abelian groups, the results have relevance for toric varieties; this is expanded a bit in Section 7, and some examples of toric quiver varieties are reviewed. We point out finally that Theorem 2 provides a source of Koszul algebras.

## 2 Ring Theoretic Characterization of the Catenary Degree

From now on $S$ will be a reduced affine monoid. The *catenary degree* $c(S)$ of the monoid $S$ is a basic arithmetical invariant studied in factorization theory, let us recall its definition. For $\alpha \in \mathbb{N}_0^{\mathcal{A}(S)}$ we set

$$|\alpha| = \sum_{a \in \mathcal{A}(S)} |\alpha(a)|$$

and

$$a^\alpha := \prod_{a \in \mathcal{A}(S)} a^{\alpha(a)} \in S.$$

For $\alpha, \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ we write $\gcd(\alpha, \gamma)$ for the greatest common divisor of $\alpha, \gamma$ in the additive monoid $\mathbb{N}_0^{\mathcal{A}(S)}$ (i.e., $\gcd(\alpha, \gamma)(a) = \min\{\alpha(a), \gamma(a)\}$ for each $a \in \mathcal{A}(S)$).

**Definition 1.** (see [14, Definition 1.6.1]) *For* $\alpha, \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ *set*

$$d(\alpha, \gamma) := \max\{|\alpha - \gcd(\alpha, \gamma)|, |\gamma - \gcd(\alpha, \gamma)|\}.$$

*Given the monoid S as above, we say that* $\alpha$ *and* $\gamma$ *can be connected by a d-chain if there exists a sequence* $\alpha^{(0)} = \alpha, \alpha^{(1)}, \dots, \alpha^{(k)} = \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ *such that* $a^{\alpha^{(j)}} = a^{\alpha^{(j+1)}}$ *and* $d(\alpha^{(j)}, \alpha^{(j+1)}) \le d$ *for* $j = 0, 1, \dots, k-1$. *The* catenary degree $c(S)$ *is the minimal non-negative integer d such that if* $a^{\alpha} = a^{\gamma}$, *then* $\alpha$ *and* $\gamma$ *can be connected by a d-chain.*

*Remark 1.* Note that $c(S) = 0$ if and only if $S$ is a free (or factorial) monoid (i.e., $S$ is isomorphic to the additive monoid $\mathbb{N}_0^m$ for some $m$), and $c(S)$ is never equal to 1.

Characterizations of the catenary degree and its variants are given in [22, 23]. In particular, [22, Proposition 16] characterizes the catenary degree in terms of the *monoid* of relations. Now extending an observation from [4] we formulate a characterization of the catenary degree in terms of semigroup congruences. Denote by $c'(S)$ the minimal non-negative integer $d$ such that there exists a generating set $\Lambda \subset M \times M$ of the semigroup congruence $\sim_S$, satisfying that for all $(x^{\alpha}, x^{\gamma}) \in \Lambda$ we have $|\alpha| \le d$ and $|\gamma| \le d$. An explicit description of the semigroup congruence generated by a subset of $M \times M$ can be found for example in [18, page 176].

**Proposition 1.** *We have* $c(S) = c'(S)$.

*Proof.* Set

$$\Lambda := \{(x^{\alpha}, x^{\gamma}) \mid x^{\alpha} \sim_S x^{\gamma} \text{ and } |\alpha| \le c(S),\ |\gamma| \le c(S)\}.$$

We claim that $\Lambda$ generates the semigroup congruence $\sim_S$. Indeed, take a pair $(\alpha, \gamma) \in \mathbb{N}_0^{\mathcal{A}(S)} \times \mathbb{N}_0^{\mathcal{A}(S)}$ such that $x^{\alpha} \sim_S x^{\gamma}$. Then $\alpha$ and $\gamma$ can be connected by a $c(S)$-chain $\alpha^{(0)} = \alpha, \alpha^{(1)}, \dots, \alpha^{(k)} = \gamma$. For $i = 0, 1, \dots, k-1$ the pair $(\alpha^{(i)}, \alpha^{(i+1)})$ is of the form $(\beta^{(i)} + \delta^{(i)}, \rho^{(i)} + \delta^{(i)})$, where $\delta^{(i)}, \beta^{(i)}, \rho^{(i)} \in \mathbb{N}_0^{\mathcal{A}(S)}$, $|\beta^{(i)}| \le c(S)$, $|\rho^{(i)}| \le c(S)$. Moreover, since $S$ is cancellative, $a^{\alpha^{(i)}} = a^{\alpha^{(i+1)}}$, implies $a^{\beta^{(i)}} = a^{\rho^{(i)}}$, so $x^{\beta^{(i)}} \sim_S x^{\rho^{(i)}}$. Thus $(x^{\beta^{(i)}}, x^{\rho^{(i)}}) \in \Lambda$. It follows that $(x^{\alpha^{(i)}}, x^{\alpha^{(i+1)}}) = (x^{\beta^{(i)}} x^{\delta^{(i)}}, x^{\rho^{(i)}} x^{\delta^{(i)}})$ belongs to the congruence generated by $\Lambda$ for $i = 0, \dots, k-1$, implying in turn that $(x^{\alpha}, x^{\gamma}) = (x^{\alpha^{(0)}}, x^{\alpha^{(k)}})$ belongs to the congruence generated by $\Lambda$. This proves the inequality $c'(S) \le c(S)$.

The reverse inequality $c(S) \le c'(S)$ is pointed out in [4, Proposition 3.1].

Fix a commutative ring $R$ (having an identity element) and consider the semigroup rings $R[M]$ and $R[S]$. Note that $R[M] = R[x_a \mid a \in \mathcal{A}(S)]$ is the polynomial ring over $R$ with indeterminates $\{x_a \mid a \in \mathcal{A}(S)\}$. The monoid homomorphism $\pi : M \to S$ extends uniquely to an $R$-algebra homomorphism

$$\pi_R : R[M] \to R[S], \quad \pi(x^\alpha) = a^\alpha. \tag{3}$$

The statement below is well known, see [18, Proposition 1.5] or [16, Chapter II.7.]:

**Proposition 2.** *The following conditions are equivalent for a set of pairs* $B \subset \mathbb{N}_0^{\mathcal{A}(S)} \times \mathbb{N}_0^{\mathcal{A}(S)}$*:*

*(1) The semigroup congruence* $\sim_S$ *is generated by* $\{(x^\alpha, x^\gamma) \mid (\alpha, \gamma) \in B\}$.
*(2) The ideal* $\ker(\pi_R)$ *is generated by the binomials* $\{x^\alpha - x^\gamma \mid (\alpha, \gamma) \in B\}$.

*Remark 2.* Condition (1) of Proposition 2 does not depend on the ring $R$; therefore, a set of binomials generates the ideal $\ker(\pi_R)$ for some ring $R$ if and only if it generates $\ker(\pi_R)$ for any ring $R$.

Propositions 1 and 2 imply the following ring theoretic characterization of $c(S)$:

**Corollary 1.** *The catenary degree* $c(S)$ *is the minimal positive integer* $d$ *such that the kernel of* $\pi_R : R[M] \to R[S]$ *is generated (as an ideal) by binomials of degree at most* $d$ *for some (hence any) commutative ring* $R$ *(where* $R[M]$ *is graded in the standard way, namely, the generators* $x_a$ *have degree* 1 *and the non-zero scalars in* $R$ *have degree* 0*).*

## 3 Graded Monoids

Let $S$ be a *graded* monoid; that is, $S$ is partitioned into the disjoint union of subsets $S_d$, $d \in \mathbb{N}_0$, such that $S_d \cdot S_e \subseteq S_{d+e}$. For $s \in S$ write $|s| = d$ if $s \in S_d$. The identity element of $S$ necessarily belongs to $S_0$. We call a graded monoid *connected graded* if $S_0$ consists only of the identity element. It seems natural to modify Definition 1 for graded monoids as follows:

**Definition 2.** *Given a connected graded reduced affine monoid* $S$*, for* $\alpha, \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ *set*

$$|\alpha|_{\mathrm{gr}} = \sum_{a \in \mathcal{A}(S)} \alpha(a)|a|$$

*and*

$$d_{\mathrm{gr}}(\alpha, \gamma) := \max\{|\alpha - \gcd(\alpha, \gamma)|_{\mathrm{gr}}, |\gamma - \gcd(\alpha, \gamma)|_{\mathrm{gr}}\}.$$

*We say that* $\alpha$ and $\gamma$ can be connected by a chain of weight at most $d$ *if there exists a sequence* $\alpha^{(0)} = \alpha, \alpha^{(1)}, \ldots, \alpha^{(k)} = \gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ *such that* $a^{\alpha^{(j)}} = a^{\alpha^{(j+1)}}$ *and* $d_{\mathrm{gr}}(\alpha^{(j)}, \alpha^{(j+1)}) \le d$ *for* $j = 0, 1, \ldots, k-1$. *The* graded catenary degree $c_{\mathrm{gr}}(S)$ *is the minimal* $d$ *such that if* $a^\alpha = a^\gamma$*, then* $\alpha$ *and* $\gamma$ *can be connected by a chain of weight at most* $d$.

As a straightforward modification of Proposition 1 we get the following.

**Proposition 3.** *The graded catenary degree $c_{\mathrm{gr}}(S)$ is the minimal non-negative integer $d$ such that there exists a generating set $\Lambda \subset M \times M$ of the semigroup congruence $\sim_S$ satisfying that for all $(x^\alpha, x^\gamma) \in \Lambda$ we have $|\alpha|_{\mathrm{gr}} \leq d$ (note that $x^\alpha \sim_S x^\gamma$ implies $|\alpha|_{\mathrm{gr}} = |\gamma|_{\mathrm{gr}}$).*

The grading of $S$ induces a grading on the semigroup ring $R[S] = \bigoplus_{d=0}^{\infty} R[S]_d$, where $R[S]_d$ is the $R$-submodule generated by $S_d$. Lift the grading to $M$ and $R[M]$ by setting the degree of $x_a$ to be equal to the degree $|a|$ of $a \in \mathcal{A}(S)$. Then the map $\pi_R : R[M] \to R[S]$ is a homomorphism of graded algebras, and so $\ker(\pi_R)$ is a homogeneous ideal. Our assumptions on the grading imply that all indeterminates $x_a$ have positive degree. Moreover, $x^\alpha \sim_S x^\gamma$ implies that $a^\alpha$ and $a^\gamma$ belong to the same homogeneous component of $S$, and therefore the binomials in $\ker(\pi_R)$ are homogeneous. For an ideal $I$ in $R[M]$ denote by $\mu(I)$ the minimal non-negative integer $d$ such that $I$ is generated by elements of degree at most $d$; this number is finite for any binomial ideal $I$.

**Corollary 2.** *For any connected graded reduced affine monoid we have the equality*

$$c_{\mathrm{gr}}(S) = \mu(\ker(\pi_R)),$$

*where $R[M]$ is endowed with the grading that makes $\pi_R$ a homomorphism of graded algebras.*

*Proof.* Recall that any homogeneous generating system of a homogeneous ideal $I$ contains a minimal (with respect to inclusion) homogeneous generating system, and $\mu(I)$ is the maximal degree of an element in any minimal homogeneous generating system (this follows from the graded Nakayama lemma). The ideal $\ker(\pi_R)$ is generated by homogeneous binomials. Take a minimal set of binomials generating $\ker(\pi_R)$. Then the maximal degree of an element in this set of binomials equals $\mu(\ker(\pi_R))$ on one hand, and it equals $c_{\mathrm{gr}}(S)$ by Propositions 2 and 3, on the other hand.

*Remark 3.* The notions introduced in this section apply for block monoids. Indeed, $\mathbb{N}_0^m$ is graded by setting the degree of $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$ to be $\alpha_1 + \cdots + \alpha_m$, and the submonoid $\mathcal{B}(\underline{g})$ inherits this grading.

## 4 Repetition of Elements

A surjective monoid homomorphism $\theta : T \to B$ between reduced affine monoids $T$ and $B$ is called a *transfer homomorphism* if for any $t \in T$, $b, c \in B$ with $\theta(t) = bc$, there exist elements $u, v \in T$ such that $t = uv$ and $\theta(u) = b$, $\theta(v) = c$ (see [14, Definition 3.2.1]).

Now let $\underline{g}$ be an $m$-tuple of elements in an abelian group $G$ and $\mathcal{B}(\underline{g})$, $\mathcal{B}(\mathrm{supp}(\underline{g}))$ the monoids introduced in Section 1. The map

$$\mathbb{N}_0^m \to \mathbb{N}_0^{\mathrm{supp}(\underline{g})}, \quad \alpha \mapsto (g \mapsto \sum_{g_i = g} \alpha_i) \tag{4}$$

restricts to a *transfer homomorphism* $\mathcal{B}(\underline{g}) \to \mathcal{B}(\mathrm{supp}(\underline{g}))$. In factorization theory transfer homomorphisms are used to reduce the computation of arithmetic invariants of monoids to the corresponding invariants of other monoids (frequently of block monoids). In particular, it is known that the catenary degrees of monoids connected by a transfer homomorphism are linked as follows:

**Lemma 1.** *[14, Theorem 3.2.5.5] Let $\theta : T \to B$ be a transfer homomorphism, where $T$ and $B$ are reduced affine monoids. Then we have the inequalities*

$$c(B) \le c(T) \le \max\{c(B), c(T, \theta)\}$$

*(see [14, page 171] for the definition of $c(T, \theta)$).*

The aim of this section is to refine Lemma 1 for the transfer homomorphism $\mathcal{B}(\underline{g}) \to \mathcal{B}(\mathrm{supp}(\underline{G}))$ given by (4). More precisely, it will be shown how one can get a generating system of the defining congruence of $\mathcal{B}(\underline{g})$ from a given generating system of the defining congruence of $\mathcal{B}(\mathrm{supp}(\underline{g}))$. This will be done in a more general setup.

Assume that $S$ is a (not necessarily connected) graded, reduced, affine monoid, and denote by $\tilde{S}$ the monoid

$$\tilde{S} = \{s[i] \mid s \in S, 0 \le i \le |s|\} \text{ with multiplication } s[i] \cdot t[j] = (s \cdot t)[i + j]. \tag{5}$$

So $\tilde{S}$ is a submonoid of the direct product of $S$ and the additive monoid $\mathbb{N}_0$. Obviously the map $\tilde{S} \to S$, $s[i] \mapsto s$ is a transfer homomorphism, and

$$\mathcal{A}(\tilde{S}) = \{a[i] \mid a \in \mathcal{A}(S),\ 0 \le i \le |a|\}.$$

This transfer homomorphism $\tilde{S} \to S$ induces a monoid homomorphism

$$\kappa : \mathbb{N}_0^{\mathcal{A}(\tilde{S})} \to \mathbb{N}_0^{\mathcal{A}(S)}, \quad \lambda \mapsto \left( a \mapsto \sum_{i=0}^{|a|} \lambda(a[i]) \right).$$

Set

$$\delta : \mathbb{N}_0^{\mathcal{A}(\tilde{S})} \to \mathbb{N}_0, \quad \lambda \mapsto \sum_{a[i] \in \mathcal{A}(\tilde{S})} i\lambda(a[i]).$$

Note that for $\lambda, \mu \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ we have

$$x^\lambda \sim_{\tilde{S}} x^\mu \iff x^{\kappa(\lambda)} \sim_S x^{\kappa(\mu)} \text{ and } \delta(\lambda) = \delta(\mu). \tag{6}$$

Also we have $\delta(\lambda) \leq |a^{\kappa(\lambda)}|$.

**Lemma 2.** *Assume that* $\alpha, \beta \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ *satisfy*

$$\kappa(\alpha) = \kappa(\beta) \quad \textit{and} \quad \delta(\alpha) = \delta(\beta).$$

*Then* $x^\alpha \sim x^\beta$ *with respect to the semigroup congruence* $\sim$ *on the free monoid* $\tilde{M} = \{x^\alpha \mid \alpha \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}\}$ *generated by*

$$\{(x_{a[k]}x_{b[l]}, x_{a[k+1]}x_{b[l-1]}) \mid a, b \in \mathcal{A}(S),\ 0 \leq k \leq |a| - 1,\ 1 \leq l \leq |b|\}.$$

*Proof.* Apply induction on $\sum_{a[j] \in \mathcal{A}(\tilde{S})} \alpha(a[j])$. If this number is 1, then clearly $\alpha = \beta$, and so the desired conclusion holds. Assume $\sum_{a[j] \in \mathcal{A}(\tilde{S})} \alpha(a[j]) > 1$.

Case I: $x^\alpha$ and $x^\beta$ involve a common variable $x_{a[i]}$. Then $x^\alpha = x_{a[i]}x^{\alpha'}$, $x^\beta = x_{a[i]}x^{\beta'}$, and the assumptions on the pair $(\alpha, \beta)$ in the statement of the lemma hold for the pair $(\alpha', \beta')$. By the induction hypothesis we may conclude that $x^{\alpha'} \sim x^{\beta'}$, implying in turn that $x^\alpha \sim x^\beta$.

Case II: $x^\alpha$ and $x^\beta$ are not divisible by a common variable. Take a variable $x_{a[i]}$ dividing $x^\alpha$. Then $\kappa(\alpha) = \kappa(\beta)$ implies that $x^\beta$ is divisible by $x_{a[k]}$ for some $k \neq i$. By symmetry it is sufficient to deal with the case $i > k$. By the assumptions on $\alpha, \beta$ there must exist an atom $b \in \mathcal{A}(S)$ and integers $j < l$ such that $x_{a[i]}x_{b[j]}$ divides $x^\alpha$ and $x_{a[k]}x_{b[l]}$ divides $T^\beta$. We have $x^\alpha = x_{a[i]}x_{b[j]}x^\gamma \sim x_{a[i-1]}x_{b[j+1]}x^\gamma = x^{\alpha'}$. The conditions of the lemma on the pair $(\alpha, \beta)$ hold also for the pair $(\alpha', \beta)$. If $i - 1 = k$, then $x^{\alpha'}$ and $x^\beta$ are divisible by a common variable, and we are back in Case I. Otherwise similarly to the above process we have $x^{\alpha'} \sim x^{\alpha''}$ where $x^{\alpha''}$ is divisible by $x_{a[i-2]}$ and $\kappa(\alpha'') = \kappa(\beta)$ and $\delta(\alpha'') = \delta(\beta)$. After finitely many such steps we get back to Case I.

*Remark 4.* Lemma 2 says that for the transfer homomorphism $\theta : \tilde{S} \to S, s[i] \mapsto s$ we have $c(\tilde{S}, \theta) \leq 2$ in Lemma 1.

**Theorem 1.** *Suppose that the congruence* $\sim_S$ *is generated by* $\{(x^\lambda, x^\mu) \mid (\lambda, \mu) \in \Lambda\}$ *for some* $\Lambda \subset \mathbb{N}_0^{\mathcal{A}(S)} \times \mathbb{N}_0^{\mathcal{A}(S)}$. *For each* $\lambda \in \mathbb{N}_0^{\mathcal{A}(S)}$ *such that* $(\lambda, \mu) \in \Lambda$ *or* $(\mu, \lambda) \in \Lambda$ *for some* $\mu$, *and for each* $0 \leq i \leq |a^\lambda|$ *choose* $\lambda[i] \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ *such that* $\kappa(\lambda[i]) = \lambda$ *and* $\delta(\lambda[i]) = i$ *(this is clearly possible). Then the congruence* $\sim_{\tilde{S}}$ *is generated by*

$$\{(x^{\lambda[i]}, x^{\mu[i]}),\ (x_{a[k]}x_{b[l]}, x_{a[k+1]}x_{b[l-1]}) \mid (\lambda, \mu) \in \Lambda,\ 0 \le i \le |a^{\lambda}|,$$
$$a, b \in \mathcal{A}(S),\ 0 \le k \le |a|-1,\ 1 \le l \le |b|\}.$$

*Proof.* The pairs given in the statement do belong to the congruence $\sim_{\tilde{S}}$. Denote by $\sim$ the semigroup congruence on $\tilde{M} = \{x^{\alpha} \mid \alpha \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}\}$ generated by them. It is sufficient to show that if $x^{\alpha} \sim_{\tilde{S}} x^{\beta}$ for some $\alpha, \beta \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$, then $x^{\alpha} \sim x^{\beta}$. By (6) we have $x^{\kappa(\alpha)} \sim_S x^{\kappa(\beta)}$ and $\delta(\alpha) = \delta(\beta)$. Therefore there exists a sequence $(\lambda_j, \mu_j) \in \mathbb{N}_0^{\mathcal{A}(S)} \times \mathbb{N}_0^{\mathcal{A}(S)}$ and $\gamma_j \in \mathbb{N}_0^{\mathcal{A}(S)}$ $(j = 1, \ldots, s)$ such that $(\lambda_j, \mu_j) \in \Lambda$ or $(\mu_j, \lambda_j) \in \Lambda$ (implying in particular that $|a^{\lambda_j}| = |a^{\mu_j}|$), $\lambda_1 + \gamma_1 = \kappa(\alpha)$, $\mu_s + \gamma_s = \kappa(\beta)$, and $\mu_j + \gamma_j = \lambda_{j+1} + \gamma_{j+1}$ for $j = 1, \ldots, s-1$. Set $d := \delta(\alpha) = \delta(\beta)$. For each $j = 1, \ldots, s$ choose a non-negative integer $k_j$ with

$$d - |a^{\gamma_j}| \le k_j \le |a^{\lambda_j}|.$$

This is possible, because

$$d \le |a^{\kappa(\alpha)}| = |a^{\lambda_j + \gamma_j}| = |a^{\lambda_j}| + |a^{\gamma_j}|.$$

Taking into account Lemma 2 we get

$$\begin{aligned} x^{\alpha} \sim x^{\kappa(\alpha)[d]} = x^{(\lambda_1+\gamma_1)[d]} \sim x^{\lambda_1[k_1]}x^{\gamma_1[d-k_1]} \sim x^{\mu_1[k_1]}x^{\gamma_1[d-k_1]} \sim \\ x^{(\mu_1+\gamma_1)[d]} = x^{(\lambda_2+\gamma_2)[d]} \sim x^{\lambda_2[k_2]}x^{\gamma_2[d-k_2]} \sim x^{\mu_2[k_2]}x^{\gamma_2[d-k_2]} \sim \\ x^{(\mu_2+\gamma_2)[d]} = x^{(\lambda_3+\gamma_3)[d]} \sim \cdots \sim x^{(\mu_s+\gamma_s)[d]} = x^{\kappa(\beta)[d]} \sim x^{\beta}. \end{aligned}$$

*Remark 5.* Statements related to Theorem 1 are proved in [21], studying toric ideals associated to nested configurations (see also [26] for some generalization). The construction of $\tilde{S}$ from $S$ (see (5)) can be seen as a special case of the construction of nested configurations. In particular, when $S$ is a submonoid of $\mathbb{N}_0^d$ generated by finitely many elements $\alpha^{(1)}, \ldots, \alpha^{(m)}$ such that there exists a $v \in \mathbb{R}^d$ with $\sum_{j=1}^{d} \alpha_j^{(i)} v_j = 1$ for all $i = 1, \ldots, m$ (this implies that $S$ can be graded in such a way that each generator has degree 1), the results of [21] apply to the binomial ideal associated to the monoid $\tilde{S}$ and yield a system of generators similar to the one given by Theorem 1.

The monoid $\mathcal{B}(\underline{g})$ can be obtained from the monoid $\mathcal{B}(\text{supp}(\underline{g}))$ by a repeated application of the construction (5), and therefore Theorem 1 can be applied to relate the catenary degree of $\mathcal{B}(\underline{g})$ to the catenary degree of $\mathcal{B}(\text{supp}(\underline{g}))$. Indeed, start with an $m$-tuple $\underline{g} = (g_1, \ldots, g_m) \in G^m$ of not necessarily distinct elements in $G$, and denote by $\underline{\tilde{g}}$ the $m+1$-tuple $(g_1, \ldots, g_m, g_m)$ obtained from $\underline{g}$ by repeating the $m$th component. Consider the grading on the monoid $\mathcal{B}(\underline{g})$ given by

$$\mathcal{B}(\underline{g})_d = \{\alpha \in \mathcal{B}(\underline{g}) \subseteq \mathbb{N}_0^m \mid \alpha_m = d\}.$$

**Proposition 4.** *We have $\mathcal{B}(\underline{\tilde{g}}) \cong \tilde{S}$, where $S = \mathcal{B}(\underline{g})$ is endowed with the above grading and $\tilde{S}$ is defined as in (5).*

*Proof.* A general element of $\tilde{S}$ is of the form $\alpha[i]$ where $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathcal{B}(\underline{g})$ and $0 \le i \le \alpha_m$. The map $\tilde{S} \to \mathcal{B}(\underline{\tilde{g}})$ sending $\alpha[i] \in \tilde{S}$ to $(\alpha_1, \dots, \alpha_{m-1}, \alpha_m - i, i)$ is an isomorphism between the monoids $\tilde{S}$ and $\mathcal{B}(\underline{\tilde{g}})$.

Proposition 1, Theorem 1, and Proposition 4 imply the following:

**Corollary 3.** *We have $c(\mathcal{B}(\underline{g})) = c(\mathcal{B}(\text{supp}(\underline{g})))$, unless $\mathcal{B}(\text{supp}(\underline{g}))$ is a free monoid and the components $g_1, \dots, g_m$ of $\underline{g}$ are not all distinct. In the latter case we have $c(\mathcal{B}(\text{supp}(\underline{g}))) = 0$ whereas $c(\mathcal{B}(\underline{g})) = 2$.*

*Remark 6.* Being a finitely generated reduced Krull monoid, $\mathcal{B}(\underline{g}) \cong \mathcal{B}(H_0)$ for some finite subset $H_0$ in an abelian group $H$ (different from $G$ in general) by [14, Theorem 2.7.14] also when $g_1, \dots, g_m$ are not all distinct. However, the representation of our monoid in the form $\mathcal{B}(\underline{g})$ is fundamental for our discussions.

An easy direct proof of the isomorphism $\mathcal{B}(\underline{g}) \cong \mathcal{B}(H_0)$ can be derived from the following observation. Take $\underline{g} \in G^m$, and suppose that $g_{m-1} = g_m$. Consider the group $H := G \times \mathbb{Z}$, and the sequence

$$\underline{h} := ((g_1, 0), \dots, (g_{m-1}, 0), (g_{m-1}, 1), (0, -1)) \in H^{m+1}.$$

It is easy to see that we have a monoid isomorphism $\mathcal{B}(\underline{g}) \cong \mathcal{B}(\underline{h})$. Now observe that there are less component repetitions in the sequence $\underline{h}$ then the number of component repetitions in $\underline{g}$. Note that the "price" for this manipulation was that we had to extend the group $G$.

## 5 Gröbner Bases

In this section we give a Gröbner basis variant of the results of Section 4. As it was explained in Sections 2 and 3, the catenary degree of a monoid can be expressed in terms of generators of a binomial ideal associated to the monoid. Since Gröbner bases are special generating systems of ideals in a polynomial algebra that are at the heart of many algorithms in computational commutative algebra (see for example [7] for Gröbner basis theory), it is worthwhile to translate this notion to the language of semigroup congruences.

Fix an admissible total order $\prec$ on the finitely generated free multiplicative monoid $M$; that is, $\prec$ is a total order such that for $x, y, z \in M$ with $x \prec y$ we have $xz \prec yz$, and $1 \prec x$ for each $x \in M \setminus \{1\}$. The latter condition ensures that the order $\prec$ is artinian (i.e., there is no infinite strictly descending chain with respect to $\prec$ in $M$), so any non-empty subset of $M$ contains a unique minimal element. Note also that $\prec$ is a term order of the polynomial ring $\mathbb{F}[M]$ (where $\mathbb{F}$ is a field) in the sense of Gröbner basis theory.

**Definition 3.** *A finite set $\Lambda \subset M \times M$ is a* Gröbner system of the semigroup congruence $\sim$ on $M$ *if the following conditions hold:*

*(i)* $x \sim y$ *and* $y \prec x$ *for each* $(x, y) \in \Lambda$;
*(ii)* $z \in M$ *is the minimal element in its congruence class with respect to* $\sim$ *if there is no* $(x, y) \in \Lambda$ *such that* $x$ *divides* $z$ *in* $M$.

The name *Gröbner system* is justified by the relation to Gröbner bases given in Proposition 5 (iii).

**Proposition 5.** *(i) If* $\Lambda \subset M \times M$ *is a Gröbner system of the semigroup congruence* $\sim$ *then* $\Lambda$ *generates* $\sim$.
*(ii) Every semigroup congruence* $\sim$ *on* $M$ *has a Gröbner system.*
*(iii)* $\Lambda \subset M \times M$ *is a Gröbner system of* $\sim$ *if and only if* $\{x - y \mid (x, y) \in \Lambda\}$ *is a Gröbner basis (satisfying* $y \prec x$ *for each of its elements* $x - y$*) of the ideal* $\ker(\pi_{\mathbb{F}})$*, where* $\mathbb{F}$ *is a field and* $\pi_{\mathbb{F}} : \mathbb{F}[M] \to \mathbb{F}[M/\sim]$ *is induced by the natural surjection* $M \to M/\sim$.

*Proof.* (i) Denote by $\sim_\Lambda$ the congruence generated by $\Lambda$. By assumption it is contained in $\sim$, since for each $(x, y) \in \Lambda$ we have $x \sim y$. To see the reverse inclusion it is sufficient to show that for any $z \in M$ we have $z \sim_\Lambda u$, where $u$ is the minimal element in the $\sim$-congruence class of $z$. If $z = u$, we are done. Otherwise $u \prec z$, hence, by assumption there exists a pair $(x, y) \in \Lambda$ and $v \in M$ such that $z = xv$. Set $z_1 = yv$. Then $z_1 = yv \prec xv = z$ and $z \sim_\Lambda z_1$. If $z_1 = u$, then we are done. Otherwise repeat the same step for $z_1$ instead of $z$ (note that $z_1 \sim z \sim u$). We obtain $z_2 \in M$ with $z_2 \prec z_1$ and $z_2 \sim_\Lambda z_1$. If $z_2 = u$ we are done, otherwise repeat the above step with $z_2$ instead of $z_1$. Since the order $\prec$ is artinian, in finitely many steps we must end up with $z \sim_\Lambda z_k = u$.

(ii) It is well known that any binomial ideal has a Gröbner basis consisting of binomials, see for example [28, Lemma 8.2.17]. Therefore the statement follows from (iii).

(iii) Suppose $\{x - y \mid (x, y) \in \Lambda\}$ is a Gröbner basis of the ideal $\ker(\pi_{\mathbb{F}})$ (where $y \prec x$ for each $(x, y) \in \Lambda$). It follows that the initial ideal of $\ker(\pi_{\mathbb{F}})$ is generated by $L := \{x \mid \exists y : (x, y) \in \Lambda\}$. Now take any $z \in M$ which is not minimal in its congruence class with respect to $\sim$. Then there is an $u \prec z$ such that $z \sim u$, so $z - u \in \ker(\pi_{\mathbb{F}})$ has initial term $z$. Therefore there is an $x \in L$ such that $x$ divides $z$, so condition (ii) of Definition 3 holds for $\Lambda$ (it is obvious that condition (i) of Definition 3 holds for $\Lambda$).

Conversely, assume that $\Lambda$ is a Gröbner system of $\sim$, and consider the subset $L := \{x - y \mid (x, y) \in \Lambda\}$ in $\mathbb{F}[M]$. Denote by $J$ the ideal generated by the initial terms of the elements in $L$. Clearly $L \subseteq \ker(\pi_{\mathbb{F}})$, hence, $J$ is contained in the ideal $K$ generated by the initial terms of the ideal $\ker(\pi_{\mathbb{F}})$. By assumption the elements of $M \setminus J$ are all minimal in their congruence class with respect to $\sim$. In particular, they are pairwise incongruent; hence, they are mapped by $\pi_{\mathbb{F}}$ to elements in $\mathbb{F}[M/\sim]$ that are linearly independent over $\mathbb{F}$. On the other hand, $M \setminus J \supseteq M \setminus K$, and the latter is mapped by $\pi_{\mathbb{F}}$ to an $\mathbb{F}$-vector space basis of $\mathbb{F}[M/\sim]$ (see for example [27, Proposition 1.1]). It follows that $M \setminus J = M \setminus K$, implying in turn that $J = K$. The latter equality means that $L$ is a Gröbner basis of $\ker(\pi_{\mathbb{F}})$.

We keep the notation of Section 4. In particular, $S$ is a reduced, affine, graded monoid, and $\tilde{S}$ is the monoid defined as in (5). Fix an admissible total order $\prec$ on $M = \{x^\alpha \mid \alpha \in \mathbb{N}_0^{\mathcal{A}(S)}\}$. Define an admissible total order (denoted also by $\prec$) on the free monoid $\tilde{M}$ generated by $\{x_a \mid a \in \mathcal{A}(\tilde{S})\}$ as follows. Enumerate the atoms in $\mathcal{A}(S) = \{a_1, \dots, a_n\}$ such that $x_{a_1} \prec x_{a_2} \prec \cdots \prec x_{a_n}$. Set $d_i = |a_i|$. For $\lambda, \mu \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ we set $x^\mu \prec x^\lambda \in \tilde{M}$ if

1. $x^{\kappa(\mu)} \prec x^{\kappa(\lambda)}$ in $(M, \prec)$; or
2. $\kappa(\mu) = \kappa(\lambda)$ and the sequence

$$(\mu(a_1[0]), \mu(a_1[1]), \dots, \mu(a_1[d_1]), \mu(a_2[0]), \dots, \mu(a_n[0]), \dots, \mu(a_n[d_n]))$$

is lexicographically greater than

$$(\lambda(a_1[0]), \lambda(a_1[1]), \dots, \lambda(a_1[d_1]), \lambda(a_2[0]), \dots, \lambda(a_n[0]), \dots, \lambda(a_n[d_n])).$$

**Theorem 2.** *Suppose that $\{(x^\lambda, x^\mu) \mid (\lambda, \mu) \in \Lambda\}$ is a Gröbner system of the semigroup congruence $\sim_S$. Then $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ is a Gröbner system of the defining congruence $\sim_{\tilde{S}}$ of $\tilde{S}$, where*

$$\Gamma_1 = \{(x^\lambda, x^\mu) \mid \lambda, \mu \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}, \quad (\kappa(\lambda), \kappa(\mu)) \in \Lambda, \quad \delta(\lambda) = \delta(\mu)\}$$

$$\Gamma_2 = \{(x_{a[i]}x_{b[j]}, x_{a[i-1]}x_{b[j+1]}) \mid a, b \in \mathcal{A}(S),\ x_a \prec x_b,\ 0 < i \le |a|,\ 0 \le j < |b|\}$$

$$\Gamma_3 = \{(x_{a[i]}x_{a[j]}, x_{a[i-1]}x_{a[j+1]}) \mid a \in \mathcal{A}(S),\ 0 < i \le j < |a|\}.$$

*Proof.* Take $(x^\lambda, x^\mu) \in \Gamma_1$. Then $(\kappa(\lambda), \kappa(\mu)) \in \Lambda$, hence, $x^{\kappa(\lambda)} \sim_S x^{\kappa(\mu)}$ and $x^{\kappa(\mu)} \prec x^{\kappa(\lambda)} \in M$. It follows that $x^\mu \prec x^\lambda \in \tilde{M}$. Moreover, $x^{\kappa(\lambda)} \sim_S x^{\kappa(\mu)}$ and $\delta(\lambda) = \delta(\mu)$ imply $x^\lambda \sim_{\tilde{S}} x^\mu$ by (6). Therefore condition (i) of Definition 3 holds for the elements of $\Gamma_1$. It obviously holds for the elements of $\Gamma_2$ and $\Gamma_3$ by definition of the ordering $\prec$ on $\tilde{M}$.

It remains to check that condition (ii) of Definition 3 holds for $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$. In order to do so, take $\lambda \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ such that $x^\lambda \in \tilde{M}$ is not minimal in its congruence class with respect to $\sim_{\tilde{S}}$.

Assume first that $x^{\kappa(\lambda)} \in M$ is not minimal in its congruence class with respect to $\sim_S$. Then by the assumption of the theorem on $\Lambda$, there exist $(\alpha, \beta) \in \Lambda$ and $\gamma \in \mathbb{N}_0^{\mathcal{A}(S)}$ such that $\kappa(\lambda) = \alpha + \gamma$. Clearly there exist $\tilde{\alpha}, \tilde{\gamma} \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ with $\lambda = \tilde{\alpha} + \tilde{\gamma}$, $\kappa(\tilde{\alpha}) = \alpha$, and $\kappa(\tilde{\gamma}) = \gamma$. Also $x^\alpha \sim_S x^\beta$ implies $\sum_{a \in \mathcal{A}(S)} \alpha(a)|a| = \sum_{a \in \mathcal{A}(S)} \beta(a)|a|$. It is easy to infer from this equality the existence of $\tilde{\beta} \in \mathbb{N}_0^{\mathcal{A}(\tilde{S})}$ with $\kappa(\tilde{\beta}) = \beta$ and $\delta(\tilde{\beta}) = \delta(\tilde{\alpha})$. Moreover, $(\alpha, \beta) \in \Lambda$ implies $x^\beta \prec x^\alpha$, hence, $x^{\tilde{\beta}} \prec x^{\tilde{\alpha}}$.

So $(x^{\tilde{\alpha}}, x^{\tilde{\beta}}) \in \Gamma_1$ by definition of $\Gamma_1$. Therefore $\Gamma_1$ testifies the non-minimality of $x^\lambda$ as it is required by (ii) of Definition 3.

Suppose next that $x^{\kappa(\lambda)}$ is minimal in its congruence class in $M$ with respect to $\sim_s$, and $x^\lambda \in \tilde{M}$ is not minimal in its congruence class with respect to $\sim_{\tilde{S}}$. It is easy to deduce from condition 2. of the definition of the ordering $\prec$ on $\tilde{M}$ that there must exist $(y, z) \in \Gamma_2 \cup \Gamma_3$ such that $y$ divides $x^\lambda$. Consequently, the non-minimality of $x^\lambda$ is testified by $\Gamma_2 \cup \Gamma_3$ as it is required by (ii) of Definition 3.

*Remark 7.* The papers [21, 26] mentioned in Remark 7 also give Gröbner bases of the binomial ideals considered there.

We call a Gröbner system $\Lambda$ *quadratic* if $|\lambda| \leq 2$, $|\mu| \leq 2$ for all $(\lambda, \mu) \in \Lambda$.

**Corollary 4.** *If the semigroup congruence $\sim_S$ has a quadratic Gröbner system, then the semigroup congruence $\sim_{\tilde{S}}$ also has a quadratic Gröbner system.*

Koszul algebras form an interesting class of rings well studied in commutative algebra, see for example [5]. In general it is a difficult task to decide whether a quadratic algebra (a factor of the multivariate polynomial algebra modulo an ideal generated by homogeneous quadratic elements) is Koszul or not. The significance of Corollary 4 is that it can be used to produce examples of Koszul algebras. Indeed, note that if $S$ has a quadratic Göbner system, then by Proposition 5 (iii) the ideal of relations among the generators of the semigroup algebra $\mathbb{F}[S]$ has a quadratic Gröbner basis, hence is Koszul (see [24] for background on Koszul algebras). Therefore an iterated use of Corollary 4 yields the following:

**Corollary 5.** *If $\mathcal{B}(\text{supp}(\underline{g}))$ has a quadratic Gröbner system, then $\mathcal{B}(\underline{g})$ also has a quadratic Gröbner system, and hence, the semigroup algebra $\mathbb{F}[\mathcal{B}(\underline{g})]$ is Koszul.*

*Example 1.* Consider the additive group $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$, and the monoid $S := \mathcal{B}((1, 2, 3))$. The atoms in this monoid are

$$\mathcal{A}(S) = \{(1, 1, 1),\ (4, 1, 0),\ (3, 0, 1),\ (2, 2, 0),\ (0, 0, 2),\ (0, 3, 0),\ (6, 0, 0)\}.$$

The commuting indeterminates corresponding to the atoms will be denoted by $x_1, x_2, x_3, x_4, x_5, x_6, x_7$, and $\pi : M \to S$ is the monoid homomorphism mapping the generator $x_i$ of the free monoid $M$ to the $i$th atom in the above list ($i = 1, \dots, 7$). Denote by $\prec$ the graded reverse lexicographic order on $M$. That is, $x^\alpha \prec x^\beta$ if $\sum_{i=1}^7 \alpha_i < \sum_{i=1}^7 \beta_i$, or if $\sum_{i=1}^7 \alpha_i = \sum_{i=1}^7 \beta_i$ and for the largest $j$ with $\alpha_j \neq \beta_j$ we have $\alpha_j > \beta_j$ (in particular, $x_7 \prec x_6 \prec \cdots \prec x_1$). We claim that the following is a Gröbner system for $S$:

$$\begin{aligned}\Lambda := \{&(x_1^2, x_4x_5),\ (x_2^2, x_4x_7),\ (x_3^2, x_5x_7),\ (x_4^2, x_2x_6),\ (x_1x_2, x_3x_4),\\ &(x_1x_3, x_2x_5),\ (x_2x_3, x_1x_7),\ (x_1x_4, x_3x_6),\ (x_2x_4, x_6x_7)\}.\end{aligned}$$

Indeed, for each pair $(x, y) \in \Lambda$ we have $x \sim_S y$ and $y \prec x$. Moreover, it is easy to see that the elements in $M$ not divisible by any of the first components of the pairs in $\Lambda$ are the following:

$$\{wx_5^i x_6^j x_7^k \mid i, j, k \in \mathbb{N}_0,\ w \in \{1, x_1, x_2, x_3, x_4, x_3x_4\}\}.$$

Now the above elements are mapped by $\pi$ to distinct elements in $S$. To see this note that the modulo 6 residue of the first component of $\pi(wx_5^i x_6^j x_7^k)$ uniquely determines $w$, and then $i, j, k$ are determined by $\pi(wx_5^i x_6^j x_7^k)$. Thus $S$ has a quadratic Gröbner system, and consequently by Corollary 5 the algebra $\mathbb{F}[\mathcal{B}(\underline{g})]$ is Koszul for any $\underline{g}$ with $\mathrm{supp}(\underline{g}) = \{1, 2, 3\} \subset \mathbb{Z}/6\mathbb{Z}$.

## 6 Relation to Invariant Theory

We need to recall a result from invariant theory (see [11] for an introduction to invariant theory). Let $H$ be a linearly reductive subgroup of the group $GL(V)$ of invertible linear transformations of a finite-dimensional vector space $V$ over an algebraically closed field $\mathbb{F}$. The action of $H$ on $V$ induces an action via graded $\mathbb{F}$-algebra automorphism on the symmetric tensor algebra $S(V)$ of $V$ (graded in the standard way, namely, $V \subset S(V)$ is the degree 1 homogeneous component). Since $H$ is linearly reductive, the algebra $S(V)^H = \{f \in S(V) \mid h \cdot f = f\ \forall h \in H\}$ of polynomial invariants is known to be finitely generated. Let $f_1, \dots, f_n$ be a minimal homogeneous generating system of $S(V)^H$, enumerated so that $\deg(f_1) \geq \deg(f_2) \geq \dots \geq \deg(f_n)$. Consider the $\mathbb{F}$-algebra surjection

$$\varphi : \mathbb{F}[x_1, \dots, x_n] \to S(V)^H \text{ with } x_i \mapsto f_i \quad (i = 1, \dots, n). \tag{7}$$

Endow $\mathbb{F}[x_1, \dots, x_n]$ with the grading given by $\deg(x_i) = \deg(f_i)$, so $\varphi$ is a homomorphism of graded algebras. Recall that the factor of $S(V)$ modulo the ideal generated by $f_1, \dots, f_n$ is called the *algebra of coinvariants*. It is a finite-dimensional graded vector space when $H$ is finite; in this case write $b(H, V)$ for its top degree (equivalently, all homogeneous elements in $S(V)$ of degree greater than $b(H, V)$ belong to the Hilbert ideal $S(V)f_1 + \dots + S(V)f_n$, and there is a homogeneous element in $S(V)$ of degree $b(H, V)$ not contained in the Hilbert ideal). Denote by $s$ the Krull dimension of $S(V)^H$. Note that $s \leq n$ with equality only if $\ker(\varphi) = \{0\}$.

**Theorem 3.** (Derksen [10, Theorems 1 and 2])

*(i) We have the inequality* $\mu(\ker(\varphi)) \leq \sum_{i=1}^{\min\{n,s+1\}} \deg(f_i) - s$,

*(ii) When $H$ is finite, we have the inequality* $\mu(\ker(\varphi)) \leq 2b(G, V) + 2$.

The *Davenport constant of a finite subset* $G_0$ of an abelian group $G$ is defined as

$$\mathsf{D}(G_0) = \max\{|\alpha| \colon \alpha \in \mathcal{A}(\mathcal{B}(G_0))\},$$

where $|\alpha| = \sum_{g \in G_0} \alpha(g)$. When $G_0$ generates a finite subgroup in $G$, the *little Davenport constant of* $G_0$ can be defined as

$$\mathsf{d}(G_0) = \max\{|\alpha| \colon \alpha \in \mathbb{N}_0^{G_0}, \ \forall \gamma \in \mathcal{A}(\mathcal{B}(G_0)) \ \exists g \in G_0 \text{ with } \gamma(g) > \alpha(g)\},$$

the maximal length of a sequence over $G_0$ containing no product-one subsequence (see [14, Proposition 5.1.3.2]).

Now let $\underline{g} = (g_1, \ldots, g_m)$ be a sequence of elements from an arbitrary abelian group $G$, and use the notation developed in Section 4. Consider the following grading of the block monoid $\mathcal{B}(\underline{g})$: for $\alpha \in \mathcal{B}(\underline{g})$ its degree is $|\alpha| = \sum_{i=1}^{m} \alpha_i$. The graded catenary degree $c_{\mathrm{gr}}(\mathcal{B}(\underline{g}))$ is defined in Definition 2 accordingly. Denote by $r(\mathcal{B}(\underline{g}))$ the rank of the free abelian subgroup in $\mathbb{Z}^m$ generated by $\mathcal{B}(\underline{g})$. Obviously $|\mathcal{A}(\mathcal{B}(\underline{g}))| \geq r(\mathcal{B}(\underline{g}))$ with equality if and only if $\mathcal{B}(\underline{g})$ is a free monoid. Set

$$\mathcal{A}(\mathcal{B}(\mathrm{supp}(\underline{g}))) := \{a_1, \ldots, a_n\} \text{ with } |a_1| \geq |a_2| \geq \cdots \geq |a_n|.$$

**Theorem 4.** *(i) We have the inequalities*

$$c_{\mathrm{gr}}(\mathcal{B}(\underline{g})) \leq \max\{2|a_1|, c_{\mathrm{gr}}(\mathcal{B}(\mathrm{supp}(\underline{g})))\}, \tag{8}$$

*and*

$$c_{\mathrm{gr}}(\mathcal{B}(\mathrm{supp}(\underline{g}))) \leq \sum_{i=1}^{\min\{n, r+1\}} |a_i| - r, \tag{9}$$

*where* $r = r(\mathcal{B}(\mathrm{supp}(\underline{g})))$.

*(ii) If* $g_1, \ldots, g_m$ *generate a finite subgroup of* $G$*, then*

$$c_{\mathrm{gr}}(\mathcal{B}(\underline{g})) \leq 2\mathsf{d}(\mathrm{supp}(\underline{g})) + 2. \tag{10}$$

*Proof.* We may assume that the components of $\underline{g}$ generate $G$. So $G$ is a finitely generated abelian group, whence it is isomorphic to $G_1 \times \mathbb{Z}^k$, where $G_1$ is a finite abelian group, and $\mathbb{Z}^k$ is the free abelian group of rank $k$. Consider the linear algebraic group $H = G_1 \times T$, where $T$ is the torus $(\mathbb{C}^\times)^k$. For an abelian linear algebraic group $A$ denote by $X(A)$ the group of homomorphisms $A \to \mathbb{C}^\times$ (as algebraic groups). Then $X(G_1) \cong G_1$ and $X(T) \cong \mathbb{Z}^k$, whence $X(H) \cong G_1 \times \mathbb{Z}^k \cong G$. From now on we identify $G$ with $X(H)$. Let $V$ be a $\mathbb{C}$-vector space with basis $x_1, \ldots, x_m$, and define an action of $H$ on $V$ via linear transformations by setting $h \cdot x_i = g_i(h) x_i$ for $i = 1, \ldots, m$. The algebra $S(V)$ is the polynomial algebra $\mathbb{C}[x_1, \ldots, x_m]$. The monomials span 1-dimensional invariant subspaces, and for $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$ and $h \in H$ we have that

$$h \cdot x^\alpha = \left(\prod_{i=1}^{m} g_i(h)^{\alpha_i}\right) x^\alpha.$$

It follows that the map $\mathbb{N}_0^m \to S(V)$, $\alpha \mapsto x^\alpha$ induces an isomorphism of the semigroup algebras

$$\mathbb{C}[\mathcal{B}(\underline{g})] \xrightarrow{\cong} \mathbb{C}[x_1, \dots, x_m]^H. \tag{11}$$

The isomorphism (11) is an isomorphism of graded algebras. We may select as homogeneous generators of $S(V)^H$ the monomials $\{x^\alpha \mid \alpha \in \mathcal{A}(\mathcal{B}(\underline{g}))\}$. Then the presentation (7) of $S(V)^H$ is identified via (11) with the presentation (3) of the semigroup algebra $\mathbb{C}[\mathcal{B}(\underline{g})]$. So $\mu(\ker(\varphi)) = \mu(\ker(\pi_{\mathbb{C}}))$ (see (3) in Section 2 for the definition of $\pi_{\mathbb{C}} : \mathbb{C}[M] \to \mathbb{C}[\mathcal{B}(\underline{g})]$). By Corollary 2 we know that $\mu(\ker(\pi_{\mathbb{C}})) = c_{\mathrm{gr}}(\mathcal{B}(\underline{g}))$. Thus we have $\mu(\ker(\varphi)) = c_{\mathrm{gr}}(\mathcal{B}(\underline{g}))$. On the other hand applying Theorem 3 (i) for $\mu(\ker(\varphi))$ in the special case when $g_1, \dots, g_m$ are distinct (i.e., when $\mathcal{B}(\underline{g}) = \mathcal{B}(\mathrm{supp}(\underline{g}))$) we obtain the inequality (9) (by (11) the Krull dimension of $\mathbb{C}[x_1, \dots, x_m]^H$ equals the Krull dimension of $\mathbb{C}[\mathcal{B}(\underline{g})]$, and the latter coincides with the rank of the free abelian subgroup of $\mathbb{Z}^m$ generated by $\mathcal{B}(\underline{g})$). Combining (9) with Theorem 1 and Proposition 4 we get the inequality (8). The explanation of (11) shows also $b(G, V) = \mathsf{d}(\mathrm{supp}(\underline{g}))$, so Theorem 3 (ii) yields (10).

*Remark 8.* When $G \cong \mathbb{Z}^k$, the group $H$ in the above proof is an algebraic torus, and the results in [29] give various bounds for $|a_1|$ in Theorem 4 (i). Moreover, [30] characterizes the cases when $\mathbb{C}[\mathcal{B}(\underline{g})] \cong S(V)^H$ (for a torus $H$) is a polynomial ring, i.e., when $c_{\mathrm{gr}}(\mathcal{B}(\underline{g}) = 0$.

**Corollary 6.** *For any subset $G_0$ of a finite abelian group $G$ we have the inequalities*

$$c_{\mathrm{gr}}(\mathcal{B}(G_0)) \le 2\mathsf{d}(G_0) + 2 \le 2\mathsf{D}(G) \le 2|G|.$$

*Proof.* The first inequality is a special case of Theorem 4 (ii). To see the second inequality note the trivial inequality $\mathsf{d}(G_0) \le \mathsf{d}(G)$, and the well known equality $\mathsf{d}(G) + 1 = \mathsf{D}(G)$ (cf. [14, Proposition 5.1.3.2]).

It follows immediately from Definitions 1 and 2 that

$$c(S) \le \frac{1}{\min\{|a| : a \in \mathcal{A}(S)\}} c_{\mathrm{gr}}(S). \tag{12}$$

Therefore Theorem 4 implies bounds on the ordinary (not graded) catenary degree. For example, an immediate consequence of Corollary 6 and (12) is the following:

**Corollary 7.** *Let $G_0$ be a subset in a finite abelian group $G$. Then*

$$c(\mathcal{B}(G_0)) \le \frac{2\mathsf{d}(G_0) + 2}{\min\{|\alpha| : \alpha \in \mathcal{A}(\mathcal{B}(G_0))\}}.$$

As an application we recover the following known bound on $c(\mathcal{B}(G))$:

**Corollary 8.** [14, Theorem 3.4.10.5] *For any finite abelian group $G$ we have the inequality $c(\mathcal{B}(G)) \leq \mathsf{D}(G)$.*

*Proof.* The monoid isomorphism $\mathcal{B}(G) \cong \mathcal{B}(G \setminus \{1_G\}) \times \mathcal{B}(\{1_G\}) \cong \mathcal{B}(G \setminus \{1_G\}) \times \mathbb{N}_0$ implies that $c(\mathcal{B}(G)) = c(\mathcal{B}(G \setminus \{1_G\})$. For a nontrivial group $G$ the minimal degree of an atom in $\mathcal{B}(G \setminus \{1_G\})$ is 2, hence, Corollary 7 gives $c(\mathcal{B}(G \setminus \{1_G\}) \leq \frac{2\mathsf{d}(G)+2}{2} = \mathsf{d}(G) + 1 = \mathsf{D}(G)$.

*Example 2.* It is known that the bound in Corollary 8 is sharp for $G$ with $|G| \geq 3$ if and only if $G$ is cyclic or $G$ is an elementary 2-group by [14, Theorem 6.4.7] (see also [15], where the finite groups with $c(\mathcal{B}(G)) = \mathsf{D}(G) - 1$ are characterized). The inequality $c_{\mathrm{gr}}(\mathcal{B}(G_0)) \leq 2\mathsf{d}(G_0) + 2$ in Corollary 6, the inequality in Corollary 7, and the inequalities (8) and (10) in Theorem 4 are also sharp for these groups:

(i) Set $G_0 := \{1, -1\} \subset \mathbb{Z}/n\mathbb{Z}$, $S := \mathcal{B}(G_0)$. Then $\mathcal{A}(S) = \{(n, 0), (0, n), (1, 1)\}$. The defining congruence $\sim_S$ of $S$ is generated by $(x^n_{(1,1)}, x_{(n,0)}x_{(0,n)})$ (a single generator). We have $\mathsf{d}(G_0) = n - 1$ and $c_{\mathrm{gr}}(S) = 2n$, whereas $\min\{|\alpha| \colon \alpha \in \mathcal{A}(S)\} = 2$ and $\max\{|\alpha| \colon \alpha \in \mathcal{A}(S)\} = n$.

(ii) Let $e_1, \dots, e_n$ be a basis of the elementary 2-group of rank $n \geq 2$, and $G_0 := \{e_1 + \cdots + e_n, e_1, \dots, e_n\}$, $S := \mathcal{B}(G_0)$. Then $\mathcal{A}(S) = \{a_1 := (1, 1, \dots, 1), a_2 := (2, 0, \dots, 0), a_3 := (0, 2, 0, \dots, 0), \dots, a_{n+2} := (0, \dots, 0, 2)\}$. The defining congruence of $S$ is generated by $(x^2_{a_1}, x_{a_2} \cdots x_{a_{n+2}})$. We have $\mathsf{d}(G_0) = n$ and $c_{\mathrm{gr}}(S) = 2n + 2$, whereas $\min\{|\alpha| \colon \alpha \in \mathcal{A}(S)\} = 2$ and $\max\{|\alpha| \colon \alpha \in \mathcal{A}(S)\} = n + 1$.

## 7 Relation to Toric Varieties

The quotient construction of toric varieties (cf. [6]) represents a toric variety as the categorical quotient of a Zariski open subset in a vector space endowed with an action of a diagonalizable group (see [8] for background on toric varieties). Rings of invariants are at the basis of quotient constructions in algebraic geometry. In the proof of Theorem 4, we recalled that the ring of invariants $\mathbb{C}[x_1, \dots, x_m]^H$ of a diagonalizable group action is isomorphic to a semigroup ring $\mathbb{C}[\mathcal{B}(\underline{g})]$ of a block monoid. Therefore the results in Sections 4, 5, 6 have relevance for toric varieties.

In more details, the coordinate rings of affine toric varieties with no torus factors are the semigroup rings (over $\mathbb{C}$) of reduced, affine Krull monoids. This class of rings (up to isomorphism) is the same as the class of rings of invariants $\mathbb{C}[x_1, \dots, x_m]^H$, where $H$ is an abelian group, and each variable spans an $H$-invariant subspace (see for example [3, Corollary 5.19]), which is the same as the class of rings of the form $\mathbb{C}[\mathcal{B}(\underline{g})]$.

Projective toric varieties can be constructed as the projective spectrum of semigroup algebras of reduced affine Krull monoids, see for example [20, Chapter

10], [8, Theorem 14.2.13]. Namely, take $\underline{g} = (g_1, \dots, g_m) \in G^m$ such that $\mathcal{B}(\underline{g}) = \{0\}$, and fix an element $h \in G$. Endow the monoid $\mathcal{B}((\underline{g}, h))$ with the grading given by $\mathcal{B}((\underline{g}, h))_d = \{\alpha \in \mathcal{B}((\underline{g}, h)) \subseteq \mathbb{N}_0^{m+1} \mid \alpha_{m+1} = d\}$, $d = 0, 1, 2, \dots$. Then $\mathbb{C}[\mathcal{B}((\underline{g}, h))]$ becomes a graded algebra, whose projective spectrum is a projective toric variety.

*Example 3.* We reformulate a result on presentations of homogeneous coordinate rings of projective toric quiver varieties from [12] in the terminology of the present paper. Let $\Gamma$ be an acyclic quiver (i.e., a finite directed graph having no oriented cycles), with vertex set $\{1, \dots, k\}$ and arrow set $\{e_1, \dots, e_m\}$. For an arrow $e_i$ denote by $s(e_i)$ the starting vertex of $e_i$, and denote by $t(e_i)$ the terminating vertex of $e_i$. In the additive group $\mathbb{Z}^k$ consider the elements $g_i = (g_{i1}, \dots, g_{ik})$, $i = 1, \dots, m$ given by

$$g_{ij} = \begin{cases} -1, & \text{if } j = s(e_i) \\ 1 & \text{if } j = t(e_i) \\ 0 & \text{otherwise.} \end{cases}$$

Pick an element $h \in \mathbb{Z}^k$ whose additive inverse is contained in the subgroup of $\mathbb{Z}^k$ generated by $g_1, \dots, g_m$. Then [12, Theorem 9.3] asserts that the catenary degree $c(\mathcal{B}((\underline{g}, h)))$ of $\mathcal{B}((\underline{g}, h))$ is at most 3. Moreover, it is shown in [13] that if we assume in addition that if $r(\mathcal{B}((\underline{g}, h))) \leq 5$ (i.e., the corresponding toric variety has dimension at most 4), then $c(\overline{\mathcal{B}}((\underline{g}, h))) \leq 2$ with essentially one exception. We mention that presentations of the coordinate ring of affine toric quiver varieties are studied in [19].

Well known open conjectures (of increasing strength) in combinatorial commutative algebra are the following (called sometimes Bøgvad's conjecture; see [27, Conjecture 13.19] or [2]): Given a smooth, projectively normal projective toric variety, its

(i) vanishing ideal is generated by quadratic elements.
(ii) homogeneous coordinate ring is Koszul.
(iii) vanishing ideal has a quadratic Göbner basis.

For a finite subset $G_0$ of $G$ with $\mathcal{B}(G_0) = \{0\}$ and an element $h$ whose inverse belongs to the subgroup generated by $G_0$, the monoid $\mathcal{B}(G_0 \cup \{h\})$ is endowed with the grading such that the degree $d$ component consists of the elements $\alpha$ in $\mathcal{B}(G_0 \cup \{h\})$ with $\alpha(h) = d$. Suppose that $\mathcal{B}(G_0 \cup \{h\})$ has a quadratic Gröbner system. According to the above conjecture this is expected to happen when $\mathcal{B}(G_0 \cup \{h\})$ is generated in degree 1 (so $\mathcal{B}(G_0 \cup \{h\})$ is half-factorial in the sense of factorization theory), and the projective spectrum of $\mathbb{C}[\mathcal{B}(G_0 \cup \{h\})]$ is a smooth projective variety. (For instance, in the setup of Example 3 this holds by [17] for almost all choices of $h$ when $\Gamma$ is a bipartite directed graph with 3 source and 3 sink vertices.) Then for any $\underline{g}$ with $\text{supp}(\underline{g}) = G_0$ we have by Corollary 5 that $\mathcal{B}((\underline{g}, h))$ has a quadratic Gröbner basis, and hence the algebra $\mathbb{C}[\mathcal{B}((\underline{g}, h))]$ is Koszul (although its projective spectrum typically fails to be a smooth projective variety).

**Acknowledgements** I thank Kálmán Cziszter, Dániel Joó, and Szabolcs Mészáros for several discussions on the topic of this paper. I am also grateful to Alfred Geroldinger for helpful comments on the manuscript.

## References

1. Blanco, V., García-Sánchez, P.A., Geroldinger, A.: Semigroup-theoretical characterizations of arithmetical invariants with applications to numerical monoids and Krull monoids. Illinois J. Math. **55**, 1385–1414 (2011)
2. Bruns, W.: The quest for counterexamples in Toric geometry, Proc. CAAG 2010, Ramanujan Math. Soc. Lect. Notes Series No. 17, 1–17 (2013)
3. Bruns, W., Gubeladze, J.: Polytopes, Rings, and K-theory. Springer, New York (2009)
4. Chapman, S.T., García-Sánchez, P.A., Llena, D., Ponomarenko, V., Rosales, J.C.: The catenary and tame degree in finitely generated commutative cancellative monoids. Manuscripta Math. **120**, 253–264 (2006)
5. Conca, A., De Negri, E., Rossi, M.E.: Koszul algebras and regularity. In: Peeva, I. (ed.) Commutative Algebra: Expository Papers Dedicated to David Eisenbud on the Occasion of His 65th Birthday, pp. 285–315. Springer (2013)
6. Cox, D.: The homogeneous coordinate ring of a toric variety. J. Algebr. Geom. **4**, 15–50 (1995)
7. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms. Springer, New York, Berlin, Heidelberg (1992)
8. Cox, D., Little, J., Schenck, H.: Toric Varieties. Amer. Math. Soc, Providence, RI (2010)
9. Cziszter, K., Domokos, M., Geroldinger, A.: The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics. In: Chapman, S.T., Fontana, M., Geroldinger, A., Olberding, B. (eds.), Multiplicative Ideal Theory and Factorization Theory, pp. 43–95, Springer (2016)
10. Derksen, H.: Degree bounds for syzygies of invariants. Adv. Math. **185**, 207–214 (2004)
11. Derksen, H., Kemper, G.: Computational Invariant Theory, Encyclopaedia of Mathematical Sciences 130. Springer, Berlin, Heidelberg, New York (2002)
12. Domokos, M., Joó, D.: On the equations and classification of toric quiver varieties. Proc. Royal Soc. Edinburgh: Sect. A Math. **146**, 265–295 (2016)
13. Domokos, M., Joó, D.: Toric quiver cells. arXiv:1609.03618
14. Geroldinger, A., Halter-Koch, F.: Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics, Vol. 278, Chapman & Hall/CRC (2006)
15. Geroldinger, A., Zhong, Q.: The catenary degree of Krull monoids II. J. Australian Math. Soc. **98**, 324–354 (2015)
16. Gilmer, R.: Commutative Semigroup Rings. The University of Chicago Press (1984)
17. Haase, C., Paffenholz, A.: Quadratic Gröbner bases for smooth $3 \times 3$ transportation polytopes. J. Algebr. Comb. **30**, 477–489 (2009)
18. Herzog, J.: Generators and relations of abelian semigroups and semigroup rings. Manuscripta Math. **3**, 175–193 (1970)
19. Joó, D.: Complete intersection quiver settings with one dimensional vertices. Algebr. Represent. Theory **16**, 1109–1133 (2013)
20. Miller, E., Sturmfels, B.: Combinatorial Commutative Algebra, Graduate Texts in Mathematics, Vol. 227. Springer (2005)
21. Ohsugi, H., Hibi, T.: Toric rings and ideals of nested configurations. J. Commut. Algebra **2**, 187–208 (2010)
22. Philipp, A.: A characterization of arithmetical invariants by the monoid of relations. Semigroup Forum **81**, 424–434 (2010)
23. Philipp, A.: A characterization of arithmetical invariants by the monoid of relations II: the monotone catenary degree and applications to semigroup rings. Semigroup Forum **90**, 220–250 (2015)

24. Polishchuk, A., Positelski, L.: Quadratic Algebras, University Lecture Series 37. AMS, Providence, Rhode Island (2005)
25. Rédei, L.: The theory of Finitely Generated Commutative Semigroups. Pergamon, Oxford-Edinburgh-New York (1965)
26. Shibuta, T.: Gröbner bases of contraction ideals. J. Algebr. Comb. **36**, 1–19 (2012)
27. Sturmfels, B.: Gröbner Bases and Convex Polytopes, University Lecture Series 8. AMS, Providence, Rhode Island (1996)
28. Villareal, R.H.: Monomial Algebras, CRC Press, Chapman and Hall Book, Monographs and Research Notes in Mathematics, Second edition, Boca Raton, Florida (2015)
29. Wehlau, D.: Constructive invariant theory for tori. Ann. Inst. Fourier Grenoble **43**, 1055–1066 (1993)
30. Wehlau, D.: When is a ring of torus invariants a polynomial ring? Manuscripta Math. **82**, 161–170 (1994)

# A Bazzoni-Type Theorem for Multiplicative Lattices

**Tiberiu Dumitrescu**

**Abstract** We prove a Bazzoni-type theorem for multiplicative lattices thus unifying several ring/monoid theoretic results of this type.

**Keywords** Prüfer domain · Multiplicative lattice

**2010 Mathematics Subject Classification** Primary 06F05 · Secondary 13F15

## 1 Introduction

Let $D$ be an integral domain. Consider the following two assertions:

(i) If $I$ is an ideal of $D$ whose localizations at the maximal ideals are finitely generated, then $I$ is finitely generated.

(ii) Every $x \in D - \{0\}$ belongs to only finitely many maximal ideals of $D$.

While $(ii) \Rightarrow (i)$ is well-known and easy to prove, Bazzoni [3, p. 630] conjectured that the converse is true for Prüfer domains. Recall that $D$ is a *Prüfer domain* if every finitely generated ideal $I$ of $D$ is locally principal.

Holland et al. [10, Theorem 10] proved Bazzoni's conjecture for Prüfer domains using techniques from lattice-ordered groups theory and McGovern [14, Theorem 11] proved the same result using a direct ring theoretic approach. Halter-Koch [9, Theorem 6.11] proved Bazzoni's conjecture for $r$-Prüfer monoids (see Section 4). Zafrullah [16, Proposition 5] proved Bazzoni's conjecture for Prüfer $v$-multiplication domains. Finocchiaro and Tartarone [6, Theorem 4.5] proved Bazzoni's conjecture for almost Prüfer ring extensions (see Section 3). Recently, Chang and Hamdi [4, Theorem 2.4] proved Bazzoni's conjecture for almost Prüfer $v$-multiplication domains (see Section 4).

---

T. Dumitrescu (✉)
Facultatea de Matematica si Informatica, University of Bucharest,
14 Academiei Street, 010014 Bucharest, RO, Romania
e-mail: tiberiu@fmi.unibuc.ro



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_6

The purpose of this paper is to prove a Bazzoni-type theorem for multiplicative lattices (see Section 2), thus unifying the results mentioned above (see Sections 3 and 4). Our standard references are [1, 7, 8].

## 2 Main Result

We use an abstract ideal theory approach, so we work with multiplicative lattices.

**Definition 1.** A *multiplicative lattice* is a complete lattice $(L, \leq)$ (with bottom element 0 and top element 1) which is also a multiplicative commutative monoid with identity 1 (the top element) and satisfies $a(\bigvee b_\alpha) = \bigvee ab_\alpha$ for each $a, b_\alpha \in L$.

Let $L$ be a multiplicative lattice. The elements in $L - \{1\}$ are said to be *proper*. Denote by $Max(L)$ the set of maximal elements of $L$. For $x, y \in L$, set $(y : x) = \bigvee\{a \in L;\ ax \leq y\}$.

We recall some standard terminology.

**Definition 2.** Let $L$ be a multiplicative lattice and let $x, p \in L$.

(1) $p$ is *prime* if $p \neq 1$ and for all $a, b \in L$, $ab \leq p$ implies $a \leq p$ or $b \leq p$. It follows easily that every maximal element is prime.

(2) $x$ is *compact* if whenever $x \leq \bigvee_{y \in S} y$ with $S \subseteq L$, we have $x \leq \bigvee_{y \in T} y$ for some finite subset $T$ of $S$.

(3) $L$ is a *$C$-lattice* if the set $L^*$ of compact elements of $L$ is closed under multiplication, $1 \in L^*$ and every element in $L$ is a join of compact elements.

(4) $x$ is *meet-principal* if $y \wedge zx = ((y : x) \wedge z)x$ for all $y, z \in L$ (in particular $(y : x)x = x \wedge y$).

(5) $x$ is *join-principal* if $y \vee (z : x) = ((yx \vee z) : x)$ for all $y, z \in L$ (in particular $(xy : x) = y \vee (0 : x)$).

(6) $x$ is *cancellative* if for all $y, z \in L$, $xy = xz$ implies $y = z$.

(7) $x$ is *CMP* (ad hoc name) if $x$ is cancellative and meet-principal.

(8) $L$ is a *lattice domain* if $(0 : a) = 0$ for all $a \in L - \{0\}$.

In the sequel, we work with $C$-lattices and their localization theory. Let $L$ be a $C$-lattice. For $p \in L$ a prime element and $x \in L$, we set

$$x_p = \bigvee\{a \in L^*;\ ab \leq x \text{ for some } b \in L^* \text{ with } b \nleq p\}.$$

Then $L_p := \{x_p;\ x \in L\}$ is again a lattice with multiplication $(x_p, y_p) \mapsto (xy)_p = (x_p y_p)_p$, join $\{(b_\alpha)_p\} \mapsto (\bigvee(b_\alpha)_p)_p = (\bigvee b_\alpha)_p$ and meet $\{(b_\alpha)_p\} \mapsto (\bigwedge(b_\alpha)_p)_p$. The next lemma collects several basic properties.

**Lemma 3.** *Let $L$ be a $C$-lattice, let $x, y \in L$ and let $p \in L$ be a prime element.*

(1) $x_p = 1$ *if and only if* $x \nleq p$.

(2) $(x \wedge y)_p = x_p \wedge y_p$.

(3) *If $x$ is compact, then $(y : x)_p = (y_p : x_p)$.*

(4) $x = y$ *if and only if* $x_m = y_m$ *for each* $m \in Max(L)$.

(5) *A cancellative element $x$ is CMP if and only if $(y : x)x = x \wedge y$ for all $y \in L$.*

(6) *If $x$ is compact, then $x_p$ is compact in $L_p$. Conversely, if $x_p$ is compact in $L_p$, then $x_p = c_p$ for some compact element $c \leq x$.*

(7) *If $x$ and $y$ are CMP elements, then so is $xy$.*

(8) *If $x$ is compact, $y$ is CMP and $x \leq y$, then $(x : y)$ is compact.*

*Proof.* For (1–4) see [11, pp. 201–202], for (5) see [15, Lemma 2.10], while (6–7) follow easily from definitions. We prove (8). Note that $(x : y)y = x \wedge y = x$. Suppose that $(x : y) \leq \bigvee_{i \in A} z_i$. Then $x = (x : y)y \leq \bigvee_{i \in A} z_i y$, so $(x : y)y \leq \bigvee_{i \in B} z_i y$ for some finite subset $B$ of $A$. Cancel $y$ to get $(x : y) \leq \bigvee_{i \in B} z_i$. □

Say that $x$ and $y \in L$ are *comaximal* if $x \vee y = 1$. Clearly, $x \vee yz = 1$ if and only if $x \vee y = 1$ and $x \vee z = 1$. When $t \leq u$ we say that $t$ is *below* $u$ or that $u$ is *above* $t$.

**Lemma 4.** *Let $L$ be a $C$-lattice and $z \in L - \{1\}$ a compact element such that $\{m \in Max(L);\ z \leq m\}$ is infinite. There exists an infinite set $\{a_n;\ n \geq 1\}$ of pairwise comaximal proper compact elements such that $z \leq a_n$ for each $n$.*

*Proof.* We may clearly assume that $z = 0$ (just change $L$ by $\{x \in L;\ x \geq z\}$). Say that a proper compact element $h$ is *big* (ad hoc name) if $h$ is below only one maximal element $M(h)$. We separate in two cases.

Case (1): *Every proper compact element is below some big compact element*. We proceed by induction. Suppose that $n \geq 1$ and we already have big compacts $a_1,...,a_n$ such that $M(a_1),...,M(a_n)$ are distinct maximal elements (for $n = 1$ just pick an arbitrary big compact $a_1$). Let $p$ be a maximal element other than $M(a_1),...,M(a_n)$. There exists a compact element $c \leq p$ such that $c \nleq M(a_i)$ for $1 \leq i \leq n$ (take $c = c_1 \vee \cdots \vee c_n$ where each $c_i \in L^*$ satisfies $c_i \leq p$ and $c_i \nleq M(a_i)$). Then take a big compact element $a_{n+1} \geq c$. This way we construct an infinite set $\{a_n;\ n \geq 1\}$ of big compacts such that all $M(a_n)$'s are distinct. Hence the $a_n$'s are pairwise comaximal.

Case (2): *There exists a proper compact element $a_0$ which is not below any big compact element*. Clearly every proper compact above $a_0$ inherits this property. Pick two distinct maximal elements $p$ and $q$ above $a_0$. As $L$ is a $C$-lattice, there exist two comaximal compacts $a_1 \leq p$ and $b_1 \leq q$ (note that $p \vee q = 1$, express $p$ and $q$ as joins of compact elements and use the fact that 1 is compact). Repeating this argument for $a_1$, there exist two comaximal proper compacts $a_2 \geq a_1$ and $b_2 \geq a_1$. Note that $b_2$ and $b_1$ are comaximal. Thus we construct inductively an infinite set $\{b_n;\ n \geq 1\}$ of pairwise comaximal proper compact elements. □

In a $C$-lattice $L$, we say that an element $x$ is *locally compact* if $x_m$ is compact in $L_m$ for each $m \in Max(L)$. We state our main result which is a Bazzoni-type theorem for $C$-lattices.

**Theorem 5.** *Let L be a C-lattice domain satisfying the following two conditions:*

$(a)$ *every nonzero element is above some cancellative compact element, and*

$(b)$ *every compact element $x \neq 1$ has some power $x^n$ below some proper CMP element.*

*Then the following conditions are equivalent:*

$(i)$ *Every locally compact element of L is compact.*

$(ii)$ *Every nonzero element is below at most finitely many maximal elements.*

*Proof.* $(ii) \Rightarrow (i)$. Although this part is well-known and easy, we include a proof for the reader's convenience. Let $x$ be a nonzero locally compact element of $L$ and let $a \leq x$ be a nonzero compact element. By $(ii)$, there are only finitely many maximal elements above $a$, say $m_1,...,m_k$. For each $i$ between 1 and $k$, pick a compact element $c_i \leq x$ such that $x_{m_i} = (c_i)_{m_i}$. A local check shows that $x = a \vee c_1 \vee \cdots \vee c_k$, so $x$ is compact. Note that this part works for any $C$-lattice.

$(i) \Rightarrow (ii)$. Deny, so suppose that some nonzero element $c$ is below infinitely many maximal elements. By hypothesis $(a)$, we may assume that $c$ is a cancellative compact element. By Lemma 4 and hypothesis $(b)$, there exist an infinite set $\{b_n;\ n \geq 1\}$ of proper pairwise comaximal CMP elements and integers $k_n \geq 1$ such that $c^{k_n} \leq b_n$ for $n \geq 1$ ($k_n$ minimal with this property). Restricting to a subsequence, we may assume that $k_n \leq k_{n+1}$ for all $n$. We then have $c^{k_n} \leq b_1 \wedge \cdots \wedge b_n = b_1 \cdots b_n$ for all $n$.

Claim $(*)$ : *The element $a := \bigvee_{n\geq 1}(c^{k_n} : b_1 \cdots b_n)$ is locally compact.*
Pick $m \in \mathrm{Max}(L)$. Since the $b_n$'s are pairwise comaximal, $m$ is above at most one of them. Assume first that $m \geq b_s$. Since each product $b_1 \cdots b_n$ is compact, we get

$$a_m = (\bigvee_{n\geq 1}((c^{k_n})_m : (b_1 \cdots b_n)_m))_m = (c^{k_1} \vee (c^{k_s} : b_s))_m$$

which is compact in $L_m$, cf. Lemma 3. Similarly, when $m$ is above no $b_n$, we get $a_m = (c^{k_1})_m$, so $a_m$ is compact in $L_m$, hence Claim $(*)$ is proved. By $(i)$, $a$ is compact. So $a = \bigvee_{n=1}^{q}(c^{k_n} : b_1 \cdots b_n)$ for some $q \geq 1$. We get

$$(c^{k_{q+1}} : b_1 \cdots b_{q+1}) \leq (c^{k_1} : b_1 \cdots b_q)$$

so multiplying by $b_1 \cdots b_{q+1}$ (which is a CMP element) and taking into account that $c^{k_{q+1}} \leq b_1 \cdots b_{q+1}$, we get

$$c^{k_{q+1}} \leq (c^{k_1} : b_1 \cdots b_q)b_1 \cdots b_{q+1} \leq c^{k_1} b_{q+1}.$$

Since $k_{q+1} \geq k_1$ and $c^{k_1}$ is cancellative, we get $c^{k_{q+1}-k_1} \leq b_{q+1}$, which is a contradiction since $k_{q+1}$ was minimal with $c^{k_{q+1}} \leq b_{q+1}$. □

Recall that a $C$-lattice domain is a *Prüfer lattice* if every compact element is principal (i.e., meet-principal and join-principal). In a $C$-lattice domain, every nonzero join-principal element $x$ is cancellative (because $(yx : x) = y \vee (0 : x) = y$ for each $y$). So in a Prüfer lattice domain every nonzero compact element is CMP.

**Corollary 6.** *Let L be a C-lattice domain in which every nonzero compact element is CMP (e.g., a Prüfer lattice domain). Then conditions* $(i)$ *and* $(ii)$ *of Theorem 5 are equivalent.*

Bazzoni's conjecture for Prüfer domains [10, Theorem 10] (see Introduction) follows from Corollary 6 since the ideal lattice of a Prüfer domain is clearly a Prüfer lattice.

## 3 Almost Prüfer Extensions

We recall several definitions from [6, 12]. Let $A \subseteq B$ be a commutative ring extension and $I$ an ideal of $A$. Then $I$ is called $B$*-regular* if $IB = B$ and $I$ is called $B$*-invertible* if $IJ = A$ for some $A$-submodule $J$ of $B$. Every $B$-invertible ideal is $B$-regular, since $A = IJ \subseteq IB$ implies $IB = B$. We say that $A \subseteq B$ is an *almost Prüfer extension* if every finitely generated $B$-regular ideal of $A$ is $B$-invertible.

Finocchiaro and Tartarone [6, Theorem 4.5] proved Bazzoni's conjecture for almost Prüfer ring extensions. We state their result and derive it from Corollary 6.

**Theorem 7.** (Finocchiaro and Tartarone) *If* $A \subseteq B$ *is an almost Prüfer extension, the following are equivalent:*

$(i)$ *Every* $B$*-regular locally principal ideal of* $A$ *is* $B$*-invertible.*

$(ii)$ *Every* $B$*-regular ideal of* $A$ *is contained in only finitely many maximal ideals of* $A$*.*

*Proof.* It is well-known and easy to prove that $(ii)$ implies $(i)$, see [6, Corollary 3.5]. We prove the converse. Let $L$ be the set of all $B$-regular ideals of $A$ together with the zero ideal and order $L$ by inclusion. As shown in [15, Lemma 7.1], $L$ is a $C$-lattice domain under usual ideal multiplication, where the join is the ideal sum and the meet is the ideal intersection except the case when we get a non-$B$-regular ideal when we put $\bigwedge = 0$. By [15, Lemma 7.1], the set $L^*$ of compact elements in $L$ is exactly the set of ($B$-regular) finitely generated ideals of $A$ together with the zero ideal. After this preparation it becomes clear that $[(i) \Rightarrow (ii)]$ follows from Corollary 6 provided we prove the two claims below. Write $x \in L$ as $\widehat{x}$ when considered as an ideal of $A$.

*Claim* 1: *Every nonzero compact element of L is a CMP element.*
Let $c$ be a nonzero compact element of $L$. As $A \subseteq B$ is almost Prüfer, $\widehat{c}$ is a $B$-invertible ideal, so $\widehat{c}J = A$ for some $A$-submodule $J$ of $B$. Then $c$ is clearly cancellative. By Lemma 3, it suffices to show that $(x : c)c = x \wedge c$ for each $x \in L$. Changing $x$ by $x \wedge c$, we may assume that $x \leq c$. We have $\widehat{x} = \widehat{x}J\widehat{c}$, so $x = yc$ where $y \in L$ is such that $\widehat{y} = \widehat{x}J$ (note that $\widehat{x}J \subseteq A$). From $x = yc$ we get $y \leq (x : c)$, so $x = yc \leq (x : c)c \leq x$, thus $(x : c)c = x$.

*Claim* 2: *Every locally compact element of L is compact.*
Suppose that $c$ is a nonzero locally compact element of $L$. Let $m$ be a maximal element of $L$, that is, $\widehat{m}$ is a $B$-regular maximal ideal of $A$. So $c_m = \bigvee\{y \in L^*;\ ys \leq c$ for some $s \in L^*, s \nleq m\}$ is compact in the lattice $L_m = \{x_m;\ x \in L\}$. Then $c_m = h_m$ for

some $h \in L^*$. Extending these ideals in $A_{\widehat{m}}$, we get $\widehat{c}A_{\widehat{m}} = \widehat{c_m}A_{\widehat{m}} = \widehat{h_m}A_{\widehat{m}} = \widehat{h}A_{\widehat{m}}$. Since $A \subseteq B$ is almost Prüfer, $\widehat{h}$ is $B$-invertible. By [12, Proposition 2.3], $\widehat{h}A_{\widehat{m}} = \widehat{c}A_{\widehat{m}}$ is a principal ideal of $A_{\widehat{m}}$. Thus $\widehat{c}$ is a locally principal ideal of $A$. By $(i)$, $\widehat{c}$ is $B$-invertible, so $\widehat{c}$ is finitely generated, cf. [12, Proposition 2.3]. Thus $c$ is compact in $L$. □

## 4 Ideal Systems on Monoids and Integral Domains

Let $H$ be a commutative multiplicative monoid (with zero element 0 and unit element 1) such that every nonzero element of $H$ is cancellative and let $\mathcal{P}(H)$ be the power set of $H$. A map $r : \mathcal{P}(H) \to \mathcal{P}(H)$, $X \mapsto X_r$, is an *ideal system* on $H$ if the following conditions hold for all $X, Y \in \mathcal{P}(H)$ and $c \in H$:

$$(1)\ cX_r = (cX)_r,\ (2)\ X \subseteq X_r,\ (3)\ X \subseteq Y \text{ implies } X_r \subseteq Y_r,\ (4)\ (X_r)_r = X_r.$$

Then $X_r$ is called the *$r$-closure* of $X$ and a set of the form $X_r$ is called an $r$-ideal. An $r$-ideal $I$ is *$r$-finite* if $I = Y_r$ for some finite subset $Y$ of $I$. The ideal system $r$ is called *finitary* if $X_r = \bigcup\{Y_r;\ Y \subseteq X \text{ finite}\}$.

*Assume* that $r$ is finitary. A proper $r$-ideal $P$ is *prime* if, for $x, y \in H$, $xy \in P$ implies $x \in P$ or $y \in P$. The *localization of $H$ at $P$* is the fraction monoid $H_P = \{x/t;\ x \in H, t \in H - P\}$ which comes together with the finitary ideal system $r_P$ defined by $\{a_1/s_1, ..., a_n/s_n\}_{r_P} = (\{a_1, ..., a_n\}_r)_P$ for all $a_1, ..., a_n \in H$ and $s_1, ..., s_n \in H - P$. A *maximal $r$-ideal* is a maximal element of the set of proper $r$-ideals of $H$. Any proper $r$-ideal is contained in a maximal one and a maximal $r$-ideal is prime. A nonzero $r$-ideal $I$ is *$r$-invertible* if $I$ is $r$-finite and *$r$-locally principal* (i.e., $I_M = \{x/t;\ x \in I, t \in H - M\} = yH_M$ with $y \in I_M$ (depending on $M$) for all maximal $r$-ideals $M$). Next $H$ is an *$r$-Prüfer monoid* if every nonzero $r$-finite $r$-ideal of $H$ is $r$-invertible. For complete details we refer to [8].

Halter-Koch [9, Theorem 6.11] proved Bazzoni's conjecture for $r$-Prüfer monoids. We state his result and derive it from Corollary 6.

**Theorem 8.** (Halter-Koch) *If $H$ is an $r$-Prüfer monoid for some finitary ideal system $r$ on $H$, the following are equivalent.*

$(i)$ *Every $r$-locally principal $r$-ideal of $H$ is $r$-finite.*

$(ii)$ *Every nonzero $r$-ideal of $H$ is contained in only finitely many maximal $r$-ideals.*

*Proof.* It is well-known and easy to prove that $(ii)$ implies $(i)$. We prove the converse. Let $L$ be the set of all $r$-ideals of $H$ ordered by inclusion. As shown in [8, Chapter 8], $L$ is a $C$-lattice domain under $r$-ideal multiplication $(I, J) \mapsto (IJ)_r$, join $\bigvee\{J_\alpha\} := (\bigcup J_\alpha)_r$ and meet $\bigwedge\{J_\alpha\} := \bigcap J_\alpha$. By [15, Lemma 8.1], the set $L^*$ of compact elements in $L$ is exactly the set of $r$-finite $r$-ideals of $H$. After this preparation it becomes clear that $[(i) \Rightarrow (ii)]$ follows from Corollary 6 provided we prove the two claims below. Write $x \in L$ as $\widehat{x}$ when considered as an $r$-ideal of $H$.

*Claim* 1: *Every nonzero compact element of L is a CMP element.*
Let $c \in L$ be a nonzero compact, in other words $\widehat{c}$ is nonzero $r$-finite $r$-ideal. Since $H$ is $r$-Prüfer, $\widehat{c}$ is $r$-invertible. So $c$ is a CMP element of $L$, cf. [15, Lemma 8.2].

*Claim* 2: *Every locally compact element of L is compact.*
Suppose that $c$ is a locally compact element of $L$. Let $m$ be a maximal element of $L$, that is, $\widehat{m}$ is a maximal $r$-ideal of $H$. So $c_m = \bigvee\{y \in L^*;\ ys \leq c$ for some $s \in L^*, s \nleq m\}$ is compact in the lattice $L_m = \{x_m;\ x \in L\}$. Then $c_m = h_m$ for some $h \in L^*$. Switching to $H$, we have $(\widehat{c})_{\widehat{m}} = (\widehat{c_m})_{\widehat{m}} = (\widehat{h_m})_{\widehat{m}} = \widehat{h}_{\widehat{m}}$. Since $H$ is an $r$-Prüfer monoid, $\widehat{h}_{\widehat{m}}$ is a principal $r_{\widehat{m}}$-ideal of $H_{\widehat{m}}$, cf. [8, Theorem 12.3]. Thus $\widehat{c}$ is an $r$-locally principal $r$-ideal. By $(i)$, $\widehat{c}$ is $r$-finite, thus $c$ is compact in $L$. □

Next we present an application for integral domains. Let $D$ be an integral domain. The $t$ ideal system on $D$ is defined by $X_t = \bigcup\{Y_v;\ Y \subseteq X$ finite$\}$ for all $X \subseteq D$, where $Y_v = \bigcap\{(aD :_D b);\ a, b \in D, bY \subseteq aD\}$. Clearly $t$ is finitary, so the set $Max_t(D)$ of maximal $t$-ideals is nonempty, see [8, Chapter 11].

The $w$ ideal system on $D$ is defined by $X_w = \bigcap\{XD_M;\ M \in Max_t(D)\}$ for all $X \subseteq D$, where $XD_M$ is the ideal generated by $X$ in $D_M$. So a $w$-ideal is an ideal of the ring $D$. For $X \subseteq D$, we have $X_w = (XD)_w$ and $X_w D_M = XD_M$ for each $M \in Max_t(D)$. Moreover, $w$ is finitary and the set of maximal $w$-ideals is exactly $Max_t(D)$. A $w$-finite ideal has the form $((a_1, ..., a_n)D)_w$ for some $a_i$'s in $D$. And a nonzero $w$-ideal is $w$-*invertible* if it is $w$-finite and $t$-locally principal (i.e., $ID_M$ is a principal ideal of $D_M$ for each $M \in Max_t(D)$). For details on the $w$ ideal system we refer to [2, 5].

According to [13], $D$ is an *almost Prüfer v-multiplication domain* (in short *APVMD*) if for every $a_1, ..., a_n \in D - \{0\}$, the ideal $((a_1^k, ..., a_n^k)D)_w$ is $w$-invertible for some $k \geq 1$. Say that a $w$-ideal $I$ of $D$ is $t$-*locally finitely generated*, if $ID_M$ is a finitely generated ideal of $D_M$ for each $M \in Max_t(D)$.

Chang and Hamdi [4, Theorem 2.4] proved Bazzoni's conjecture for APVMDs. We state their result and derive it from Theorem 5.

**Theorem 9.** (Chang and Hamdi) *For an APVMD D, the following statements are equivalent:*

$(i)$ *Each nonzero t-locally finitely generated w-ideal of D is w-finite.*

$(ii)$ *Every nonzero ideal of D is contained in only finitely many maximal t-ideals.*

*Proof.* It is well-known and easy to prove that $(ii)$ implies $(i)$, see for instance the proof of (3) ⇒ (1) in [4, Theorem 2.4]. We prove that $(i)$ implies $(ii)$. Let $L$ be the set of all $w$-ideals of $D$ ordered by inclusion. As shown in [8, Chapter 8], $L$ is a $C$-lattice domain under $w$-ideal multiplication $(I, J) \mapsto (IJ)_w$, join $\bigvee\{J_\alpha\} := (\bigcup J_\alpha)_w$ and meet $\bigwedge\{J_\alpha\} := \bigcap J_\alpha$. By [15, Lemma 8.1], the set $L^*$ of compact elements in $L$ is exactly the set of $w$-finite ideals of $D$. Condition $(a)$ of Theorem 5 holds clearly for $L$ (any nonzero ideal contains a nonzero principal ideal). After this preparation it becomes clear that $[(i) \Rightarrow (ii)]$ follows from Theorem 5 provided we prove the two claims below. Write $x \in L$ as $\widehat{x}$ when considered as a $w$-ideal of $D$.

*Claim* 1: *Every* $d \in L^* - \{1\}$ *has some power* $d^n$ *below some proper CMP element.*
Let $d \in L^* - \{1\}$. Then $\widehat{d} = (a_1, ..., a_k)_w$ for some elements $a_i \in \widehat{d}$. Since $D$ is an APVMD, $(a_1^s, ..., a_k^s)_w$ is $w$-invertible for some $s \geq 1$. If $(a_1^s, ..., a_k^s)_w = \widehat{f}$ with $f \in L$, then $f$ is a proper CMP element of $L$, cf. [15, Lemma 8.2]. Moreover $d^{sk} \leq f$, so Claim 1 is proved.

*Claim* 2: *Every locally compact element of L is compact.*
Suppose that $c$ is a locally compact element of $L$. Let $m$ be a maximal element of $L$, that is, $\widehat{m}$ is a maximal $w$-ideal of $D$. So $c_m = \bigvee\{y \in L^*;\ ys \leq c$ for some $s \in L^*, s \not\leq m\}$ is compact in the lattice $L_m = \{x_m;\ x \in L\}$. Then $c_m = h_m$ for some $h \in L^*$. Hence $\widehat{h} = (b_1, ..., b_n)_w$ for some elements $b_i \in \widehat{h}$. Switching to $D$, we have

$$\widehat{c}D_{\widehat{m}} = \widehat{c_m}D_{\widehat{m}} = (\widehat{h_m})D_{\widehat{m}} = \widehat{h}D_{\widehat{m}} = (b_1, ..., b_n)_w D_{\widehat{m}} = (b_1, ..., b_n)D_{\widehat{m}}.$$

Thus $\widehat{c}$ is a $t$-locally finitely generated ideal of $D$. By $(i)$, $\widehat{c}$ is $w$-finite, thus $c$ is compact in $L$. □

**Acknowledgements** I thank the referee for the close reading of the manuscript and for the detailed report which heavily improved the quality of this paper.

## References

1. Anderson, D.D.: Abstract commutative ideal theory without chain conditions. Algebra Univ. **6**, 131–145 (1976)
2. Anderson, D.D., Cook, S.J.: Two star-operations and their induced lattices. Comm. Algebra **28**, 2461–2475 (2000)
3. Bazzoni, S.: Class semigroups of Prüfer domains. J. Algebra **184**, 613–631 (1996)
4. Chang, G.W. Hamdi, H.: Bazzoni's conjecture and almost Prüfer domains, to appear in Comm. Algebra
5. Fanggui, W., McCasland, R.L.: On w-modules over strong Mori domains. Comm. Algebra **25**, 1285–1306 (1997)
6. Finnochiaro, C., Tartarone, F.: Invertibility of ideals in Prüfer extensions. Comm. Algebra **45**, 4521–4527 (2017)
7. Gilmer, R.: Multiplicative Ideal Theory. Marcel Dekker, New York (1972)
8. Halter-Koch, F.: Ideal System. An Introduction to Multiplicative Ideal Theory, Marcel Dekker, New York (1998)
9. Halter-Koch, F.: Clifford semigroups of ideals in monoids and domains. Forum Math. **21**, 1001–1020 (2009)
10. Holland, W.C., Martinez, J., McGovern, W.W., Tesemma, M.: Bazzoni's conjecture. J. Algebra **320**, 1764–1768 (2008)
11. Jayaram, C., Johnson, E.G.: S-prime elements in multiplicative lattices. Periodica Math. Hungarica **31**, 201–208 (1995)
12. Knebusch, M., Zhang, D.: Manis Valuations and Prüfer Extensions I: A New Chapter in Commutative Algebra. Springer, Berlin, Heidelberg (2002)
13. Lewin, R.L.: Generalizations of GCD-domains and related topics, Ph.D. Thesis, University of Iowa (1991)

14. McGovern, W.W.: Prüfer domains with Clifford class semigroup. J. Comm. Algebra **3**, 551–559 (2011)
15. Olberding, B., Reinhart, A.: Radical factorization in commutative rings, monoids and multiplicative lattices, Math. (2018). arXiv: 1811.00242v1, math.AC
16. Zafrullah, M.: t-invertibility and Bazzoni-like statements. J. Pure Appl. Algebra **214**, 654–657 (2010)

# What is the Spectral Category?

**María José Arroyo Paniagua, Alberto Facchini, Marino Gran, and George Janelidze**

**Abstract** For a category $\mathcal{C}$ with finite limits and a class $\mathcal{S}$ of monomorphisms in $\mathcal{C}$ that is pullback stable, contains all isomorphisms, is closed under composition, and has the strong left cancellation property, we use pullback stable $\mathcal{S}$-essential monomorphisms in $\mathcal{C}$ to construct a spectral category $\mathrm{Spec}(\mathcal{C}, \mathcal{S})$. We show that it has finite limits and that the canonical functor $\mathcal{C} \to \mathrm{Spec}(\mathcal{C}, \mathcal{S})$ preserves finite limits. When $\mathcal{C}$ is a normal category, assuming for simplicity that $\mathcal{S}$ is the class of all monomorphisms in $\mathcal{C}$, we show that pullback stable $\mathcal{S}$-essential monomorphisms are the same as what we call subobject-essential monomorphisms.

**Keywords** Spectral category · Normal category · Essential monomorphism

M. J. Arroyo Paniagua
Departamento de Matemáticas, Universidad Autónoma Metropolitana, Unidad Iztapalapa, Ciudad de México, México
e-mail: mariajose.mja@gmail.com

A. Facchini (✉)
Dipartimento di Matematica "Tullio Levi-Civita", Università di Padova, Padova, Italy
e-mail: facchini@math.unipd.it

M. Gran
Institut de Recherche en Mathématique et Physique, Université catholique de Louvain, 1348 Louvain-la-Neuve, Belgique
e-mail: marino.gran@uclouvain.be

G. Janelidze
Department of Mathematics and Applied Mathematics, University of Cape Town, Rondebosch 7700, South Africa
e-mail: george.janelidze@uct.ac.za



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*, Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_7

# 1 Introduction

The *spectral category* $\mathrm{Spec}(\mathcal{C})$ of a Grothendieck category $\mathcal{C}$ was introduced by Gabriel and Oberst [11]. According to the Abstract of [11], $\mathrm{Spec}(\mathcal{C})$ is obtained from $\mathcal{C}$ by formally inverting all essential monomorphisms. Although there is no reference to Gabriel and Zisman [12], the definition given in Section 1.2 of [11] is, in fact, a construction based on the fact that the class of essential monomorphisms in $\mathcal{C}$ admits the calculus of right fractions. Indeed, it presents the abelian groups $\mathrm{Hom}_{\mathrm{Spec}(\mathcal{C})}(A, B)$ (for all $A, B \in \mathrm{Ob}(\mathcal{C}) = \mathrm{Ob}(\mathrm{Spec}(\mathcal{C}))$) as directed colimits

$$\mathrm{Hom}_{\mathrm{Spec}(\mathcal{C})}(A, B) = \mathrm{colim}\,\mathrm{Hom}_{\mathcal{C}}(A', B)$$

taken over all subobjects $A'$ of $A$. It is also easy to see that the spectral category $\mathrm{Spec}(\mathcal{C})$ can equivalently be defined as the quotient category of the category of injective objects in $\mathcal{C}$ modulo the ideal consisting of all morphisms in $\mathcal{C}$ whose kernels are essential monomorphisms. Although this is not mentioned in [11], it is said there that $\mathrm{Spec}(\mathcal{C})$ is a replacement of the *spectrum* of $\mathcal{C}$, which is defined (when $\mathcal{C}$ is the category of modules over a ring) as the collection of isomorphism classes of indecomposable injective objects.

Introducing the spectral category of a Grothendieck category $\mathcal{C}$ can also be motivated by non-functoriality of injective envelopes as follows. For each object $C$ in $\mathcal{C}$, let us fix an injective envelope (=injective hull) $\iota_C : C \to E(C)$ of it. One might expect $E$ to become an endofunctor of $\mathcal{C}$, and $\iota$ to become a natural transformation $1_{\mathcal{C}} \to E$. However, there are strong negative results against these expectations:

- According to Proposition 1.12 in [13], $E$ cannot be made a functor even when $\mathcal{C}$ is the category of abelian groups.
- Let $R$ be a ring and $\mathcal{C}$ the category of $R$-modules. The ring $R$ can be chosen in such a way that not all $R$-modules are injective, but $E$ can be made an endofunctor of $\mathcal{C}$ (see [13, Exercise 24, p. 48] or [8]), but even in those cases $\iota$ will not become a natural transformation $1_{\mathcal{C}} \to E$. This follows from a very general Theorem 3.2 of [2].

On the other hand, the canonical functor $P : \mathcal{C} \to \mathrm{Spec}(\mathcal{C})$, which the spectral category $\mathrm{Spec}(\mathcal{C})$ comes equipped with, nicely plays the roles of both $1_{\mathcal{C}}$ and $E$, since each object in $\mathrm{Spec}(\mathcal{C})$ is injective, as shown in [11].

In this paper, however, we are not interested in injective objects, and our main aim is to construct $\mathrm{Spec}(\mathcal{C})$ in full generality, when $\mathcal{C}$ is supposed to be an arbitrary category with finite limits. Apart from the Grothendieck category case above, this was already done in the case of an arbitrary abelian category [13, p. 15], and for some nonadditive categories [3].

In fact we begin by taking not just an arbitrary category $\mathcal{C}$ with finite limits, but also any class $\mathcal{S}$ of its monomorphisms that contains all isomorphisms and is pullback stable and closed under composition. We define the spectral category $\mathrm{Spec}(\mathcal{C}, \mathcal{S})$ of the pair $(\mathcal{C}, \mathcal{S})$ to be the category

$$\mathcal{C}[(\mathrm{St}(\mathrm{Mono}_E(\mathcal{C}, \mathcal{S})))^{-1}]$$

of fractions of $\mathcal{C}$ for the class $\mathrm{St}(\mathrm{Mono}_E(\mathcal{C}, \mathcal{S}))$ of pullback stable $\mathcal{S}$-essential monomorphisms of $\mathcal{C}$. When $\mathcal{S}$ is the class of all monomorphisms in $\mathcal{C}$, we write $\mathrm{Spec}(\mathcal{C}, \mathcal{S}) = \mathrm{Spec}(\mathcal{C})$ and call this category the spectral category of $\mathcal{C}$.

We make various observations concerning the spans and fractions involved. The most important one is that the class $\mathrm{St}(\mathrm{Mono}_E(\mathcal{C}, \mathcal{S}))$ admits the calculus of right fractions, just as the class of essential monomorphism in an abelian category does.

We point out that the spectral category $\mathrm{Spec}(\mathcal{C})$ has finite limits and that the canonical functor $P : \mathcal{C} \to \mathrm{Spec}(\mathcal{C})$ preserves finite limits. When $\mathcal{C}$ is a normal category [18], assuming for simplicity that $\mathcal{S}$ is the class of all monomorphisms in $\mathcal{C}$, we show that pullback stable $\mathcal{S}$-essential monomorphisms are the same as what we call subobject-essential monomorphisms. These are those monomorphisms $m : M \to A$ in $\mathcal{C}$ such that, for any monomorphism $n : N \to A$, one has that $N = 0$ whenever $M \times_A N = 0$. Finally, when $\mathcal{C}$ is normal, the monoid $\mathrm{End}_{\mathrm{Spec}(\mathcal{C})}(P(A))$ of endomorphisms of an object $P(A)$ in the spectral category is a division monoid whenever $A$ is a *uniform* object (a notion extending the classical one of uniform module in the additive context).

The theory we develop is indeed an extension of what was done in [11] for the case of Grothendieck categories and in [3] for the category of $G$-groups. Note that there are several papers involving essential monomorphisms in non-abelian contexts (see e.g. [4, 21] and the references therein), although it is not their purpose to introduce spectral categories.

*Throughout this paper, $\mathcal{C}$ denotes a category with finite limits.*

## 2 Stabilization of Classes of Morphisms

Let $\mathcal{M}$ be a class of morphisms in $\mathcal{C}$. Following [7], define the stabilization $\mathrm{St}(\mathcal{M})$ of $\mathcal{M}$ as the class of morphisms $m\colon M \to A$ such that, for every pullback diagram of the form

$$\begin{array}{ccc} U & \xrightarrow{u} & X \\ \downarrow & & \downarrow \\ M & \xrightarrow[m]{} & A, \end{array}$$

$u$ is in $\mathcal{M}$. Let us recall that the symbol "St" was used in [15], while in [7] the stabilization of $\mathcal{M}$ was simply denoted by $\mathcal{M}'$. Similar constructions were also used before, of course.

**Proposition 1.** *The stabilization* $\mathrm{St}(\mathcal{M})$ *of* $\mathcal{M}$ *has the following properties:*

*(a)* *The class* $\mathrm{St}(\mathcal{M})$ *is pullback stable.*
*(b)* *If* $\mathcal{M}$ *contains all isomorphisms, then so does* $\mathrm{St}(\mathcal{M})$.
*(c)* *If* $\mathcal{M}$ *is closed under composition, then so is* $\mathrm{St}(\mathcal{M})$.
*(d)* *If* $\mathcal{M}$ *has the right cancellation property of the form*

$$(mm' \in \mathcal{M} \ \&\ m' \in \mathcal{S}) \Rightarrow m \in \mathcal{M}$$

*for some pullback stable class* $\mathcal{S}$ *of morphisms in* $\mathcal{C}$*, then* $\mathrm{St}(\mathcal{M})$ *has the same property with respect to the same class* $\mathcal{S}$.
*(e)* *If* $\mathcal{M}$ *has the weak right cancellation property*

$$(mm' \in \mathcal{M} \ \&\ m' \in \mathcal{M}) \Rightarrow m \in \mathcal{M},$$

*then* $\mathrm{St}(\mathcal{M})$ *has the same property.*
*(f)* $\mathrm{St}(\mathcal{M})$ *has the left cancellation property of the form*

$$(mm' \in \mathrm{St}(\mathcal{M}) \ \&\ m \in \mathrm{Mono}(\mathcal{C})) \Rightarrow m' \in \mathrm{St}(\mathcal{M}),$$

*where* $\mathrm{Mono}(\mathcal{C})$ *denotes the class of all monomorphisms in* $\mathcal{C}$.

*Proof.* (a) and (b) are obvious.

To prove (c), (d), and (e), use a diagram of the form

$$\begin{array}{ccccc}
U' & \longrightarrow & U & \longrightarrow & X \\
\downarrow & & \downarrow & & \downarrow \\
M' & \xrightarrow[m']{} & M & \xrightarrow[m]{} & A,
\end{array}$$

where the squares are pullbacks and the unlabeled arrows are the suitable pullback projections.

To prove (f), consider the diagram

$$\begin{array}{ccccc}
M' \times_M L & \longrightarrow & L & \xrightarrow{1_L} & L \\
\downarrow & & \downarrow{\scriptstyle l} & & \downarrow{\scriptstyle l} \\
M' & \xrightarrow{m'} & M & \xrightarrow{1_M} & M \\
{\scriptstyle 1_{M'}}\downarrow & & {\scriptstyle 1_M}\downarrow & & \downarrow{\scriptstyle m} \\
M' & \xrightarrow[m']{} & M & \xrightarrow[m]{} & A,
\end{array}$$

where $l \colon L \to M$ is an arbitrary morphism and the unlabeled arrows are the pullback projections. Note that all its squares are pullbacks, except for the right-hand bottom square, although it is also a pullback if $m$ is a monomorphism. Therefore, if $mm'$ is in $\mathrm{St}(\mathcal{M})$ and $m$ is a monomorphism, the pullback projection $M' \times_M L \to L$ is in $\mathcal{M}$. This proves the desired implication. □

*Remark 1.* Properties 1(a)–(c) are mentioned in [7] and 1(d) is 'almost' there, with $\mathcal{E}$ instead of $\mathcal{M}$. Property 1(e) also holds in the main example there, but for the trivial reason that $(mm' \in \mathrm{St}(\mathcal{E})\ \&\ m \in \mathrm{Mono}(\mathcal{C}))$ implies that $m$ is an isomorphism.

## 3 Essential and Pullback Stable Essential Monomorphisms

*Throughout this paper, we will consider a class $\mathcal{S}$ of monomorphisms in $\mathcal{C}$ that is pullback stable, contains all isomorphisms, is closed under composition, and has the strong left cancellation property*

$$mm' \in \mathcal{S} \Rightarrow m' \in \mathcal{S}.$$

According to a well-known definition, a morphism $m\colon M \to A$ from $\mathcal{S}$ is said to be an $\mathcal{S}$-*essential monomorphism*, if a morphism $f\colon A \to B$ from $\mathcal{C}$ is in $\mathcal{S}$ whenever so is $fm$. When $\mathcal{S}$ is the class of all monomorphisms in $\mathcal{C}$, we will say "essential" instead of "$\mathcal{S}$-essential". The class of all $\mathcal{S}$-essential monomorphisms will be denoted by $\mathrm{Mono}_E(\mathcal{C}, \mathcal{S})$. This class has many "good" properties well-known in the case of an abelian $\mathcal{C}$ with $\mathcal{S}$ being the class of all monomorphisms in $\mathcal{C}$ (see, e.g., any of the following: Section 5 in Chapter II of [10], Section 2 in Chapter III of [19], or Section 15.2 of [20]), and also known in the general case, as briefly mentioned in Remark 9.23 of [1]. The known properties we will need are collected in:

**Proposition 2.** *The class* $\mathrm{Mono}_E(\mathcal{C}, \mathcal{S})$ *of $\mathcal{S}$-essential monomorphisms*

*(a) contains all isomorphisms;*
*(b) is closed under composition;*
*(c) has the right cancellation property of the form*

$$(mm' \in \mathrm{Mono}_E(\mathcal{C}, \mathcal{S})\ \&\ m \in \mathcal{S}) \Rightarrow m \in \mathrm{Mono}_E(\mathcal{C}, \mathcal{S});$$

*(d) has the weak right cancellation property*

$$(mm' \in \mathrm{Mono}_E(\mathcal{C}, \mathcal{S})\ \&\ m' \in \mathrm{Mono}_E(\mathcal{C}, \mathcal{S})) \Rightarrow m \in \mathrm{Mono}_E(\mathcal{C}, \mathcal{S}),$$

*and, in particular, every split monomorphism that belongs to* $\mathrm{Mono}_E(\mathcal{C}, \mathcal{S})$ *is an isomorphism.* □

*Remark 2.* Note the difference between our Proposition 2(c) and Proposition 9.14(3) of [1]: we have omitted the redundant assumption $m' \in \mathcal{S}$.

From Propositions 1 and 2, we immediately obtain:

**Theorem 1.** *The class* $\mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}))$ *of pullback stable* $\mathcal{S}$*-essential monomorphisms in* $\mathcal{C}$

*(a) is pullback stable;*
*(b) contains all isomorphisms;*
*(c) is closed under composition;*
*(d) has the right cancellation property of the form*

$$(mm' \in \mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}))\ \&\ m \in \mathcal{S}) \Rightarrow m \in \mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}));$$

*(e) has the weak right cancellation property*

$$(mm' \in \mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}))\ \&\ m' \in \mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}))) \Rightarrow m \in \mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S})),$$

*and, in particular, every split monomorphism that belongs to* $\mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}))$ *is an isomorphism;*
*(f) has the left cancellation property of the form*

$$(mm' \in \mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}))\ \&\ m \in \mathrm{Mono}(\mathcal{C})) \Rightarrow m' \in \mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S})).$$

□

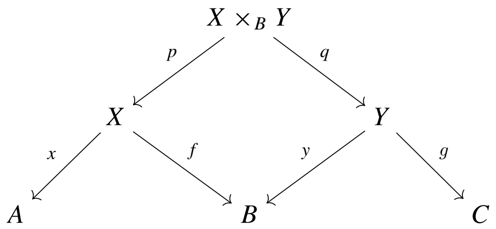
## 4 Spans and Fractions

Let $\mathcal{C}$ be a category with pullbacks. The bicategory $\mathrm{Span}(\mathcal{C})$ of spans in $\mathcal{C}$, originally introduced in [5] (motivated by the study of spans of additive categories in [22]) is constructed as follows, omitting obvious coherent isomorphisms:

- The objects (=0-cells) of $\mathrm{Span}(\mathcal{C})$ are the same as the objects of $\mathcal{C}$.
- A morphism (1-cell) $A \to B$ in $\mathrm{Span}(\mathcal{C})$ is a diagram in $\mathcal{C}$ of the form

$$A \xleftarrow{\ x\ } X \xrightarrow{\ f\ } B,$$

  usually written either as the triple $(f, X, x)$ or as the pair $(f, x)$.
- The composite $(g, Y, y)(f, X, x) = (gq, X \times_B Y, xp)$ of $(f, X, x)\colon A \to B$ and $(g, Y, y)\colon B \to C$ is defined via the diagram




in which $p\colon X \times_B Y \to X$ and $q\colon X \times_B Y \to Y$ are the pullback projections.

– A 2-cell from $(f, X, x)\colon A \to B$ to $(f', X', x')\colon A \to B$ is a morphism $s\colon X \to X'$ with $x's = x$ and $f's = f$, and the 2-cells compose as in $\mathcal{C}$.

More generally, given a pullback stable class $\mathcal{M}$ of morphisms in $\mathcal{C}$ that contains all identity morphisms and is closed under composition—we can then form the bicategory $\mathrm{Span}_{\mathcal{M}}(\mathcal{C})$ as above but requiring its morphisms $(f, x)$ to have $x$ in $\mathcal{M}$. As it was observed in a discussion with Janelidze and Mac Lane [14] (and most probably known before, which is why the content of that discussion was never published), the assignment $(cls(f, x)\colon A \to B) \mapsto (fx^{-1}\colon A \to B)$ (here $cls$ is the abbreviation for "class") determines an isomorphism

$$\Pi(\mathrm{Span}_{\mathcal{M}}(\mathcal{C})) \approx \mathcal{C}[\mathcal{M}^{-1}],$$

in which:

– $\Pi(\mathrm{Span}_{\mathcal{M}}(\mathcal{C}))$ is the Poincaré category of $\mathrm{Span}_{\mathcal{M}}(\mathcal{C})$ (in the sense of [5]), that is, it has the same objects as $\mathrm{Span}_{\mathcal{M}}(\mathcal{C})$, and its hom sets are the sets of connected components of hom categories of $\mathrm{Span}_{\mathcal{M}}(\mathcal{C})$.
– $\mathcal{C}[\mathcal{M}^{-1}]$ is the category of fractions [12] of $\mathcal{C}$ for $\mathcal{M}$.

We are assuming that the reader is familiar with the content of [5]. Repeating here the necessary details from that influential paper would take too much space.

Under the isomorphism above, the functor $\mathcal{C} \to \Pi(\mathrm{Span}_{\mathcal{M}}(\mathcal{C}))$, corresponding to the canonical functor

$$P_{\mathcal{M}}\colon \mathcal{C} \to \mathcal{C}[\mathcal{M}^{-1}],$$

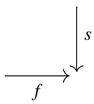
is defined by $(f\colon A \to B) \mapsto (cls(f, 1_A)\colon A \to B)$.

Recall that a class $\mathcal{M}$ is *focal* [6] if it satisfies the following four conditions:

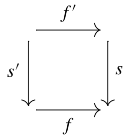
($F_0$) For each object $X \in \mathcal{C}$ there exists an $s \in \mathcal{M}$ with codomain $X$.

($F_1$) For all $\xrightarrow{s_1}\ \xrightarrow{s_0}$ with $s_i \in \mathcal{M}$, there exists a morphism $f$ in $\mathcal{C}$ such that the composite $s_0 s_1 f$ is defined and is in $\mathcal{M}$.

($F_2$) Each diagram



with $s \in \mathcal{M}$ can be completed in a commutative square




where $s' \in \mathcal{M}$.

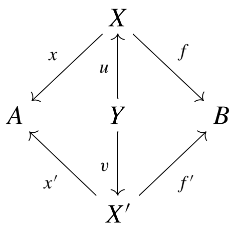
$(F_3)$ If a pair $(f, g)$ of parallel morphisms is coequalized by some $s \in \mathcal{M}$, it is also equalized by some $s' \in \mathcal{M}$.

**Proposition 3.** *If $\mathcal{M}$ is a pullback stable class of morphisms in $\mathcal{C}$ that contains all identity morphisms and is closed under composition, with $\mathcal{M} \subseteq \mathrm{Mono}(\mathcal{C})$, then $\mathcal{M}$ is focal and, moreover, $\mathcal{M}$ admits the calculus of right fractions in the sense of [12].*

*Proof.* All we need to check is that $\mathcal{M}$ satisfies the condition dual to condition 2.2(d) in Chapter I of [12], i.e., that whenever two parallel morphisms $f$ and $g$ admit a morphism $m \in \mathcal{M}$ with $mf = mg$, they also admit a morphism $n \in \mathcal{M}$ with $fn = gn$. This condition holds trivially because $\mathcal{M} \subseteq \mathrm{Mono}(\mathcal{C})$. □

*Remark 3.* Note the following levels of generality (in fact there are many more of them, including those suggested by distinguishing sets of morphisms from proper classes of morphisms), where we omitted all required conditions on $\mathcal{M}$ in the first five items:

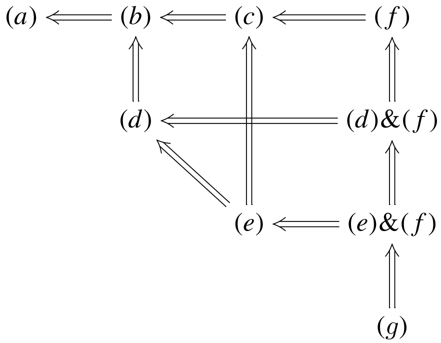
(a) For an arbitrary class $\mathcal{M}$ of morphisms of $\mathcal{C}$, we can still form the category $\mathcal{C}[\mathcal{M}^{-1}]$ of fractions of $\mathcal{C}$ for $\mathcal{M}$.
(b) As shown in [6], the morphisms of $\mathcal{C}[\mathcal{M}^{-1}]$ can be presented in the form $P_{\mathcal{M}}(f)P_{\mathcal{M}}(x)^{-1}$ with $x \in \mathcal{M}$ if and only if $\mathcal{M}$ satisfies conditions $(F_0)$, $(F_1)$, and $(F_2)$.
(c) In particular, this is the case when $\mathcal{M}$ satisfies the conditions dual to conditions 2.2(a), 2.2(b), and 2.2(c) in Chapter I of [12].
(d) If the equivalent conditions in (b) hold, then the following conditions are equivalent: ($d_1$) $\mathcal{M}$ is focal; ($d_2$) $\mathcal{M}$ satisfies condition $(F_3)$, which is the same as condition 2.2(d) in Chapter I of [12]; ($d_3$) not only can the morphisms of $\mathcal{C}[\mathcal{M}^{-1}]$ be presented as in (b), but also $P_{\mathcal{M}}(f)P_{\mathcal{M}}(x)^{-1} = P_{\mathcal{M}}(f')P_{\mathcal{M}}(x')^{-1}$ if and only there exists a commutative diagram in $\mathcal{C}$ of the form




with $xu \in \mathcal{M}$.

(e) In particular, the equivalent conditions ($d_1$)–($d_3$) hold when the class $\mathcal{M}$ admits the calculus of right fractions in the sense of [12].
(f) If $\mathcal{M}$ contains all identity morphisms, is closed under composition, and is pullback stable, then not only are we in the situation (c), but we also have the isomorphism between $\mathcal{C}[\mathcal{M}^{-1}]$ and $\Pi(\mathrm{Span}_{\mathcal{M}}(\mathcal{C}))$ mentioned above.
(g) The situation of Proposition 3. Note, in particular, that in this case the morphisms $u$ and $v$ in the diamond diagram of (d) belong to $\mathcal{M}$. This follows from Proposition 1(f) and the fact that $\mathrm{St}(\mathcal{M}) = \mathcal{M}$ here.

The levels of generality listed above are related as follows:




*Remark 4.* We recall from [12] that already in the situation (d), the equivalent conditions mentioned there imply that the hom sets of $\mathcal{C}[\mathcal{M}^{-1}]$ can be constructed as filtered colimits

$$\hom_{\mathcal{C}[\mathcal{M}^{-1}]}(A, B) = \mathrm{colim}(\hom(M, B)),$$

where the colimit is taken over all $m \colon M \to A$ in $\mathcal{M}$ (see Page 13 in [12], where the dual construction is described explicitly).

## 5 The Spectral Category

Let $\mathcal{S}$ be a class of monomorphisms in $\mathcal{C}$ satisfying the conditions required at the beginning of Section 3. Then, as follows from (a)–(c) and (f) of Theorem 1, the class $\mathcal{M} = \mathrm{St}(\mathrm{Mono}_E(\mathcal{C}, \mathcal{S}))$ satisfies the conditions required in Proposition 3. We are ready to give the following:

**Definition 1.** *The* spectral category $\mathrm{Spec}(\mathcal{C}, \mathcal{S})$ *of* $(\mathcal{C}, \mathcal{S})$ *is the category*

$$\mathcal{C}[(\mathrm{St}(\mathrm{Mono}_E(\mathcal{C}, \mathcal{S})))^{-1}]$$

*of fractions of* $\mathcal{C}$ *for the class* $\mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}))$ *of pullback stable* $\mathcal{S}$*-essential monomorphisms of* $\mathcal{C}$*. When* $\mathcal{S}$ *is the class of all monomorphisms in* $\mathcal{C}$*, we shall simply write* $\mathrm{Mono}_E(\mathcal{C},\mathcal{S}) = \mathrm{Mono}_E(\mathcal{C})$ *and* $\mathrm{Spec}(\mathcal{C},\mathcal{S}) = \mathrm{Spec}(\mathcal{C})$*, and say that* $\mathrm{Spec}(\mathcal{C})$ *is the spectral category of* $\mathcal{C}$*.*

Thanks to the results of [12], specifically Proposition 3.1 and Corollary 3.2 of Chapter I there, our Proposition 3 implies:

**Theorem 2.** *The spectral category* $\mathrm{Spec}(\mathcal{C},\mathcal{S})$ *has finite limits. Moreover, the canonical functor*

$$P_{\mathcal{C},\mathcal{S}} = P_{\mathrm{St}(\mathrm{Mono}_E(\mathcal{C},\mathcal{S}))} : \mathcal{C} \to \mathrm{Spec}(\mathcal{C},\mathcal{S}),$$

*defined by* $(f : A \to B) \mapsto (cls(f, 1_A) : A \to B)$*, preserves finite limits.* □

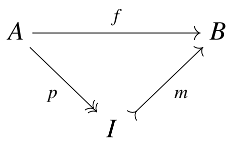
## 6 Subobject-Essential Monomorphisms

Assuming $\mathcal{C}$ to be pointed, we define:

**Definition 2.** *A monomorphism* $m : M \to A$ *in* $\mathcal{C}$ *is said to be* subobject-essential *if, for a monomorphism* $n : N \to A$*, one has* $M \times_A N = 0 \Rightarrow N = 0$*. The class of all subobject-essential monomorphisms in* $\mathcal{C}$ *will be denoted by* $\mathrm{Mono}_{SE}(\mathcal{C})$*.*

Recall that a regular epimorphism in a category $\mathcal{C}$ is a morphism that is the coequalizer of two morphisms in $\mathcal{C}$.

A finitely complete category $\mathcal{C}$ is *regular* if any morphism $f\colon A \to B$ can be factorized as the composite morphism of a regular epimorphism $p\colon A \to I$ and a monomorphism $m\colon I \to B$




and these factorizations are pullback stable. Following [18], we will call $\mathcal{C}$ *normal* if it is pointed, regular, and any regular epimorphism is a normal epimorphism (i.e., a cokernel of some arrow in $\mathcal{C}$). In such a category, any regular epimorphism is then the cokernel of its kernel and, as a consequence, a morphism in $\mathcal{C}$ is a monomorphism if and only if its kernel is zero.

*Remark 5.* For a pointed variety $\mathcal{V}$ of universal algebras, being a normal category is the same as being a 0-regular variety in the sense of [9] (see [17] for further explanations and historical remarks about the relationship between the properties of 0-regularity and normality). The algebraic theory of a pointed 0-regular variety $\mathcal{V}$ is characterized by the existence of a unique constant 0 and binary terms $d_1, ..., d_n$ such that the identities $d_i(x, x) = 0$ (for $i \in \{1, \dots, n\}$) and the implication $(d_1(x, y) = 0\ \&\ \dots\ \&\ d_n(x, y) = 0) \Rightarrow x = y$ hold. Intuitively, these operations $d_i(x, y)$ can then be thought of as a kind of "generalized subtraction". This implies that the varieties of groups, loops, rings, associative algebras, Lie algebras, crossed modules, and $G$-groups (for a group $G$) are all normal. There are also plenty of examples of normal categories that are not varieties, such as the categories of topological groups, cocommutative $K$-Hopf algebras over a field $K$, and $C^*$-algebras, for instance. In general, any semi-abelian category [16] is, in particular, a normal category.

For an object $A$ in $\mathcal{C}$, the smallest and the largest congruence (=effective equivalence relation) on $A$ will be denoted by $\Delta_A$ and $\nabla_A$, respectively. Note that equalities like $E = \Delta_A$ should usually be understood as equalities of subobjects (of $A \times A$ in this case).

When $\mathcal{C}$ is normal, it is natural to ask how different subobject-essential monomorphisms are from essential ones (recall that "essential" means $\mathcal{S}$-essential for $\mathcal{S} = \mathrm{Mono}(\mathcal{C})$). Most of this section is devoted to studying various ways to compare them.

Let us begin with the following proposition, well-known in the case of an abelian category $\mathcal{C}$:

**Proposition 4.** *If $\mathcal{C}$ is normal, then the following conditions on a monomorphism $m : M \to A$ in $\mathcal{C}$ are equivalent:*

*(a) $m$ is an essential monomorphism, that is, a morphism $f : A \to B$ is a monomorphism whenever so is $fm$.*
*(b) For any congruence $E$ on $A$, one has $(M \times M) \times_{A \times A} E = \Delta_M \Rightarrow E = \Delta_A$.*
*(c) For any normal monomorphism $n : N \to A$, one has $M \times_A N = 0 \Rightarrow N = 0$.*
*(d) For any morphism $f : A \to B$, one has $\mathsf{Ker}(fm) = 0 \Rightarrow \mathsf{Ker}(f) = 0$.*

*Proof.* (a) $\Rightarrow$ (b). Let $(E, e_1, e_2)$ be a congruence on $A$, and $f : A \to C$ a morphism such that $E$ is the kernel pair of $f$:

$$\begin{array}{ccc} E & \xrightarrow{e_2} & A \\ {\scriptstyle e_1}\downarrow & & \downarrow{\scriptstyle f} \\ A & \xrightarrow[f]{} & C. \end{array} \tag{1}$$

Consider the commutative diagram

$$\begin{array}{ccccc} M & \longrightarrow & E & \longrightarrow & C \\ {\scriptstyle (1_M, 1_M)}\downarrow & & {\scriptstyle (e_1, e_2)}\downarrow & & \downarrow{\scriptstyle (1_C, 1_C)} \\ M \times M & \xrightarrow[m \times m]{} & A \times A & \xrightarrow[f \times f]{} & C \times C \end{array}$$

where the right-hand square is a pullback by definition of kernel pair, and the left-hand square is a pullback by the assumption $(M \times M) \times_{A \times A} E = \Delta_M$. The fact that the rectangle is a pullback means that $fm$ is a monomorphism. Since $m$ is an essential monomorphism, it follows that $f$ is a monomorphism and $E = \Delta_A$.

(b) $\Rightarrow$ (c) This follows from the fact that a congruence $(E, e_1, e_2)$ as in (1) is the discrete equivalence relation $\Delta_A$ if and only if the normal monomorphism $\ker(f)\colon N \to A$ corresponding to $E$ is $0 \to A$.

(c) $\Rightarrow$ (d) It suffices to apply the assumption to the pullback

$$\begin{array}{ccc} 0 = \mathsf{Ker}(fm) & \longrightarrow & \mathsf{Ker}(f) \\ \downarrow & & \downarrow \\ M & \xrightarrow[m]{} & A. \end{array}$$

(d) $\Rightarrow$ (a) This is immediate since, in a normal category, monomorphisms are characterized by the fact that their kernel is 0. □

From Proposition 4, we immediately obtain:

**Corollary 1.** *Let $\mathcal{C}$ be a normal category. Then:*

*(a) Every subobject-essential monomorphism is essential.*
*(b) If $A$ is an object in $\mathcal{C}$ for which every monomorphism with codomain $A$ is normal, then a monomorphism $m : M \to A$ is subobject-essential if and only if it is essential.*
*(c) In particular, if $\mathcal{C}$ is abelian, then a monomorphism in $\mathcal{C}$ is subobject-essential if and only if it is essential.*

Next, we have:

**Proposition 5.** *The class $\mathrm{Mono}_{SE}(\mathcal{C})$ of subobject-essential monomorphisms in $\mathcal{C}$*

*(a) contains all isomorphisms;*
*(b) is closed under composition;*
*(c) has the right cancellation property of the form*

$$(mm' \in \mathrm{Mono}_{SE}(\mathcal{C}) \ \&\ m \in \mathrm{Mono}(\mathcal{C})) \Rightarrow m \in \mathrm{Mono}_{SE}(\mathcal{C}).$$

*(d) If $\mathcal{C}$ is normal, then the class $\mathrm{Mono}_{SE}(\mathcal{C})$ has the weak right cancellation property*

$$(mm' \in \mathrm{Mono}_{SE}(\mathcal{C}) \ \&\ m' \in \mathrm{Mono}_{SE}(\mathcal{C})) \Rightarrow m \in \mathrm{Mono}_{SE}(\mathcal{C})$$

*and, in particular, every split monomorphism that belongs to it is an isomorphism.*
*(e) It has the left cancellation property of the form*

$$(mm' \in \mathrm{Mono}_{SE}(\mathcal{C}) \ \&\ m \in \mathrm{Mono}(\mathcal{C})) \Rightarrow m' \in \mathrm{Mono}_{SE}(\mathcal{C}).$$

*(f) If $\mathcal{C}$ is normal, then the class $\mathrm{Mono}_{SE}(\mathcal{C})$ is pullback stable.*

*Proof.* (a) is obvious.

(b) and (c): Given monomorphisms $m\colon M \to A$, $m'\colon M' \to M$ and $n\colon N \to A$, consider the diagram

$$\begin{array}{ccccc}
M' \times_A N & \xrightarrow{m' \times 1} & M \times_A N & \longrightarrow & N \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle n} \\
M' & \xrightarrow[m']{} & M & \xrightarrow[m]{} & A,
\end{array}$$

where the unlabeled arrows are the suitable pullback projections. Since both squares in this diagram are pullbacks, we can argue as follows:

- If $m, m' \in \mathcal{M}$, then $M' \times_A N = 0 \Rightarrow M \times_A N = 0 \Rightarrow N = 0$.
- If $mm' \in \mathcal{M}$, then $M \times_A N = 0 \Rightarrow M' \times_A N = 0 \Rightarrow N = 0$, where the first implication holds because $\mathsf{Ker}(m') = 0$.

(d): Suppose $mm'$ and $m$ are in $\mathrm{Mono}_{SE}(\mathcal{C})$. Thanks to (c), we only need to prove that $m$ is a monomorphism. Therefore, since $\mathcal{C}$ is normal, it suffices to prove that $m$ has zero kernel. For, consider the diagram

$$\begin{array}{ccccc}
0 & \longrightarrow & \mathsf{Ker}(m) & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle \ker(m)} & & \downarrow \\
M' & \xrightarrow[m']{} & M & \xrightarrow[m]{} & A
\end{array}$$

and observe that:

- Its left-hand square is a pullback because so is its right-hand square, and $mm'$ is a monomorphism because it is in $\mathrm{Mono}_{SE}(\mathcal{C})$.
- Since $m'$ is in $\mathrm{Mono}_{SE}(\mathcal{C})$, we have that $\mathsf{Ker}(m) = 0$.

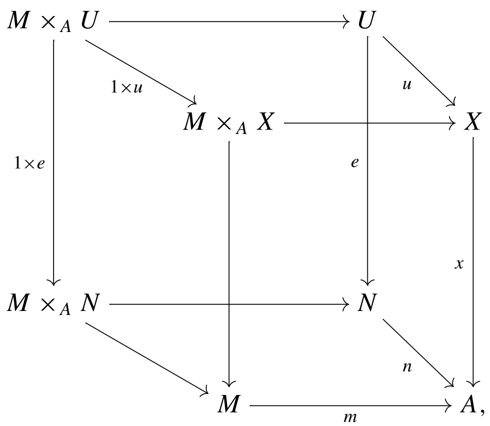
(e): Suppose $mm'$ is in $\mathrm{Mono}_{SE}(\mathcal{C})$ and $m$ is a monomorphism. First notice that, since $mm'$ is a monomorphism, so is $m'$. After that, consider the diagram

$$\begin{array}{ccccc}
M' \times_M L & \longrightarrow & L & \xrightarrow{1_L} & L \\
\downarrow & & {\scriptstyle l}\downarrow & & \downarrow{\scriptstyle ml} \\
M' & \xrightarrow[m']{} & M & \xrightarrow[m]{} & A,
\end{array}$$

where the unlabeled arrows are the suitable pullback projections. Since both squares in this diagram are pullbacks, we have

$$M' \times_M L = 0 \Rightarrow M' \times_A L = 0 \Rightarrow L = 0.$$

(f): Given $m\colon M \to A$ from $\mathrm{Mono}_{SE}(\mathcal{C})$, a morphism $x\colon X \to A$, and a monomorphism $u\colon U \to X$, consider the diagram




in which $M \times_A U = (M \times_A X) \times_X U$, $xu = ne$ is a (regular epi, mono) factorization of $xu$, and the unlabeled arrows are the suitable pullback projections. Assuming $M \times_A U = 0$, we have to prove that $U = 0$. Indeed:

- Since $e$ is a regular epimorphism, so is $1 \times e$.
- Since $1 \times e$ is an epimorphism and $M \times_A U = 0$, we have $M \times_A N = 0$.
- Since $M \times_A N = 0$ and $m$ is in $\mathrm{Mono}_{SE}(\mathcal{C})$, we have that $N = 0$.
- Since $N = 0$, we have $xe = ne = 0$, and so $u$ factors through the kernel of $x$.
- Since $u$ factors through the kernel of $x$, it also factors through the pullback projection $M \times_A X \to X$.
- Since $u$ factors through the pullback projection $M \times_A X \to X$, and the top part of our diagram is a pullback, the pullback projection $M \times_A U \to U$ is a split epimorphism.

It follows that $U = 0$, as desired. □

*Remark 6.* For a composable pair $(m, m')$ of monomorphisms, $m'$ can be seen as a pullback of $mm'$ along $m$ (this well-known fact was used in the proof of Proposition 1(f) for the pair $(m, l)$). This implies that every pullback stable class of monomorphisms has the strong left cancellation property and, in particular, that, in the case of normal $\mathcal{C}$, Proposition 5(e) could be deduced from Proposition 5(f).

*Remark 7.* In contrast to Theorem 1(f) and Proposition 5(e), the class $\mathrm{Mono}_E(\mathcal{C})$ does not even have, in general, the weak left cancellation property $m, mm' \in \mathrm{Mono}_E(\mathcal{C}) \Rightarrow m' \in \mathrm{Mono}_E(\mathcal{C})$. One can easily construct counterexamples in many non-abelian semi-abelian algebraic categories by suitably choosing $m' : M' \to M$ to be a split monomorphism (that is not an isomorphism) and choosing $m : M \to A$ with simple $A$. For example:

(a) Let $\mathcal{C}$ be the category of groups, $A$ any simple group that has an element $a$ of order $pq$ with relatively prime $p$ and $q$, $M$ the subgroup of $A$ generated by $a$, $M'$ the subgroup of $A$ generated by $a^p$, and $m : M \to A$ and $m' : M' \to M$ the inclusion maps. Then $m$ and $mm'$ are in $\mathcal{M}_E$, but $m'$ is not.
(b) Let $\mathcal{C}$ be the category of rings (commutative or not; we do not require them to have identity element, to make $\mathcal{C}$ semi-abelian), $M' = K$ be a field, $M = K[x]$ the polynomial ring in one variable $x$ over $K$, $A = K(x)$ the field of fractions of $M$, and $m : M \to A$ and $m' : M' \to M$ the canonical monomorphisms. Then, again, $m$ and $mm'$ are in $\mathcal{M}_E$, but $m'$ is not.

*Remark 8.* Although the non-pullback-stability of $\mathrm{Mono}_E(\mathcal{C})$ in the category of groups follows from Remark 7(a), let us give what seems to be the simplest counterexample. Consider the pullback

$$\begin{array}{ccc} 0 & \longrightarrow & S_2 \\ \downarrow & & \downarrow \\ A_3 & \longrightarrow & S_3 \end{array}$$

of monomorphisms, where $S_2$, $S_3$, $A_3$ are the symmetric/alternating groups. Its bottom arrow is an essential monomorphism, while the top one is not. This also shows that $A_3 \to S_3$ is an example of an essential monomorphism that is not subobject-essential.

**Theorem 3.** *If $\mathcal{C}$ is normal, then* $\mathrm{Mono}_{SE}(\mathcal{C}) = \mathrm{St}(\mathrm{Mono}_E(\mathcal{C}))$*, that is, a morphism in $\mathcal{C}$ is a subobject-essential monomorphism if and only if it is a pullback stable essential monomorphism.*

*Proof.* The inclusion $\mathrm{Mono}_{SE}(\mathcal{C}) \subseteq \mathrm{St}(\mathrm{Mono}_E(\mathcal{C}))$ follows from Corollary 1(a) and Proposition 5(f). Conversely, let $m : M \to A$ be a pullback stable essential monomorphism in $\mathcal{C}$ and $n : N \to A$ a monomorphism in $\mathcal{C}$ with $M \times_A N = 0$. Then $0 \to N$ is an essential monomorphism because it is a pullback of $m$. Hence, from the last assertion of Proposition 2(d), $0 \to N$ is an isomorphism, that is, $N = 0$. □

Since every abelian category is normal, we easily get:

**Corollary 2.** *If $\mathcal{C}$ is abelian then* $\mathrm{Spec}(\mathcal{C})$ *is the same as the spectral category of $\mathcal{C}$ in the usual sense (see [11] and [12]).*

*Proof.* Having in mind Corollary 1(c), this follows from Theorem 3 and the description of the spectral category of an abelian category given in 2.5(e) of [12, Chapter I]. □

## 7 Uniform Objects

Let us return to the general situation of Remark 4(a), where $\mathcal{M}$ is an arbitrary class of morphisms in $\mathcal{C}$, but let us assume that $\mathcal{C}$ is pointed and that

$$x \in \mathcal{M} \Rightarrow \mathsf{Ker}(x) = 0.$$

As already observed, in any *normal* category, this property simply says that $\mathcal{M}$ is a class of monomorphisms.

**Definition 3.** *An object $A$ of $\mathcal{C}$ is said to be $\mathcal{M}$-*uniform *if a morphism $x\colon X \to A$ belongs to $\mathcal{M}$ whenever $X \neq 0$ and $\mathsf{Ker}(x) = 0$.*

The term *uniform* comes from module theory, where a nonzero module $M$ is called a uniform module if every nonzero submodule $N$ of $M$ is an essential submodule. Note that this term was also used in [3] for an analogue notion in the category of $G$-groups.

**Proposition 6.** *Let $A$ and $B$ be $\mathcal{M}$-uniform objects in $\mathcal{C}$. Every nonzero morphism $A \to B$ in $\mathcal{C}[\mathcal{M}^{-1}]$ of the form $P_{\mathcal{M}}(f)P_{\mathcal{M}}(x)^{-1}$ with $x$ in $\mathcal{M}$ is an isomorphism.*

*Proof.* Consider the diagram

$$\begin{array}{ccccc} & & \mathsf{Ker}(f) & & \\ & & \Big\downarrow{\scriptstyle \ker(f)} & & \\ A & \xleftarrow{\;x\;} & X & \xrightarrow{\;f\;} & B, \end{array}$$

where $X$ is the domain of $x$ (the domain of $f$).

Suppose $\mathsf{Ker}(f) \neq 0$. Since $A$ is $\mathcal{M}$-uniform and $x$ and $\ker(f)$ have zero kernels, the composite $\mathsf{Ker}(f) \to X \to A$ belongs to $\mathcal{M}$. As $x$ also belongs to $\mathcal{M}$, this implies that $P_{\mathcal{M}}(\ker(f))$ is an isomorphism, and we can write

$$\begin{aligned} P_{\mathcal{M}}(f)P_{\mathcal{M}}(x)^{-1} &= P_{\mathcal{M}}(f)P_{\mathcal{M}}(\ker(f))P_{\mathcal{M}}(\ker(f))^{-1}P_{\mathcal{M}}(x)^{-1} \\ &= P_{\mathcal{M}}(f(\ker(f))P_{\mathcal{M}}(\ker(f))^{-1}P_{\mathcal{M}}(x)^{-1} \\ &= P_{\mathcal{M}}(0)P_{\mathcal{M}}(\ker(f))^{-1}P_{\mathcal{M}}(x)^{-1} \\ &= 0. \end{aligned}$$

That is, we can suppose $\mathsf{Ker}(f) = 0$. If so, then, since $B$ is $\mathcal{M}$-uniform, $f$ belongs to $\mathcal{M}$, which makes $P_{\mathcal{M}}(f)P_{\mathcal{M}}(x)^{-1}$ an isomorphism. □

In order to state the next result, let us recall that a *division monoid* is a nontrivial monoid $M$ with the property that the submonoid $U(M)$ of invertible elements is given by $U(M) = M \setminus \{0\}$. We write $\mathrm{End}_{\mathrm{Spec}(\mathcal{C})}(A)$ for the monoid of endomorphisms of an object $A$ in the spectral category $\mathrm{Spec}(\mathcal{C})$, where $\mathcal{C}$ is a normal category.

**Corollary 3.** *Let $\mathcal{C}$ be a normal category, and $A$ an $\mathcal{M}$-uniform object in $\mathcal{C}$ for $\mathcal{M}$ being the class of subobject-essential monomorphisms in $\mathcal{C}$. Then the monoid* $\mathrm{End}_{\mathrm{Spec}(\mathcal{C})}(A)$ *of endomorphisms of $A$ in* $\mathrm{Spec}(\mathcal{C})$ *is a division monoid.*

*Proof.* This immediately follows from Proposition 6, by taking into account the fact that the class of subobject-essential monomorphisms coincides with the class of pullback stable essential monomorphisms whenever $\mathcal{C}$ is a normal category (by Theorem 3). □

This last result extends Lemma 5.4 in [3], where the base category $\mathcal{C}$ was the category of $G$-groups, to the general context of a normal category $\mathcal{C}$.

**Acknowledgements** The second author was partially supported by Ministero dell' Istruzione, dell' Università e della Ricerca (Progetto di ricerca di rilevante interesse nazionale "Categories, Algebras: Ring-Theoretical and Homological Approaches (CARTHA)") and Dipartimento di Matematica "Tullio Levi-Civita" of Università di Padova (Research program DOR1828909 "Anelli e categorie di moduli"). The third author was supported by a "Visiting scientist scholarship—year 2019" by Università degli Studi di Padova. The fourth author was partially supported by South African NRF.

## References

1. Adámek, J., Herrlich, H., Strecker, G.E.: Abstract and concrete categories. The joy of cats, Pure and Applied Math., John Wiley & Sons, Inc., New York (1990)
2. Adámek, J., Herrlich, H., Rosický, J., Tholen, W.: Injective hulls are not natural. Algebra Universalis **48**, 374–388 (2002)
3. Arroyo Paniagua, M.J., Facchini, A.: Category of $G$-groups and its spectral category, Comm. Algebra **45**(4), 1696–1710 (2017)
4. Banaschewski, B.: Injectivity and essential extensions in equational classes of algebras. "Queen's papers in Pure and Applied Mathematics No. 25" (Proceedings of the Conference on Universal Algebra, Kingston 1969), pp. 131–147. Kingston, Ontario (1970)
5. Bénabou, J.: Introduction to bicategories. In: 1967 Reports of the Midwest Category Seminar. Springer, Berlin, pp. 1–77
6. Bénabou, J.: Some geometric aspects of the calculus of fractions, the European Colloquium of category theory (Tours, 1994). Appl. Categ. Struct. **4**(2), 139–165 (1996)
7. Carboni, A., Janelidze, G., Kelly, G.M., Paré, R.: On localization and stabilization of factorization systems. Appl. Categ. Struct. **5**, 1–58 (1997)
8. Facchini, A.: Injective modules, spectral categories, and applications. In: Jain, S.K., Parvathi, S. (eds.) Noncommutative Rings, Group Rings, Diagram Algebras and their Applications, Contemp. Math. 456, Amer. Math. Soc., Providence, RI, pp. 1–17 (2008)
9. Fichtner, K.: Eine Bermerkung über Mannigfaltigkeiten universeller Algebren mit Idealen. Monatsh. d. Deutsch. Akad. d. Wiss. (Berlin) **12**, 21–25 (1970)
10. Gabriel, P.: Des catégories abéliennes. Bull. Soc. Math. Fr. **90**, 323–448 (1962)
11. Gabriel, P., Oberst, U.: Spektralkategorien und reguläre Ringe im von-Neumannschen Sinn. Math. Z. **92**, 389–395 (1966)
12. Gabriel, P., Zisman, M.: Calculus of Fractions and Homotopy Theory. Springer, Berlin (1967)
13. Goodearl, K.R.: Ring Theory. Nonsingular Rings and Modules. Marcel Dekker Inc., New York and Basel (1976)
14. Janelidze, G., Mac Lane, S.: Private communication
15. Janelidze, G., Tholen, W.: Strongly separable morphisms in general categories. Theory Appl. Categ. **23**(7), 136–149 (2010)
16. Janelidze, G., Márki, L., Tholen, W.: Semi-abelian categories. J. Pure Appl. Algebra **168**, 367–386 (2002)
17. Janelidze, G., Márki, L., Ursini, A.: Ideals and clots in universal algebra and in semi-abelian categories. J. Algebra **307**, 191–208 (2007)

18. Janelidze, Z.: The pointed subobject functor, $3 \times 3$ lemmas, and subtractivity of spans. Theory Appl. Categ. **23**(11), 221–242 (2010)
19. Mitchell, B.: Theory of categories. Pure Appl. Math. **17** (1965). Academic Press
20. Schubert, H.: Categories. Springer, New York, Heidelberg (1972)
21. Tholen, W.: Injective objects and cogenerating sets. J. Algebra **73**, 139–155 (1981)
22. Yoneda, N.: On Ext and exact sequences. J. Fac. Sci. Univ. Tokyo Sect. **I**(8), 507–576 (1960)

# A Survey on the Local Invertibility of Ideals in Commutative Rings

**Carmelo Antonio Finocchiaro and Francesca Tartarone**

**Abstract** Let $D$ be an integral domain. We give an overview on connections between the $(t)$-finite character property of $D$ (i.e., each nonzero element of $D$ is contained in finitely many $(t)$-maximal ideals) and problems of local invertibility of ideals.

**Keywords** Finite character · Invertible ideal · Star operation

**2000 Mathematics Subject Classification** Primary: 13A15 · 13F05 · Secondary: 13B30 · 13G05

## 1 Introduction

A well-known characterization of invertible ideals in integral domains states that "a nonzero ideal is invertible if and only if it is finitely generated and locally principal" [8, II §5, Theorem 4].

The condition that the ideal is finitely generated can be dropped down, for instance, if the domain has the finite character on maximal ideals, i.e., each nonzero element is contained in finitely many maximal ideals (see, for instance, the argument provided in the proof of [3, Chapter 7, Exercise 9]. Here the fact that finite character allows to characterize Noetherian domains among locally Noetherian domains is put in light).

C. A. Finocchiaro
Dipartimento di Matematica, Università degli Studi di Padova, Via Trieste 63, 35121 Padova, Italy
e-mail: carmelo@math.unipd.it; cafinocchiaro@unict.it

Dipartimento di Matematica e Informatica, Università degli Studi di Catania, Viale Andrea Doria 6, 95125 Catania, Italy

F. Tartarone (✉)
Dipartimento di Matematica e Fisica, Università degli Studi Roma Tre, Largo San Leonardo Murialdo 1, 00146 Roma, Italy
e-mail: tfrance@mat.uniroma3.it



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*, Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_8

An interesting problem considered, for instance, by S. Glaz and W. Vasconcelos in [22, 23], asks for conditions on a domain $D$ in order to have that flat ideals of $D$ are invertible. This question can be specialized by asking when faithfully flat ideals are invertible.

We recall that for ideals in a domain, projective is equivalent to invertible and faithfully flat is equivalent to locally principal ([2]). Thus the condition "faithfully flat ideals are projective" is exactly "locally principal ideals are invertible".

In [22], the authors conjecture the equivalence between faithfully flat and projective ideals in H-domains (i.e., a domain in which $t$-maximal ideals are divisorial). This conjecture has been disproved by G. Picozza and F. T. in [32, Example 1.10], but the problem that S. Glaz and W. Vasconcelos posed has also been considered for other classes of domains like the Prüfer ones (i.e., domains whose localization at a prime ideal is a valuation domain).

Bazzoni [6] conjectured that:

*In a Prüfer domain $D$ "locally principal ideals are invertible" if and only if $D$ has the finite character on maximal ideals.*

Bazzoni's conjecture was proved at the same time by W.C. Holland, J. Martinez, W. Wm. McGovern, M. Tesemma in [27] by using methods (of independent interest) of the theory of lattice-ordered groups and by F. Halter-Koch using the theory of $r$-Prüfer monoids [25], where $r$ is an ideal system.

After the publication of these papers, a growing interest in this question (in more general contexts) came up.

It was considered a kind of $t$-version of Bazzoni's conjecture which replaces the finite character with the $t$-finite character and the local invertibility with the $t$-local invertibility. In this context, the original conjecture has been generalized to Prüfer $v$-multiplication domains and to even larger classes of integral domains (cfr. [18, 25, 35]). Section 3 of the paper is completely dedicated to a discussion of the $t$-local invertibility.

Finally, in Section 4, we present some recent results about the local invertibility and its connections with the finite character on maximal ideals in commutative (not necessarily integral) rings. As seen in Theorem 4.5, Bazzoni's conjecture can be extended to general rings with zero-divisors. In this context, the authors use the concept of Manis valuations and Prüfer extensions in place of Prüfer domains (see [28]).

## 2 The Prüfer Case

In this section, we will provide a deeper insight into the so-called Bazzoni's conjecture, which states that a Prüfer domain $D$ has finite character if and only if every locally principal of $D$ is invertible (i.e., finitely generated). This conjecture, stated in [4] and [6], was first solved by Holland, Martinez, Mc Govern and Tesemma in [27] and their result was then generalized to several other classes of rings (see, for instance, [18, 25, 35]). We are going to present the main steps of the first proof of Bazzoni's conjecture. It is based on an argument involving some basic tools on lattice-ordered abelian groups. Thus we will recall now some preliminaries for the reader's convenience.

As usual, for any ring $R$, $\mathrm{Spec}(R)$ denotes the set of all prime ideals of $R$ and, if $S$ is any subset of $R$, we set

$$V(S) := \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \supseteq S\}.$$

If $(X, \leq)$ is a partially ordered set and $x_1, \ldots, x_n \in X$, then $\sup(x_1, \ldots, x_n)$ (resp., $\inf(x_1, \ldots, x_n)$) will denote the supremum (resp., the infimum) of $\{x_1, \ldots, x_n\}$ in $X$, if it exists. Recall that a nonempty and proper subset $F$ of a partially ordered set $(X, \leq)$ is a *filter* (see [12, Definition 14.1]) if it satisfies the following properties:

- given $x, y \in F$, there exists $\inf(x, y)$ and $\sup(x, y) \in F$;
- if $f \in F, x \in X$ and $f \leq x$, then $x \in F$.

Let $\mathcal{F}(X)$ denote the set of all filters on $X$. If $(X, \leq)$ is a lattice, for any $a \in X$, the set $\{x \in X : x \geq a\}$ is clearly a filter and it is called *a principal filter*.

Now, let $(G, \cdot, \leq)$ be a lattice-ordered abelian group (for short, a $\ell$-group). Recall that an $\ell$-subgroup $H$ of $G$ is *convex* if, given elements $h, k \in H$, $g \in G$ such that $h \leq g \leq k$, then $g \in H$. Clearly, the intersection of any nonempty collection of convex $\ell$-subgroups of $G$ is still convex, and thus for any subset $S$ of $G$ there exists the smallest convex $\ell$-subgroup $\mathrm{Conv}(S)$ of $G$ containing $S$, and it is called *the convex envelop of* $S$. If $e$ is the identity element of $G$, let

$$G^+ := \{g \in G : g \geq e\}$$

be the positive cone of $G$. If $S \subseteq G^+$, then, by [12, Proposition 7.11(b)],

$$\mathrm{Conv}(S) = \{g \in G : |g| \leq s_1 \cdots s_n, \text{ for some } s_1, \ldots, s_n \in S, n \in \mathbb{N}^+\},$$

where $|g| := \sup(g, e) \cdot \sup(g^{-1}, e)$. A convex $\ell$-subgroup $P$ of $G$ is *prime* if, whenever $g, h \in G$ and $\inf(g, h) = e$, then either $g \in P$ or $h \in P$. A straightforward application of Zorn's Lemma shows that $G$ admits *minimal prime subgroups* (i.e., prime subgroups which are minimal under inclusion) and every prime subgroup of $G$ contains some minimal prime subgroup [12, Theorem 9.6]. Let $\mathcal{P}(G)$ (resp., $\mathcal{M}(G)$) denote the set of all prime (resp., minimal prime) subgroups of $G$. For every $g \in G$, let $U(g) := \{P \in \mathcal{M}(G) : g \notin P\}$.

The bridge which links Bazzoni's conjecture and the theory of $\ell$-groups is the ideal structure of a Prüfer domain. Let $D$ be an integral domain and let $\mathrm{Inv}(D)$ be the multiplicative group consisting of all invertible fractional ideals of $D$, endowed with partial order given by the opposite inclusion $\supseteq$. Since $D$ is the identity of $\mathrm{Inv}(D)$, the positive cone $\mathrm{Inv}(D)^+$ of $\mathrm{Inv}(D)$ is just the set of all integral invertible ideals.

**Theorem 2.1** ([9, Theorem 2]). *If $D$ is a Prüfer domain, then* $\mathrm{Inv}(D)$ *is an* $\ell$*-group.*

More precisely, given two fractional ideals $I, J \in \mathrm{Inv}(D)$, then they are finitely generated, in particular. Thus $I + J$ is finitely generated too and, since $D$ is Prüfer, $I + J \in \mathrm{Inv}(D)$, proving that $I + J = \inf(I, J)$. Moreover, $D$ is a coherent domain (meaning that the intersection of finitely many finitely generated fractional ideals is finitely generated too), being it Prüfer, by [21, Proposition (25.4)(1)], and thus $I \cap J \in \mathrm{Inv}(D)$, proving that $I \cap J = \sup(I, J)$. Let $\mathcal{I}^\bullet(D)$ denote the set of all nonzero (integral) ideals of $D$.

**Lemma 2.2** (see [27, Lemma 1]). *Let $D$ be a Prüfer domain. The following properties hold.*

*(1) The map $\varphi : \mathcal{I}^\bullet(D) \longrightarrow \mathcal{F}(\mathrm{Inv}(D)^+)$ defined by setting*

$$\varphi(\mathfrak{i}) := \{\mathfrak{a} \in \mathrm{Inv}(D)^+ : \mathfrak{a} \subseteq \mathfrak{i}\}$$

*is a bijection.*

*(2) For every $\mathfrak{i} \in \mathcal{I}^\bullet(D)$, $\varphi(\mathfrak{i})$ is a principal filter if and only if $\mathfrak{i}$ is invertible (i.e., finitely generated).*

*Proof.* (1). The fact that $\varphi$ is well defined and injective is trivial. Now, let $F$ be a filter on $\mathrm{Inv}(D)^+$ and set $\mathfrak{i} := \sum_{\mathfrak{a} \in F} \mathfrak{a}$. Thus, by definition, $F \subseteq \varphi(\mathfrak{i})$. Conversely, take an ideal $\mathfrak{b} \in \varphi(\mathfrak{i})$, i.e., $\mathfrak{b}$ is invertible and $\mathfrak{b} \subseteq \mathfrak{i}$. Since $\mathfrak{b}$ is, in particular, finitely generated, there exist ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \in F$ such that $\mathfrak{b} \subseteq \mathfrak{a}_1 + \ldots + \mathfrak{a}_n$, that is, $\mathfrak{b} \geq \inf(\mathfrak{a}_1, \ldots, \mathfrak{a}_n)$. Keeping in in mind that $F$ is a filter it follows $\inf(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \in F$ and finally $\mathfrak{b} \in F$.

(2) is clear, for the definitions. □

*Remark 2.3.* Let $D$ be a Prüfer domain and let $\mathrm{Spec}(D)^\bullet$ denote the set of all nonzero prime ideals of $D$. For any ideal $\mathfrak{p} \in \mathrm{Spec}(D)^\bullet$, set $X_\mathfrak{p} := \{\mathfrak{a} \in \mathrm{Inv}(D)^+ : \mathfrak{a} \not\subseteq \mathfrak{p}\}$ and $\overline{\mathfrak{p}} := \mathrm{Conv}(X_\mathfrak{p})$.

(1) $\overline{\mathfrak{p}}$ is a prime subgroup of $\mathrm{Inv}(D)$. Take invertible ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ of $D$ such that $\inf(\mathfrak{a}_1, \ldots, \mathfrak{a}_n) := \mathfrak{a}_1 + \ldots + \mathfrak{a}_n = D$. It follows $\mathfrak{a}_i \not\subseteq \mathfrak{p}$, for some $i$, i.e., $\mathfrak{a}_i \in X_\mathfrak{p} \subseteq \overline{\mathfrak{p}}$. Furthermore, by [12, Proposition 7.11(b)] and keeping in mind that $X_\mathfrak{p}$ is closed under multiplication, we infer

$$\overline{\mathfrak{p}} = \{I \in \mathrm{Inv}(D) : |I| \supseteq \mathfrak{a}, \text{ for some } \mathfrak{a} \in X_\mathfrak{p}\}.$$

(2) Since $|\mathfrak{a}| = \mathfrak{a}$, for any $\mathfrak{a} \in \mathrm{Inv}(D)^+$, it follows that $\overline{\mathfrak{p}} \cap \mathrm{Inv}(D)^+ = X_\mathfrak{p}$.

(3) Consider $G = \mathrm{Inv}(D)$ and the map $\psi : \mathrm{Spec}(D)^\bullet \longrightarrow \mathcal{P}(G)$ defined by setting, $\psi(\mathfrak{p}) := \overline{\mathfrak{p}}$, for every $\mathfrak{p} \in \mathrm{Spec}(D)^\bullet$. Keeping in mind part (2) of the present remark, it easily follows that, for every $\mathfrak{p}, \mathfrak{q} \in \mathrm{Spec}(D)^\bullet$, $\mathfrak{p} \subseteq \mathfrak{q}$ if and only if $\overline{\mathfrak{q}} \subseteq \overline{\mathfrak{p}}$. In particular, $\psi$ is injective and order reversing.

(4) $\psi$ restricts to a bijection of $\mathrm{Max}(D)$ onto $\mathcal{M}(\mathrm{Inv}(D))$. As a matter of fact, let $P$ be a minimal prime subgroup of $\mathrm{Inv}(D)$. If, for every maximal ideal $\mathfrak{m}$ of

$D$, $X_{\mathfrak{m}} \nsubseteq P$, there is an invertible integral ideal $\mathfrak{a}_{\mathfrak{m}}$ of $D$ such that $\mathfrak{a}_{\mathfrak{m}} \nsubseteq \mathfrak{m}$ and $\mathfrak{a}_{\mathfrak{m}} \notin P$. It follows $\sum_{\mathfrak{m}\in \mathrm{Max}(D)} \mathfrak{a}_{\mathfrak{m}} = D$ and thus (since every ring has the identity element) there are maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ of $D$ such that $\mathfrak{a}_{\mathfrak{m}_1} + \ldots + \mathfrak{a}_{\mathfrak{m}_r} = D$. Since $P$ is a prime subgroup, there exists $i \in \{1, \ldots, r\}$ such that $\mathfrak{a}_{\mathfrak{m}_i} \in P$, a contradiction. It follows that there is a maximal ideal $\mathfrak{m}$ of $D$ such that $X_{\mathfrak{m}} \subseteq P$ and, since $P$ is a minimal prime subgroup (and, in particular, it is convex), we deduce $\overline{\mathfrak{m}} := \mathrm{Conv}(X_{\mathfrak{m}}) = P$. Conversely, if $\mathfrak{m}$ any maximal ideal of $D$ and $P$ is a minimal prime subgroup of $\mathrm{Inv}(D)$ such that $\overline{\mathfrak{m}} \supseteq P$, take a maximal ideal $\mathfrak{n}$ of $D$ such that $P = \overline{\mathfrak{n}}$ (in view of what we have just proved). By part (3) it follows $\mathfrak{m} = \mathfrak{n}$ and thus $\overline{\mathfrak{m}}$ is minimal.

(5) By the previous parts, for every integral invertible ideal $\mathfrak{a}$ of $D$, we have

$$\psi(\mathrm{Max}(D) \cap V(\mathfrak{a})) = U(\mathfrak{a}).$$

The following result immediately follows from parts (4, 5) of the previous remark.

**Lemma 2.4** ([27, Theorem 2]). *A Prüfer domain $D$ has a finite character if and only if, for every integral invertible ideal $\mathfrak{a}$ of $D$, the set $U(\mathfrak{a})$ is finite.*

Thus the previous lemma provides the translation of the finite character of a Prüfer domain into a statement in the language of $\ell$-groups. The next goal is to provide the translation of the LPI property.

**Definition 2.5** ([27, Definition 3]). Let $G$ be an $\ell$-group and let $F$ be a filter on $G^+$. Then $F$ is said to be a *cold filter* provided that, for every $P \in \mathcal{M}(G)$, there exists some element $f \in F$ such that $f + P \leq g + P$, for all $g \in F$ (where $\leq$ is the canonical total order induced by the order of $G$ into the factor group $G/P$).

**Lemma 2.6** ([27, Proposition 5]). *Let $D$ be a Prüfer domain. Then a nonzero ideal $\mathfrak{i}$ of $D$ is locally principal if and only if the filter $\varphi(\mathfrak{i})$ (see Lemma 2.2) is a cold filter.*

Combining Lemmas 2.2 and 2.6, it is clear that for a Prüfer domain $D$ the following conditions are equivalent.

(1) Every nonzero locally principal ideal of $D$ is invertible.
(2) Every cold filter on $\mathrm{Inv}(D)^+$ is principal.

This provides the complete translation of Bazzoni's conjecture into a conjecture regarding $\ell$-groups. The key step to show it is to observe that, if $G$ is an $\ell$-group such that every cold filter on $G^+$ is principal, then every element of $G^+$ is greater than only finitely many mutually disjoint elements ([27, Proposition 7]). Now several relevant results of Conrad [11] are very helpful, together with the Finite Basis Theorem ([12, Theorem 46.12]). These tools lead to the main result.

**Theorem 2.7** ([27, Theorem 9]). *Let $G$ be an $\ell$-group such that every cold filter on $G^+$ is principal. Then, for every $g \in G^+$, the set $U(g)$ is finite.*

Thus finally, keeping in mind the previous theorem and Lemmas 2.4, 2.6, the desired conclusion follows.

**Corollary 2.8.** *A Prüfer domain D has finite character if and only if every nonzero locally principal ideal of D is invertible.*

## 3 Generalization to Non-Prüfer Domains

We start this section by recalling some basic facts about star operations.

Let $D$ be an integral domain with quotient field $K$. The set $\mathbf{F}(D)$ denotes the nonzero fractional ideals of $D$ and $\mathbf{f}(D)$ the nonzero finitely generated fractional ideals of $D$.

A map $\star : \mathbf{F}(D) \to \mathbf{F}(D)$, $I \mapsto I^\star$ is called a *star operation* if the following conditions hold for all $x \in K \setminus \{0\}$ and $I, J \in \mathbf{F}(D)$:

($\star_1$) $(xD)^\star = xD$;
($\star_2$) $I \subseteq J \Rightarrow I^\star \subseteq J^\star$;
($\star_3$) $I \subseteq I^\star$ and $I^{\star\star} := (I^\star)^\star = I^\star$.

Given a star operation $\star$, a nonzero ideal $I$ of $D$ such that $I = I^\star$ is called a $\star$*–ideal*.

Examples of star operations are the $d$-operation, the $v$-operation, and the $t$-operation:

- The *$d$-operation* is the identity map $I \mapsto I$.
- The *$v$-operation* is the map:

$$I \mapsto I^v := (D\colon (D\colon I)), \quad \text{where} \quad (D\colon I) := I^{-1} = \{x \in K \mid xI \subseteq D\}.$$

- the *$t$-operation* is the map:

$$I \mapsto I^t := \bigcup_{J \in \mathbf{f}(D),\, J \subseteq I} J^v.$$

A star operation $\star$ on $D$ is *of finite type* if for all $I \in F(D)$,

$$I^\star = \bigcup \{J^\star : J \subseteq I,\, J \in \mathbf{f}(D)\}.$$

From the definition, it follows that the $t$-operation is of finite type.

**Definition 3.1.** Given a star operation $\star$ on a domain $D$ and $I \in \mathbf{F}(D)$,

$I$ is $\star$*-invertible* if there exists $J \in \mathbf{F}(D)$ such that $(IJ)^\star = D$ (it is easy to see that, in this case, $J = I^{-1}$).

Thus, taking $\star = d$, we find the usual definition of invertible ideal, that is $II^{-1} = D$.

An ideal $I$ is $\star$-finite if there exists a finitely generated ideal $J$ such that $J^\star = I^\star$. If $\star$ is of finite type, $J$ can always be taken inside $I$.

If $\star$ is a star operation of finite type, the set of $\star$-ideals has (proper) maximal elements called $\star$-maximal ideals (this set is denoted by $\star - \mathrm{Max}(D)$). A $\star$-maximal ideal is a prime ideal and every integral $\star$-ideal is contained in a $\star$-maximal ideal.

A domain $D$ has the *$\star$-finite character* if each $\star$-ideal (equivalently, each nonzero element) of $D$ is contained in finitely many $\star$-maximal ideals.

It is well-known that a nonzero ideal of a domain $D$ is invertible if and only if $I$ is finitely generated and locally principal (see [8, II Section 5, Theorem 4]).

A similar characterization holds for $\star$-invertible ideals.

In fact, an ideal $I$ is $\star$-invertible if and only it is $\star$-finite and $\star$-locally principal (that is, $ID_M$ is principal for each $M \in \star - \mathrm{Max}(D)$) ([26, page 137]).

In the characterization of invertible ideals given above, the hypothesis that $I$ is finitely generated can be dropped down in some classes of domains, called LPI domains, introduced by D. D. Anderson and M. Zafrullah in [1].

A domain D is LPI if every nonzero locally principal ideal is invertible, or equivalently, if every faithfully flat ideal is finitely generated. Thus, LPI domains are exactly the domains in which faithfully flat ideals are projective.

Mori domains, and therefore Noetherian domains are LPI.

The finite character condition on a domain $D$ is sufficient to have that $D$ is LPI. In fact, it is a straightforward exercise to prove that the finite character implies that a locally principal ideal is finitely generated. Nevertheless, this condition is not necessary for the LPI property of $D$.

For instance, Noetherian domains are LPI but they do not always have the finite character (see $\mathbb{Z}[X]$).

**Definition 3.2.** A domain $D$ has the $t$-finite character if each nonzero element $x \in D$ is contained in only finitely many $t$-maximal ideals.

Noetherian domains have the $t$-finite character (see [5, Proposition 2.2(b)]) and the $t$-finite character is a sufficient condition for a general domain $D$ to be LPI ([32, Lemma 1.12]).

*Remark 3.3.* In Prüfer domains the $t$-operation is the identity ([21, Theorem 22.1 (3)]), that is, each ideal is a $t$-ideal. Thus, for this class of domains, the $t$-finite character coincides with the finite character, which is exactly the property required for Prüfer domains to be LPI in the conjecture by S. Bazzoni.

The above remark brings to consider the $t$-version of Prüfer domain, the Prüfer $v$-multiplication domains (P$v$MD).

We recall that a domain $D$ is a P$v$MD if each $t$-finite ideal is $t$-invertible. Equivalently, if and only if $D_P$ is a valuation domain for each $t$-prime (or $t$-maximal) ideal $P$ of $D$ ([29, Theorem 4.3]).

Thus, by replacing the finite character with the $t$-finite character and the invertibility property for ideals with the $t$-invertibility property it is possible to generalize S. Bazzoni's conjecture using the $t$-operation.

A first step in this direction is the definition of $t$-LPI domains.

**Definition 3.4.** A domain $D$ is $t$-LPI if each nonzero $t$-locally principal $t$-ideal is $t$-invertible.

The $t$-version of Bazzoni's conjecture is then:

"A P$v$MD is $t$-LPI if and only if it has the $t$-finite character."

M. Zafrullah and F. Halter-Koch proved this result almost at the same time using different techniques (see [35, Proposition 5] and [25]). F. Halter-Koch considered the problem in a more general setting involving a general $\star$-operation.

Now, we consider the $t$-version of Bazzoni's conjecture outside the natural context of P$v$MD and present contributions that prove the equivalence ($\diamond$)

"$t$-finite character $\Leftrightarrow$ each nonzero $t$-locally principal ideal is $t$-invertible"

for more general classes of domains.

We have seen that the $t$-finite character is a sufficient condition for a general domain $D$ in order to have that $D$ is $t$-LPI ([32, Lemma 1.12]).

Conversely, by [18, Example 2.3], if $D$ is not a P$v$MD, the $t$-finite character is not a necessary condition to have that $D$ is $t$-LPI.

Thus, a question that was investigated, for instance, by T. Dumitrescu and M. Zafrullah in [13] and, independently, by C.A. F. - G. Picozza and F.T. in [18], concerns the characterization of classes of domains strictly larger than P$v$MD verifying condition ($\diamond$) given above.

T. Dumitrescu and M. Zafrullah considered the case of $t$-Schreier domains, that we define below.

Given a domain $D$, $\text{Inv}_t(D)$ is the set of the $t$-invertible $t$-ideals of $D$.

A domain $D$ is $t$-Schreier if $\text{Inv}_t(D)$ is a Riesz group, that is: if every finite intersection of nonzero principal ideals is a direct union of $t$-invertible $t$-ideals. For instance, P$v$MD's are $t$-Schreier (see [15, Lemma 1.8]). More precisely, an integral domain is a P$v$MD if and only if it is $t$-Schreier and $v$-coherent, by [14, Corollary 6(a)].

**Theorem 3.5.** [14, Proposition 17] *If $D$ is $t$-Schreier, then $D$ is $t$-LPI if and only if $D$ has the $t$-finite character.*

Thus $t$-Schreier domains enlarge the class of domains verifying the $t$-version of Bazzoni's conjecture.

In this direction, we also find the results by C.A. F. - G. Picozza and F.T. about $v$-coherent domains.

In their paper [18] the authors consider the more general case of a $\star$-operation of finite type, thus including the $t$-operation.

The general question is then to find a characterization of domains for which the $\star$-finite character is equivalent to $\star$-LPI (that is, every $\star$-locally principal $\star$-ideal is $\star$-invertible).

We have seen as Noetherian domains suggest to use the $t$-finite character condition in the study of ($t$)-local invertibility for ideals.

Again, Noetherian domains bring to consider another interesting condition involving ($t$)-comaximal ideals.

In a Noetherian domain every nonzero nonunit element belongs to only a finite number of *mutually comaximal* proper invertible ideals.

**Definition 3.6.** Two proper ideals $I, J \subset D$ are $t$-comaximal if $(I + J)_t = D$. In particular, $I$, $J$ are $t$-comaximal if $(I + J)_t = D$, which means that $I$ and $J$ are not contained in a common $t$-maximal ideal.

**Theorem 3.7.** [18, Proposition 1.6] *Let D be an integral domain. Then the following conditions are equivalent.*

*(i) D has the $t-$finite character.*
*(ii) Every family of mutually $t$-comaximal $t$-finite $t$-ideals of D with nonzero intersection is finite.*

Thus, in order to prove that $t$-LPI is equivalent to the $t$-finite character, it would be interesting to see whether the condition (ii) of the above Theorem has connections with the $t$-LPI property.

Since in Prüfer domains the $t$-operation is the identity, we can restate Theorem 3.7 as follows:

**Corollary 3.8.** *A Prüfer domain D has the finite character if and only if each invertible integral ideal of D is contained in at most a finite number of mutually comaximal invertible ideals.*

Corollary 3.8 can be easily extended to P$v$MD's by replacing comaximality with $t$-comaximality.

**Corollary 3.9.** *A PvMD has the $t$-finite character if and only if each integral $t$-invertible $t$-ideal is contained in at most a finite number of mutually $t$-comaximal $t$-invertible $t$-ideals.*

*Remark 3.10.* Consider the following $t$-invertibility like conditions for ideals in a domain $D$:

(1) $t$-locally $t$-finite (i.e. $I_M$ is $t$-finite for each $M \in t-\mathrm{Max}(D)$, with respect to the $t$-operation of $D_M$) $t$-ideals are $t$-finite;
(2) $t$-locally principal (i.e., $I_M$ is principal for each $M \in t-\mathrm{Max}(D)$) $t$-ideals are $t$-invertible ($t$-LPI);

We observe that

(a) (1) $\Rightarrow$ (2);
(b) conditions (1)–(2) are equivalent to LPI in the case of Prüfer domains and to $t$-LPI for P$v$MD's;
(c) the $t$-finite character implies conditions (1)–(2).

We recall that a domain $D$ is *$v$-coherent* if for any nonzero finitely generated ideal $I$ of $D$, $I^{-1}$ is $v$-finite (see, for instance, [16, Proposition 3.6] and [30]).

A domain $D$ is *$t$-locally $v$-coherent* if $D_M$ is $v$-coherent, for each $M \in t-\mathrm{Max}(D)$.

Important classes of $v$-coherent domains are Noetherian domains, Mori domains, Prüfer domains, P$v$MD's, finite conductor domains (i.e., $(x) \cap (y)$ is finitely generated for each $x, y \in A$), coherent domains (i.e., the intersection of two finitely generated ideals is finitely generated).

Using pullback constructions it is possible to give examples of $t$-locally $v$-coherent domains which are not $v$-coherent (cfr. [20]).

Since both Prüfer domains and P$v$MD's are $t$-locally $v$-coherent, a first step in the direction of generalizing Bazzoni's conjecture to any domain is the following theorem.

**Theorem 3.11.** [18, Theorem 1.11] *Let $D$ be an integral domain which is $t$-locally $v$-coherent. Then the following conditions are equivalent.*

*(i) $D$ has the $t$-finite character;*
*(ii) every family of $t$-finite, $t$-comaximal, $t$-ideals over a nonzero element $a \in D$ is finite;*
*(iii) every nonzero $t$-locally $t$-finite $t$-ideal is $t$-finite.*

*Remark 3.12.* (a) A $t$-locally $v$-coherent domain is not necessarily a P$v$MD. In fact any Noetherian domain is $t$-locally $v$-coherent (and it is not always a P$v$MD). Thus, the class of domains considered in Theorem 3.11 is larger than one of the P$v$MD's.

(b) Condition (iii) of Theorem 3.11 is exactly point (1) of Remark 3.10. Thus it implies the $t$-LPI property (point (2) of the same Remark) and it is equivalent to $t$-LPI in P$v$MD's. In general, we don't know whether these two conditions are equivalent.
Anyway, Theorem 3.11 suggests that a natural statement to generalize to any domain of the $t$-version of Bazzoni's conjecture should claim the equivalence between the $t$-finite character and condition (1) of Remark 3.10.

(c) In general, Theorem 3.11 cannot be extended to any finite type star operation. For instance, it fails if we take the identity operation $d$. In fact, a Noetherian domain does not need to have the finite character on maximal ideals, but each locally finitely generated ideal is finitely generated.

So far, the $t$-operation seems to be the only star operation of finite type that has an interesting role in the generalization of Bazzoni's conjecture.

In fact there is not an analogue of Theorem 3.11 for a generic $\star$-operation. Here below we give two partial results in this direction.

Independently, the authors in [13, Corollary 3] and in [18, Proposition 1.6] put in connection some families of mutually $\star$-comaximal ideals of $D$ with the $\star$-finite character of $D$.

The following theorem generalizes Theorem 3.7 to any star operation of finite type.

**Theorem 3.13.** *Let $D$ be an integral domain and $\star$ a finite type star operation on $D$. Then the following conditions are equivalent.*

*(i)* *$D$ has the $\star$-finite character.*
*(ii)* *Every nonzero element $a \in D$ is contained in at most finitely many proper $\star$-finite, mutually $\star$-comaximal $\star$-ideals of $D$.*

There is not a proven connection between condition (ii) of the theorem above and generalizations of $\star$-LPI condition as it happens for the $t$-operation by Theorem 3.11.

The following result states that if things "work well" for the $t$-operation, then there are positive cascade results for finite type star operations.

**Proposition 3.14.** [18, Proposition 2.2] *Let $D$ be a domain in which each $t$-locally principal $t$-ideal is $t$-finite. Then, for any star operation of finite type, each $\star$-locally principal $\star$-ideal is $\star$-finite. In particular, a locally principal ideal is finitely generated (and so, invertible).*

In Proposition 3.14 the $t$-operation cannot be replaced by any finite type star operation. For instance, [18, Example 2.3] shows that it does not hold when $\star = d$.

Another interesting class of domains recently studied in this context are the *finitely stable* domains.

**Definition 3.15.** An ideal $I$ of a domain $D$ is *finitely stable* if $I$ is invertible (or projective) in its endomorphism ring

$$End(I) = (I : I) = \{x \in K \mid xI \subseteq I\}.$$

A domain $D$ is *stable* if each nonzero ideal is stable and $D$ is *finitely stable* if each finitely generated ideal is stable. Obviously, stable domains are finitely stable.

An important result proven by B. Olberding in [31] states that stable domains have the finite character. Moreover, integrally closed stable domains are Prüfer, thus they are LPI.

It is also well-known that integrally closed, finitely stable domains are exactly Prüfer domains, hence they generalize the Prüfer ones.

Moreover, finitely stable domains are a distinct class from $v$-coherent domains. In fact, $D = K[[X^2, X^3]]$ (where $K$ is any field) is Mori, hence $v$-coherent, but it is not finitely stable because its maximal ideal is not stable (see [7, Example 1]).

On the other hand, if we take a P$v$MD that is not Prüfer (e.g., $\mathbb{Z}[X]$), then this is not finitely stable but it is $v$-coherent.

S. Bazzoni in [7] before, and S. Xing and F. Wang in [34] after, study conditions on finitely stable domains in order to verify the LPI property.

A domain has the *local stability property* if each nonzero ideal that is locally stable is stable.

In [7, Theorem 4.5] a characterization of finitely stable domains with finite character is given.

**Theorem 3.16.** *Let $D$ be a finitely stable domain. Then $D$ has the finite character if and only if it has the local stability property.*

[7, Lemma 3.2] shows that if $D$ is a finitely stable domain that has the local stability property then it is LPI.

As we know, the question whether a finitely stable LPI domain has the local stability property is still open ([7, Question 4.6]).

In view of Theorem 3.16, if the answer to this question is positive, then this would imply that also for (non integrally closed) finitely stable domain the finite character is equivalent to LPI, as it happens in the Prüfer case.

Other interesting results about the interplay between the finite character and the LPI property for finitely stable domains are given in [34].

First of all, in this paper the authors show that LPI is not a local property. In fact they give an example of a domain $D$ that is LPI, but $D_S$ is not LPI for a suitable multiplicatively closed subset $S \subseteq D$ ([34, Example 2.4]). This fact has no connections with the finite character question, but it is interesting by itself.

Anyway, the main result of [34] gives a characterization of LPI finitely stable involving the finite character.

The authors denote by $\mathcal{T}(D)$ the set of maximal ideals $m$ of $D$ for which there exists a finitely generated ideal $I$ such that $m$ is the only maximal ideal containing $I$. For each ideal $I$, $\Omega(I)$ is the set of maximal ideals of $D$ containing $I$. Thus, the finite character is equivalent to ask that $\Omega(I)$ is finite for each nonzero ideal $I \subseteq D$.

Then, the following results are proven:

**Theorem 3.17.** [34, Theorem 2.6] *Let $D$ be a finitely stable LPI domain. Then every nonzero element of $D$ is contained in, at most, finitely many ideals of $\mathcal{T}(D)$.*

Thus we have that LPI on finitely stable domains implies the finite character on the subset $\mathcal{T}(D)$ of $\mathrm{Max}(D)$.

From Theorem 3.17 it follows the next corollary:

**Corollary 3.18.** [34, Corollary 2.7] *Let $D$ be a finitely stable LPI domain. Then, the following conditions are equivalent:*

*(i)* *$D$ ha the finite character;*
*(ii)* *$\mathcal{T}(D) \cap \Omega(I) \neq \emptyset$, for each nonzero, finitely generated ideal $I$ of $D$.*

We observe that Corollary 3.18 does not hold without the LPI hypothesis.

In fact, the following example shows that there exists a Prüfer domain $D$ without the finite character and such that $\mathcal{T}(D) = \emptyset$. In this case $D$ is finitely stable (since it is Prüfer) and point (ii) of Corollary 3.18 trivially holds since $\mathcal{T}(D) = \emptyset$, but the domain has not the finite character.

*Example 3.19.* Consider the integer valued polynomial ring

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

It is well-known that Int($\mathbb{Z}$) is a Prüfer domain ([10, Theorem VI.1.7]) and it has not the finite character. In fact, each prime $p \in \mathbb{Z}$ is contained in infinitely many maximal ideals of the type $M_{p,\alpha}$ described in [10, Theorem V.2.7].

We easily see that $\mathcal{T}(\text{Int}(\mathbb{Z})) = \emptyset$. By [10, Theorem V.2.7], the maximal ideals of Int($\mathbb{Z}$) are the $M_{p,\alpha}$, $p \in \mathbb{Z}$, $\alpha \in \widehat{\mathbb{Z}_p}$ (the $p$-adic completion of $\mathbb{Z}$). Suppose that a maximal ideal $M_{p,\alpha}$ belongs to $\mathcal{T}(\text{Int}(\mathbb{Z}))$ and let $I$ be a finitely generated ideal such that $M_{p,\alpha}$ is the only maximal ideal containing $I$. Since Int($\mathbb{Z}$) is a Prüfer domain, $I$ is invertible. But

$$I^{-1} \subseteq \bigcap_{\mathcal{M} \in \text{Max}(\text{Int}(\mathbb{Z})), I \nsubseteq \mathcal{M}} \text{Int}(\mathbb{Z})_{\mathcal{M}},$$

where second term is an overring of Int($\mathbb{Z}$) defined by Kaplansky and so-called the *Kaplansky transform* of the ideal $I$ [17, Theorem 3.2.2]. Using the same argument of [33, Proposition 2.2] to see that $\mathfrak{P}^{-1} = \text{Int}(D)$, we can show that $I^{-1} = \text{Int}(\mathbb{Z})$ against the hypothesis that $I$ is a proper ideal.

## 4 Generalization to Rings with Zero-Divisors

In the present section we will present a generalization of Bazzoni's conjecture to (commutative) rings with zero-divisors. We start with recalling some terminology and preliminaries and we will follow [28]. Let $A \subseteq B$ be a ring extension and let $X$ be an $A$-submodule of $B$. We will say that $X$ is $B$-*regular* if $XB = B$. Furthermore, $X$ is said to be $B$-*invertible* if $XY = A$, for some $A$-submodule $Y$ of $B$. It is worth noting that, in case $B$ is the total ring of fractions $\text{T}(A)$ of $A$, then $X$ is $B$-regular if and only if it is regular (i.e., it contains a regular element of $A$) and $X$ is $B$-invertible if and only if it is invertible in the sense of Griffin (see [24]). Several known facts about fractional ideals of integral domains extend naturally in this setting: for instance, $X$ is $B$-invertible if and only if $X$ is $B$-regular, finitely generated and locally principal [28, Section 2, Proposition 2.3].

**Definition 4.1.** Let $A \subseteq B$ be a ring extension. We say that $A \subseteq B$ *has finite character* if every $B$-regular ideal of $A$ is contained only in finitely many maximal ideals of $A$.

Clearly, if $B = \text{T}(A)$, then $A \subseteq B$ has finite character if and only if every regular ideal of $A$ is contained only in finitely many maximal ideal. The following result extends Theorem 3.13 (in case $\star = d$) to every ring extension.

**Proposition 4.2.** [19, Corollary 3.3] *For a ring extension $A \subseteq B$ the following conditions are equivalent.*

*(1) $A \subseteq B$ has finite character.*
*(2) For any finitely generated and $B$-regular ideal $\mathfrak{a}$ of $A$, every collection of mutually comaximal finitely generated (and $B$-regular) ideals of $A$ containing $\mathfrak{a}$ is finite.*

Finite character ring extensions allows to test relevant properties of ideals locally, as the following result shows.

**Proposition 4.3.** ([19, Proposition 3.4 and Corollary 3.5]) *Let $A \subseteq B$ be a ring extension with finite character and let $\mathfrak{a}$ be a $B$-regular ideal of $A$. If $\mathfrak{a}$ is locally finitely generated, then $\mathfrak{a}$ is finitely generated. In particular, $\mathfrak{a}$ is $B$-invertible if and only if it is locally principal.*

According to [28, Chapter 2, Theorem 2.1], we say that a ring extension $A \subseteq B$ is a *Prüfer extension* if $A \subseteq B$ is a flat epimorphism (in the category of rings) and every finitely generated $B$-regular ideal of $A$ is $B$-invertible. In case $B = \mathrm{T}(A)$, then the previous definition extends the notion of Prüfer ring given by Griffin (i.e., every regular finitely generated ideal is invertible). In what follows it will suffice to work with the following weaker notion.

**Definition 4.4.** A ring extension $A \subseteq B$ is said to be an *almost Prüfer* extension if every finitely generated $B$-regular ideal of $A$ is $B$-invertible.

Now we are in condition to state Bazzoni's conjecture for rings with zero-divisors.

**Theorem 4.5.** [19, Theorem 4.5] *For an almost Prüfer extension $A \subseteq B$ the following conditions are equivalent.*

*(1) $A \subseteq B$ has finite character.*
*(2) Every $B$-regular locally principal ideal of $A$ is $B$-invertible.*

Keeping in mind the remarks made at the beginning of the present section, the following corollary is now clear.

**Corollary 4.6.** [19, Corollary 4.6] *Let A be a Prüfer ring. Then every regular locally principal ideal of A is invertible if and only if every regular element of A is contained in only finitely many maximal ideal.*

Finally we list some problems and questions that can motivate further investigation about this topic.

**Question 1**. Is there a class of integral domains, larger than that of $t$-locally $v$-coherent domains, for which the equivalent conditions of Theorem 3.11 hold?

**Question 2**. Does the statement of Theorem 3.16 admit some generalization for rings with zero-divisors?

**Acknowledgements** The first and the second authors were partially supported by GNSAGA of Istituto Nazionale di Alta Matematica. The first author was partially supported by Dipartimento di Matematica e Informatica of Università di Catania (Research program "Proprietà algebriche locali e globali di anelli associati a curve e ipersuperfici" PTR 2016–18), and by the research program "Reducing complexity in algebra, logic, combinatorics - REDCOM" "Ricerca Scientifica di Eccellenza 2018" Fondazione Cariverona.

## References


1. Anderson, D.D., Zafrullah, M.: Integral domains in which nonzero locally principal ideals are invertible. Commun. Algebra **39**(3), 933–941 (2011)
2. Anderson, D.D., Anderson, D.F.: Some remarks on cancellation ideals. Math. Jpn. **29**(6), 879–886 (1984)
3. Atiyah, M.F., MacDonald, I.G.: Introduction to Commutative Algebra, Addison-Wesley Series in Mathematics (1969)
4. Bazzoni, S.: Clifford regular domains. J. Algebra **238**, 703–722 (2001)
5. Barucci, V., Gabelli, S.: How far is a Mori domain from being a Krull domain? J. Pure Appl. Algebra **2**(45), 101–112 (1987)
6. Bazzoni, S.: Class semigroups of Prüfer domains. J. Algebra **184**, 613–631 (1996)
7. Bazzoni, S.: Finite character of finitely stable domains. J. Pure Appl. Algebra **215**(6), 1127–1132 (2011)
8. Bourbaki, N.: Algèbre Commutative. Chapter 1–7. Hermann Paris, pp. 1961–1965
9. Brewer, J., Klingler, L.: The ordered group of invertible ideals of a Prüfer domain of finite character. Commun. Algebra **33**(11), 4197–4203 (2005)
10. Cahen, P.-J. Chabert, J.-L.: Integer-Valued Polynomials. Surveys and Monographs, vol. 48, Providence (1997) (Am. Math. Soc.)
11. Conrad, P.: Some structure theorems for lattice-ordered groups. Trans. Am. Math. Soc. **99**(2), 212–240 (1961)
12. Darnel, M.: Theory of Lattice-Ordered Groups. Monographs and Textbooks Pure and Applied Mathematics, vol. 187. Marcel Dekker (1995)
13. Dumitrescu, T., Zafrullah, M.: Characterizing domains of finite star-character. J. Pure Appl. Algebra **214**(11), 2087–2091 (2010)
14. Dumitrescu, T., Zafrullah, M.: t-Schreier Domains. Commun. Algebra **39**(3), 808–818 (2011)
15. El Baghdadi, S., Gabelli, S., Zafrullah, M.: Unique representation domains II. J. Pure Appl. Algebra **212**, 376–393 (2008)
16. Fontana, M., Gabelli, S.: On the class group and the local class group of a pullback. J. Algebra **181**(3), 803–835 (1996)
17. Fontana, M., Huckaba, J.A., Papick, I.J.: Prüfer Domains. Pure and Applied Mathematics, vol. 203. Marcel Dekker, New York (1997)
18. Finocchiaro, C.A., Picozza, G., Tartarone, F.: Star-invertibility and t-finite character in integral domains. J. Algebra Appl. **10**(4), 755–769 (2011)
19. Finocchiaro, C.A., Tartarone,F.: Invertibility of ideals in Prüfer extensions. Commun. Algebra **45**(10), 4521–4527 (2017)
20. Gabelli, S., Houston, E.G.: Coherent-like conditions in pullbacks. Mich. Math. J. **44**, 99–123 (1997)
21. Gilmer, R.: Multiplicative Ideal Theory. Marcel Dekker, New York (1972)
22. Glaz, S., Vasconcelos, W.V.: Flat ideals II. Manuscripta Math. **22**(4), 325–341 (1977)
23. Glaz, S., Vasconcelos, W.V.: Flat ideals. III. Commun. Algebra **12**(2), 199–227 (1984)
24. Griffin, M.: Prüfer rings with zero-divisors. J. Reine Angew Math. **239**(240), 55–67 (1970)
25. Halter-Koch, F.: Clifford semigroups of ideals in monoids and domains. Forum Math. **21**, 1001–1020 (2009)
26. Halter-Koch, F.: Ideal Systems. An Introduction to Multiplicative Ideal Theory. Monographs and Textbooks in Pure and Applied Mathematics, vol. 211. Marcel Dekker (1998)
27. Holland, W.C., Martinez, J., McGovern, W.Wm., Tesemma, M.: Bazzoni's conjecture. J. Algebra **320**, 1764–1768 (2008)
28. Knebush, M., Zhang, D.: Manis Valuations and Prüfer Extensions I. Lecture Notes in Mathematics, vol. 1791. Springer (2002)
29. Mott, J., Zafrullah, M.: On Prüfer $v$-multiplication domains. Manuscripta Math. **35**(1–2), 1–26 (1981)
30. Nour El Abidine, D.: Groupe des classes de certains aimeaux integres et ideaux transformes. These de Doctorat, Universite Claude Bernard, F-Lyon 1 (1992)

31. Olberding, B.: On the structure of stable domains. Commun. Algebra **30**(2), 877–895 (2002)
32. Picozza, G., Tartarone, F.: Flat ideals and stability in integral domains. J. Algebra **324**, 1790–1802 (2010)
33. Tartarone, Francesca: Divisorial prime ideals of Int(D) when D is a Krull-type domain. Commun. Algebra **28**(10), 4647–4663 (2000)
34. Xing, S., Wang, F.: Two questions on domains in which locally principal ideals are invertible. J. Algebra Appl. **16**(6), 1750112 (2017)
35. Zafrullah, M.: t-Invertibility and Bazzoni-like statements. J. Pure Appl. Algebra **210**(5), 654–657 (2010)

# Idempotence and Divisoriality in Prüfer-Like Domains

**Marco Fontana, Evan Houston, and Mi Hee Park**

**Abstract** Let $D$ be a Prüfer $\star$-multiplication domain, where $\star$ is a semistar operation on $D$. We show that certain ideal-theoretic properties related to idempotence and divisoriality hold in Prüfer domains, and we use the associated semistar Nagata ring of $D$ to show that the natural counterparts of these properties also hold in $D$.

**Keywords** Idempotent ideal · Semistar operation · Prüfer $\star$-multiplication domain · Nagata ring · Divisorial ideal

## 1 Introduction and Preliminaries

Throughout this work, $D$ will denote an integral domain, and $K$ will denote its quotient field. Recall that Arnold [1] proved that $D$ is a Prüfer domain if and only if its associated Nagata ring $D[X]_N$, where $N$ is the set of polynomials in $D[X]$ whose coefficients generate the unit ideal, is a Prüfer domain. This was generalized

The first-named author was partially supported by *GNSAGA* of *Istituto Nazionale di Alta Matematica*.
The second-named author was supported by a grant from the Simons Foundation (#354565).
The third-named author was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2015R1C1A2A01055124).

M. Fontana
Dipartimento di Matematica e Fisica, Università degli Studi Roma Tre,
Largo San Leonardo Murialdo, 1, 00146 Roma, Italy
e-mail: fontana@mat.uniroma3.it

E. Houston (✉)
Department of Mathematics and Statistics, University of North Carolina at Charlotte,
Charlotte, NC 28223, USA
e-mail: eghousto@uncc.edu

M. H. Park
Department of Mathematics, Chung-Ang University, Seoul 06974, Korea
e-mail: mhpark@cau.ac.kr



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_9

to Prüfer $v$-multiplication domains (P$v$MDs) by Zafrullah [16] and Kang [14] and to Prüfer $\star$-multiplication domains (P$\star$MDs) by Fontana, Jara, and Santos [8].

Our goal in this paper is to show that certain ideal-theoretic properties that hold in Prüfer domains transfer in a natural way to P$\star$MDs. For example, we show that an ideal $I$ of a Prüfer domain is idempotent if and only if it is a radical ideal each of whose minimal primes is idempotent (Theorem 2.9), and we use a Nagata ring transfer "machine" to transfer a natural counterpart of this characterization to P$\star$MDs. For another example, in Theorem 3.5 we show that an ideal in a Prüfer domain of finite character is idempotent if and only if it is a product of idempotent prime ideals and, perhaps more interestingly, we characterize ideals that are simultaneously idempotent and divisorial as (unique) products of incomparable divisorial idempotent primes; and we then extend this to P$\star$MDs.

Let us review the terminology and notation. Denote by $\overline{\boldsymbol{F}}(D)$ the set of all nonzero $D$–submodules of $K$, and by $\boldsymbol{F}(D)$ the set of all nonzero fractional ideals of $D$, i.e., $E \in \boldsymbol{F}(D)$ if $E \in \overline{\boldsymbol{F}}(D)$ and there exists a nonzero $d \in D$ with $dE \subseteq D$. Let $\boldsymbol{f}(D)$ be the set of all nonzero finitely generated $D$–submodules of $K$. Then, obviously, $\boldsymbol{f}(D) \subseteq \boldsymbol{F}(D) \subseteq \overline{\boldsymbol{F}}(D)$.

Following Okabe-Matsuda [15], a *semistar operation* on $D$ is a map $\star : \overline{\boldsymbol{F}}(D) \to \overline{\boldsymbol{F}}(D)$, $E \mapsto E^\star$, such that, for all $x \in K$, $x \neq 0$, and for all $E, F \in \overline{\boldsymbol{F}}(D)$, the following properties hold:

($\star_1$) $(xE)^\star = xE^\star$;
($\star_2$) $E \subseteq F$ implies $E^\star \subseteq F^\star$;
($\star_3$) $E \subseteq E^\star$ and $E^{\star\star} := (E^\star)^\star = E^\star$.

Of course, semistar operations are natural generalizations of star operations–see the discussion following Corollary 2.5 below.

The semistar operation $\star$ is said to have *finite type* if $E^\star = \bigcup\{F^\star \mid F \in \boldsymbol{f}(D), F \subseteq E\}$ for each $E \in \overline{\boldsymbol{F}}(D)$. To any semistar operation $\star$ we can associate a finite-type semistar operation $\star_f$ given by

$$E^{\star_f} := \bigcup\{F^\star \mid F \in \boldsymbol{f}(D), F \subseteq E\}.$$

We say that a nonzero ideal $I$ of $D$ is a *quasi-$\star$-ideal* if $I = I^\star \cap D$, a *quasi-$\star$-prime ideal* if it is a prime quasi-$\star$-ideal, and a *quasi-$\star$-maximal ideal* if it is maximal in the set of all proper quasi-$\star$-ideals. A quasi-$\star$-maximal ideal is a prime ideal. We will denote by $\mathrm{QMax}^\star(D)$ ($\mathrm{QSpec}^\star(D)$) the set of all quasi-$\star$-maximal ideals (quasi-$\star$-prime ideals) of $D$. While quasi-$\star$-maximal ideals may not exist, quasi-$\star_f$-maximal ideals are plentiful in the sense that each proper quasi-$\star_f$-ideal is contained in a quasi-$\star_f$-maximal ideal. (See [9] for details.) Now we can associate to $\star$ yet another semistar operation: for $E \in \overline{\boldsymbol{F}}(D)$, set

$$E^{\widetilde{\star}} := \bigcap\{ED_Q \mid Q \in \mathrm{QMax}^{\star_f}(D)\}.$$

Then $\widetilde{\star}$ is also a finite-type semistar operation, and we have $E^{\widetilde{\star}} \subseteq E^{\star_f} \subseteq E^{\star}$ for all $E \in \overline{\boldsymbol{F}}(D)$.

Let $\star$ be a semistar operation on $D$. Set $N(\star) = \{g \in D[X] \mid c(g)^{\star} = D^{\star}\}$, where $c(g)$ is the *content* of the polynomial $g$, i.e., the ideal of $D$ generated by the coefficients of $g$. Then $N(\star)$ is a saturated multiplicatively closed subset of $D[X]$, and we call the ring $\mathrm{Na}(D, \star) := D[X]_{N(\star)}$ the *semistar Nagata ring of* $D$ *with respect to* $\star$. The domain $D$ is called a *Prüfer* $\star$*- multiplication domain* (P$\star$MD) if $(FF^{-1})^{\star_f} = D^{\star_f}$ $(= D^{\star})$ for each $F \in \boldsymbol{f}(D)$ (i.e., each such $F$ is $\star_f$-invertible). (Recall that $F^{-1} = (D : F) = \{u \in K \mid uF \subseteq D\}$.)

In the following two lemmas, we assemble the facts we need about Nagata rings and P$\star$MDs. Most of the proofs can be found in [6, 9] or [5].

**Lemma 1.1.** *Let $\star$ be a semistar operation on $D$. Then:*

(1) $D^{\star} = D^{\star_f}$.
(2) $\mathrm{QMax}^{\star_f}(D) = \mathrm{QMax}^{\widetilde{\star}}(D)$.
(3) *The map* $\mathrm{QMax}^{\star_f}(D) \to \mathrm{Max}(\mathrm{Na}(D, \star))$, $P \mapsto P\mathrm{Na}(D, \star)$, *is a bijection with inverse map* $M \mapsto M \cap D$.
(4) $P \mapsto P\mathrm{Na}(D, \star)$ *defines an injective map* $\mathrm{QSpec}^{\widetilde{\star}}(D) \to \mathrm{Spec}(\mathrm{Na}(D, \star))$.
(5) $N(\star) = N(\star_f) = N(\widetilde{\star})$ *and (hence)* $\mathrm{Na}(D, \star) = \mathrm{Na}(D, \star_f) = \mathrm{Na}(D, \widetilde{\star})$.
(6) *For each* $E \in \overline{\boldsymbol{F}}(D)$, $E^{\widetilde{\star}} = E\mathrm{Na}(D, \star) \cap K$, *and* $E^{\widetilde{\star}}\mathrm{Na}(D, \star) = E\mathrm{Na}(D, \star)$.
(7) *A nonzero ideal $I$ of $D$ is a quasi-$\widetilde{\star}$-ideal if and only if* $I = I\mathrm{Na}(D, \star) \cap D$.

**Lemma 1.2.** *Let $\star$ be a semistar operation on $D$.*

(1) *The following statements are equivalent.*
  (a) *$D$ is a P$\star$MD.*
  (b) $\mathrm{Na}(D, \star)$ *is a Prüfer domain.*
  (c) *The ideals of* $\mathrm{Na}(D, \star)$ *are extended from ideals of $D$.*
  (d) *$D_P$ is a valuation domain for each* $P \in \mathrm{QMax}^{\star_f}(D)$.
(2) *Assume that $D$ is a P$\star$MD. Then:*
  (a) $\widetilde{\star} = \star_f$ *and (hence)* $D^{\star} = D^{\widetilde{\star}}$.
  (b) *The map* $\mathrm{QSpec}^{\star_f}(D) \to \mathrm{Spec}(\mathrm{Na}(D, \star))$, $P \mapsto P\mathrm{Na}(D, \star)$, *is a bijection with inverse map* $Q \mapsto Q \cap D$.
  (c) *Finitely generated ideals of* $\mathrm{Na}(D, \star)$ *are extended from finitely generated ideals of $D$.*

## 2 Idempotence

We begin with our basic definition.

**Definition 2.1.** *Let $\star$ be a semistar operation on $D$. An element* $E \in \overline{\boldsymbol{F}}(D)$ *is said to be $\star$-idempotent if* $E^{\star} = (E^2)^{\star}$.

Our primary interest will be in (nonzero) $\star$-idempotent *ideals* of $D$. Let $\star$ be a semistar operation on $D$, and let $I$ be a nonzero ideal of $D$. It is well known that $I^\star \cap D$ is a quasi-$\star$-ideal of $D$. (This is easy to see: we have

$$(I^\star \cap D)^\star \subseteq I^{\star\star} = I^\star = (I \cap D)^\star \subseteq (I^\star \cap D)^\star,$$

and hence $I^\star = (I^\star \cap D)^\star$; it follows that $I^\star \cap D = (I^\star \cap D)^\star \cap D$.) It, therefore, seems natural to call $I^\star \cap D$ the *quasi-$\star$-closure* of $I$. If we also call $I$ *$\star$-proper* when $I^\star \subsetneq D^\star$, then it is easy to see that $I$ is $\star$-proper if and only if its quasi-$\star$-closure is a proper quasi-$\star$-ideal. Now suppose that $I$ is $\star$-idempotent. Then

$$(I^\star \cap D)^\star = I^\star = (I^2)^\star = ((I^\star)^2)^\star = (((I^\star \cap D)^\star)^2)^\star = ((I^\star \cap D)^2)^\star,$$

whence $I^\star \cap D$ is a $\star$-idempotent quasi-$\star$-ideal of $D$. A similar argument gives the converse. Thus a ($\star$-proper) nonzero ideal is $\star$-idempotent if and only if its quasi-$\star$-closure is a (proper) $\star$-idempotent quasi-$\star$-ideal.

Our study of idempotence in Prüfer domains and P$\star$MDs involves the notions of sharpness and branchedness. We recall some notation and terminology.

Given an integral domain $D$ and a prime ideal $P \in \text{Spec}(D)$, set

$$\nabla(P) := \{M \in \text{Max}(D) \mid M \not\supseteq P\} \text{ and}$$
$$\Theta(P) := \bigcap\{D_M \mid M \in \nabla(P)\}.$$

We say that $P$ is *sharp* if $\Theta(P) \nsubseteq D_P$ (see [11, Lemma 1] and [3, Section 1 and Proposition 2.2]). The domain $D$ itself is *sharp* (*doublesharp*) if every maximal (prime) ideal of $D$ is sharp. (Note that a Prüfer domain $D$ is doublesharp if and only if each overring of $D$ is sharp [7, Theorem 4.1.7].) Now let $\star$ be a semistar operation on $D$. Given a prime ideal $P \in \text{QSpec}^{\star_f}(D)$, set

$$\nabla^{\star_f}(P) := \{M \in \text{QMax}^{\star_f}(D) \mid M \not\supseteq P\} \text{ and}$$
$$\Theta^{\star_f}(P) := \bigcap\{D_M \mid M \in \nabla^{\star_f}(P)\}.$$

Call $P$ *$\star_f$-sharp* if $\Theta^{\star_f}(P) \nsubseteq D_P$. For example, if $\star = d$ is the identity, then the $\star_f$-sharp property coincides with the sharp property. We then say that $D$ is $\star_f$-(double)sharp if each quasi-$\star_f$-maximal (quasi-$\star_f$-prime) ideal of $D$ is $\star_f$-sharp. (For more on sharpness, see [10, 11, 13], [7, page 62], [3], [4, Chapter 2, Section 3] and [5].)

Recall that a prime ideal $P$ of a ring is said to be *branched* if there is a $P$-primary ideal distinct from $P$. Also, recall that the domain $D$ has *finite character* if each nonzero ideal of $D$ is contained in only finitely many maximal ideals of $D$.

We now prove a lemma that discusses the transfer of ideal-theoretic properties between $D$ (on which a semistar operation $\star$ has been defined) and its associated Nagata ring.

**Lemma 2.2.** *Let $\star$ be a semistar operation on $D$.*

(1) *Let $E \in \overline{\boldsymbol{F}}(D)$. Then $E$ is $\widetilde{\star}$-idempotent if and only if $E\mathrm{Na}(D,\star)$ is idempotent. In particular, if $D$ is a P$\star$MD, then $E$ is $\star_f$-idempotent if and only if $E\mathrm{Na}(D,\star)$ is idempotent.*

(2) *Let $P$ be a quasi-$\widetilde{\star}$-prime of $D$ and $I$ a nonzero ideal of $D$. Then:*

   (a) *$I$ is $P$-primary in $D$ if and only if $I$ is a quasi-$\widetilde{\star}$-ideal of $D$ and $I\mathrm{Na}(D,\star)$ is $P\mathrm{Na}(D,\star)$-primary in $\mathrm{Na}(D,\star)$.*

   (b) *$P$ is branched in $D$ if and only if $P\mathrm{Na}(D,\star)$ is branched in $\mathrm{Na}(D,\star)$.*

(3) *$D$ has $\star_f$-finite character (i.e., each nonzero element of $D$ belongs to only finitely many (possibly zero) $M \in \mathrm{QMax}^{\star_f}(D)$) if and only if $\mathrm{Na}(D,\star)$ has finite character.*

(4) *Let $I$ be a quasi-$\widetilde{\star}$-ideal of $D$. Then $I$ is a radical ideal if and only if $I\mathrm{Na}(D,\star)$ is a radical ideal of $\mathrm{Na}(D,\star)$.*

(5) *Assume that $D$ is a P$\star$MD. Then:*

   *(a) If $P \in \mathrm{QSpec}^{\star_f}(D)$, then $P$ is $\star_f$-sharp if and only if $P\mathrm{Na}(D,\star)$ is sharp in $\mathrm{Na}(D,\star)$.*

   *(b) $D$ is $\star_f$-(double)sharp if and only if $\mathrm{Na}(D,\star)$ is (double)sharp.*

*Proof.* (1) We use Lemma 1.1(6). If $E\mathrm{Na}(D,\star)$ is idempotent, then $E^{\widetilde{\star}} = E\mathrm{Na}(D,\star) \cap K = E^2\mathrm{Na}(D,\star) \cap K = (E^2)^{\widetilde{\star}}$. Conversely, if $E$ is $\widetilde{\star}$-idempotent, then $(E\mathrm{Na}(D,\star))^2 = E^2\mathrm{Na}(D,\star) = (E^2)^{\widetilde{\star}}\mathrm{Na}(D,\star) = E^{\widetilde{\star}}\mathrm{Na}(D,\star) = E\mathrm{Na}(D,\star)$. The "in particular" statement follows because $\star_f = \widetilde{\star}$ in a P$\star$MD (Lemma 1.2(2a)).

(2) (a) Suppose that $I$ is $P$-primary. Then $ID[X]$ is $PD[X]$-primary. Since $P$ is a quasi-$\widetilde{\star}$-prime of $D$, $P\mathrm{Na}(D,\star)$ is a prime ideal of $\mathrm{Na}(D,\star)$ (Lemma 1.1(4)), and then, since $\mathrm{Na}(D,\star)$ is a quotient ring of $D[X]$, $I\mathrm{Na}(D,\star)$ is $P\mathrm{Na}(D,\star)$-primary in $\mathrm{Na}(D,\star)$. Also, again using the fact that $ID[X]$ is $PD[X]$-primary (along with Lemma 1.1(6)), we have

$$I^{\widetilde{\star}} \cap D = I\mathrm{Na}(D,\star) \cap D \subseteq ID[X]_{PD[X]} \cap D[X] \cap D = ID[X] \cap D = I,$$

whence $I$ is a quasi-$\widetilde{\star}$-ideal of $D$. Conversely, assume that $I$ is a quasi-$\widetilde{\star}$-ideal of $D$ and that $I\mathrm{Na}(D,\star)$ is $P\mathrm{Na}(D,\star)$-primary. Then for $a \in P$, there is a positive integer $n$ for which $a^n \in I\mathrm{Na}(D,\star) \cap D = I^{\widetilde{\star}} \cap D = I$. Hence $P = \mathrm{rad}(I)$. It now follows easily that $I$ is $P$-primary. (b) Suppose that $P$ is branched in $D$. Then there is a $P$-primary ideal $I$ of $D$ distinct from $P$, and $I\mathrm{Na}(D,\star)$ is $P\mathrm{Na}(D,\star)$-primary by (a). Also by (a), $I$ is a quasi-$\widetilde{\star}$-ideal, from which it follows that $I\mathrm{Na}(D,\star) \neq P\mathrm{Na}(D,\star)$. Now suppose that $P\mathrm{Na}(D,\star)$ is branched and that $J$ is a $P\mathrm{Na}(D,\star)$-primary ideal of $\mathrm{Na}(D,\star)$ distinct from $P\mathrm{Na}(D,\star)$. Then it is straightforward to show that $J \cap D$ is distinct from $P$ and is $P$-primary.

(3) Let $\psi$ be a nonzero element of $\mathrm{Na}(D,\star)$, and let $N$ be a maximal ideal with $\psi \in N$. Then $\psi\mathrm{Na}(D,\star) = f\mathrm{Na}(D,\star)$ for some $f \in D[X]$, and writing $N = M\mathrm{Na}(D,\star)$ for some $M \in \mathrm{QMax}^{\star_f}(D)$ (Lemma 1.1(3)), we must have $f \in MD[X]$

and hence $c(f) \subseteq M$. Therefore, if $D$ has finite $\star_f$-character, then $\text{Na}(D, \star)$ has finite character. The converse is even more straightforward.

(4) Suppose that $I$ is a radical ideal of $D$, and let $\psi^n \in I\text{Na}(D, \star)$ for some $\psi \in \text{Na}(D, \star)$ and positive integer $n$. Then there is an element $g \in N(\star)$ with ($g\psi^n$ and hence) $(g\psi)^n \in ID[X]$. Since $ID[X]$ is a radical ideal of $D[X]$, $g\psi \in ID[X]$ and we must have $\psi \in I\text{Na}(D, \star)$. Therefore, $I\text{Na}(D, \star)$ is a radical ideal of $\text{Na}(D, \star)$. The converse follows easily from the fact that $I\text{Na}(D, \star) \cap D = I^{\tilde{\star}} \cap D = I$ (Lemma 1.1(7)).

(5) (a) This is part of [5, Proposition 3.5], but we give here a proof more in the spirit of this paper. Let $P \in \text{QSpec}^{\star_f}(D)$. If $P$ is $\star_f$-sharp, then by [5, Proposition 3.1] $P$ contains a finitely generated ideal $I$ with $I \nsubseteq M$ for all $M \in \nabla^{\star_f}(P)$, and, using the description of $\text{Max}(\text{Na}(D, \star))$ given in Lemma 1.1(3), $I\text{Na}(D, \star)$ is a finitely generated ideal of $\text{Na}(D, \star)$ contained in $P\text{Na}(D, \star)$ but in no element of $\nabla(P\text{Na}(D, \star))$. Therefore, $P\text{Na}(D, \star)$ is sharp in the Prüfer domain $\text{Na}(D, \star)$. For the converse, assume that $P\text{Na}(D, \star)$ is sharp in $\text{Na}(D, \star)$. Then $P\text{Na}(D, \star)$ contains a finitely generated ideal $J$ with $J \subseteq P\text{Na}(D, \star)$ but $J \nsubseteq N$ for $N \in \nabla(P\text{Na}(D, \star))$ [13, Corollary 2]. Then $J = I\text{Na}(D, \star)$ for some finitely generated ideal $I$ of $D$ (necessarily) contained in $P$ by Lemma 1.2(2c), and it is easy to see that $I \nsubseteq M$ for $M \in \nabla^{\star_f}(D)$. Then by [5, Proposition 3.1], $P$ is $\star_f$-sharp. Statement (b) follows easily from (a) (using Lemma 1.2). □

Let $D$ be an almost Dedekind domain with a non-finitely generated maximal ideal $M$. Then $M^{-1} = D$, but $M$ is not idempotent (since $MD_M$ is not idempotent in the Noetherian valuation domain $D_M$). Our next result shows that this cannot happen in a sharp Prüfer domain.

**Theorem 2.3.** *Let $D$ be a Prüfer domain. If $D$ is ($d$-)sharp and $I$ is a nonzero ideal of $D$ with $I^{-1} = D$, then $I$ is idempotent.*

*Proof.* Assume that $D$ is sharp. Proceeding contrapositively, suppose that $I$ is a nonzero, non-idempotent ideal of $D$. Then, for some maximal ideal $M$ of $D$, $ID_M$ is not idempotent in $D_M$. Since $D$ is a sharp domain, we may choose a finitely generated ideal $J$ of $D$ with $J \subseteq M$ but $J \nsubseteq N$ for all maximal ideals $N \neq M$. Since $ID_M$ is a non-idempotent ideal in the valuation domain $D_M$, there is an element $a \in I$ for which $I^2D_M \subsetneq aD_M$. Let $B := J + Da$. Then $I^2D_M \subseteq BD_M$ and, for $N \in \text{Max}(D) \setminus \{M\}$, $I^2D_N \subseteq D_N = BD_N$. Hence $I^2 \subseteq B$. Since $B$ is a proper finitely generated ideal, we then have $(I^2)^{-1} \supseteq B^{-1} \supsetneq D$. Hence $(I^2)^{-1} \neq D$, from which it follows that $I^{-1} \neq D$, as desired. □

Kang [14, Proposition 2.2] proves that, for a nonzero ideal $I$ of $D$, we always have $I^{-1}\text{Na}(D, v) = (\text{Na}(D, v)) : I)$. This cannot be extended to general semistar Nagata rings; for example, if $D$ is an almost Dedekind domain with non-invertible maximal ideal $M$ and we define a semistar operation $\star$ by $E^\star = ED_M$ for $E \in \overline{\boldsymbol{F}}(D)$, then $(D : M) = D$ and hence $(D : M)\text{Na}(D, \star) = \text{Na}(D, \star) = D[X]_{M[X]} = D_M(X) \subsetneq (D_M : MD_M)D_M(X) = (\text{Na}(D, \star) : M\text{Na}(D, \star))$ (where the proper inclusion holds because $MD_M$ is principal in $D_M$). At any rate, what we really require is the equality

$(D^\star : E)\mathrm{Na}(D,\star) = (\mathrm{Na}(D,\star) : E)$ for $E \in \overline{\boldsymbol{F}}(D)$. In the next lemma, we show that this holds in a P⋆MD but not in general. The proof of part (1) of the next lemma is a relatively straightforward translation of the proof of [14, Proposition 2.2] to the semistar setting. In carrying this out, however, we discovered a minor flaw in the proof of [14, Proposition 2.2]. The flaw involves a reference to [12, Proposition 34.8], but this result requires that the domain $D$ be integrally closed. To ensure complete transparency, we give the proof in full detail.

**Lemma 2.4.** *Let $\star$ be a semistar operation on $D$. Then:*

(1) $(D^\star : E)\mathrm{Na}(D,\star) \supseteq (\mathrm{Na}(D,\star) : E)$ *for each* $E \in \overline{\boldsymbol{F}}(D)$.
(2) *The following statements are equivalent:*
   (a) $(D^\star : E)\mathrm{Na}(D,\star) = (\mathrm{Na}(D,\star) : E)$ *for each* $E \in \overline{\boldsymbol{F}}(D)$.
   (b) $D^\star = D^{\tilde{\star}}$.
   (c) $D^\star \subseteq \mathrm{Na}(D,\star)$.
(3) $(D^{\tilde{\star}} : E)\mathrm{Na}(D,\star) = (\mathrm{Na}(D,\star) : E)$ *for each* $E \in \overline{\boldsymbol{F}}(D)$.
(4) *If $D$ is a P⋆MD, then the equivalent conditions in (2) hold.*

*Proof.* (1) Let $E \in \overline{\boldsymbol{F}}(D)$, and let $\psi \in (\mathrm{Na}(D,\star) : E)$. For $a \in E$, $a \neq 0$, we may find $g \in N(\star)$ such that $\psi a g \in D[X]$. This yields $\psi g \in a^{-1}D[X] \subseteq K[X]$, and hence $\psi = f/g$ for some $f \in K[X]$. We claim that $c(f) \subseteq (D^\star : E)$. Granting this, we have $f \in (D^\star : E)D[X]$, from which it follows that $\psi = f/g \in (D^\star : E)\mathrm{Na}(D,\star)$, as desired. To prove the claim, take $b \in E$, and note that $fb \in \mathrm{Na}(D,\star)$. Hence $fbh \in D[X]$ for some $h \in N(\star)$, and so $c(fh)b \subseteq D$. By the content formula [12, Theorem 28.1], there is an integer $m$ for which $c(f)c(h)^{m+1} = c(fh)c(h)^m$. Using the fact that $c(h)^\star = D^\star$, we obtain $c(f)^\star = c(fh)^\star$ and hence that $c(f)b \subseteq c(fh)^\star b \subseteq D^\star$. Therefore, $c(f) \subseteq (D^\star : E)$, as claimed.

(2) Under the assumption in (c), $D^\star \subseteq \mathrm{Na}(D,\star) \cap K = D^{\tilde{\star}}$ (Lemma 1.1(6)). Hence (c) ⇒ (b). Now assume that $D^\star = D^{\tilde{\star}}$. Then for $E \in \overline{\boldsymbol{F}}(D)$, we have $(D^\star : E)E \subseteq D^\star = D^{\tilde{\star}} \subseteq \mathrm{Na}(D,\star)$; using (1), the implication (b) ⇒ (a) follows. That (a) ⇒ (c) follows upon taking $E = D$ in (a).

(3) This follows easily from (2), because $\mathrm{Na}(D,\star) = \mathrm{Na}(D,\tilde{\star})$ by Lemma 1.1(5).

(4) This follows from (2), since if $D$ is a P⋆MD, then $D^\star = D^{\tilde{\star}}$ by Lemma 1.2(2a). □

The conditions in Lemma 2.4(2) need not hold: Let $F \subsetneq k$ be fields, $V = k[[x]]$ the power series ring over $V$ in one variable, and $D = F + M$, where $M = xk[[x]]$. Define a (finite-type) semistar operation $\star$ on $D$ by $A^\star = AV$ for $A \in \overline{\boldsymbol{F}}(D)$. Then $D^\star = V \supsetneq D = D_M = D^{\tilde{\star}}$.

We can now extend Theorem 2.3 to P⋆MDs.

**Corollary 2.5.** *Let $\star$ be a semistar operation on $D$ such that $D$ is a $\star_f$-sharp P⋆MD, and let $I$ be a nonzero ideal of $D$ with $(D^\star : I) = D^\star$. Then $I$ is $\star_f$-idempotent.*

*Proof.* By Lemma 2.4(3), we have

$$(\mathrm{Na}(D,\star) : I\mathrm{Na}(D,\star)) = (D^\star : I)\mathrm{Na}(D,\star) = D^\star \mathrm{Na}(D,\star) = \mathrm{Na}(D,\star).$$

Hence $I\mathrm{Na}(D,\star)$ is idempotent in the Prüfer domain $\mathrm{Na}(D,\star)$ by Theorem 2.3. Lemma 2.2(1) then yields that $I$ is $\star_f$-idempotent. □

Many semistar counterparts of ideal-theoretic properties in domains result in equations that are "external" to $D$, since for a semistar operation $\star$ on $D$ and a nonzero ideal $I$ of $D$, it is possible that $I^\star \nsubseteq D$. Of course, $\star$-idempotence is one such property. Often, one can obtain a "cleaner" counterpart by specializing from P$\star$MDs to "ordinary" P$v$MDs. We recall some terminology. Semistar operations are generalizations of *star* operations, first considered by Krull and repopularized by Gilmer [12, Sections 32, 34]. Roughly, a star operation is a semistar operation restricted to the set $\boldsymbol{F}(D)$ of nonzero fractional ideals of $D$ with the added requirement that one has $D^\star = D$. The most important star operation (aside from the $d$-, or trivial, star operation) is the *$v$-operation*: For $E \in \boldsymbol{F}(D)$, put $E^{-1} = \{x \in K \mid xE \subseteq D\}$ and $E^v = (E^{-1})^{-1}$. Then $v_f$ (restricted to $\boldsymbol{F}(D)$) is the *$t$-operation* and $\widetilde{v}$ is the $w$-operation. Thus a *P$v$MD* is a domain in which each nonzero finitely generated ideal is $t$-invertible. Corollary 2.5 then has the following restricted interpretation (which has the advantage of being *internal* to $D$).

**Corollary 2.6.** *If $D$ is a $t$-sharp P$v$MD and $I$ is a nonzero ideal of $D$ for which $I^{-1} = D$, then $I$ is $t$-idempotent.*

Our next result is a partial converse to Theorem 2.3.

**Proposition 2.7.** *Let $D$ be a Prüfer domain such that $I$ is idempotent whenever $I$ is a nonzero ideal of $D$ with $I^{-1} = D$. Then, every branched maximal ideal of $D$ is sharp.*

*Proof.* Let $M$ be a branched maximal ideal of $D$. Then $MD_M = \mathrm{rad}(aD_M)$ for some nonzero element $a \in M$ [12, Theorem 17.3]. Let $I := aD_M \cap D$. Then $I$ is $M$-primary, and since $ID_M = aD_M$, ($ID_M$ and hence) $I$ is not idempotent. By hypothesis, we may choose $u \in I^{-1} \setminus D$. Since $Iu \subseteq D$ and $ID_N = D_N$ for $N \in \mathrm{Max}(D) \setminus \{M\}$, then $u \in \bigcap\{D_N \mid N \in \mathrm{Max}(D), N \neq M\}$. On the other hand, since $u \notin D$, $u \notin D_M$. It follows that $M$ is sharp. □

Now we extend Proposition 2.7 to P$\star$MDs.

**Corollary 2.8.** *Let $\star$ be a semistar operation on $D$, and assume that $D$ is a P$\star$MD such that $I$ is $\star_f$-idempotent whenever $I$ is a nonzero ideal of $D$ with $(D^\star : I) = D^\star$. Then, each branched quasi-$\star_f$-maximal ideal of $D$ is $\star_f$-sharp. (In particular if $D$ is a P$v$MD in which $I$ is $t$-idempotent whenever $I$ is a nonzero ideal of $D$ with $I^{-1} = D$, then each branched maximal $t$-ideal of $D$ is $t$-sharp.)*

*Proof.* Let $J$ be a a nonzero ideal of the Prüfer domain $\mathrm{Na}(D, \star)$ with $(\mathrm{Na}(D, \star) : J) = \mathrm{Na}(D, \star)$. By Lemma 1.2(1c), $J = I\mathrm{Na}(D, \star)$ for some ideal $I$ of $D$. Applying Lemma 2.4(3) and Lemma 1.1(6), we obtain $(D^\star : I) = D^\star$. Hence, by hypothesis, $I$ is $\star_f$-idempotent, and this yields that $J = I\mathrm{Na}(D, \star)$ is idempotent in the Prüfer domain $\mathrm{Na}(D, \star)$ (Lemma 2.2(1)). Now, let $M$ be a branched quasi-$\star_f$-maximal ideal of $D$. Then, by Lemma 2.2(2), $M\mathrm{Na}(D, \star)$ is a branched maximal ideal of $\mathrm{Na}(D, \star)$. We may now apply Proposition 2.7 to conclude that $M\mathrm{Na}(D, \star)$ is sharp. Therefore, $M$ is $\star_f$-sharp in $D$ by Lemma 2.2(5). □

If $P$ is a prime ideal of a Prüfer domain $D$, then powers of $P$ are $P$-primary by [12, Theorem 23.3(b)]; it follows that $P$ is idempotent if and only if $PD_P$ is idempotent. We use this fact in the next result.

It is well known that a proper idempotent ideal of a valuation domain must be prime [12, Theorem 17.1(3)]. In fact, according to [12, Exercise 3, p. 284], a proper idempotent ideal in a Prüfer domain must be a radical ideal. We (re-)prove and extend this fact and add a converse.

**Theorem 2.9.** *Let $D$ be a Prüfer domain, and let $I$ be an ideal of $D$. Then $I$ is idempotent if and only if $I$ is a radical ideal each of whose minimal primes is idempotent.*

*Proof.* The result is trivial for $I = (0)$ and vacuously true for $I = D$. Suppose that $I$ is a proper nonzero idempotent ideal of $D$, and let $P$ be a prime minimal over $I$. Then $ID_P$ is idempotent, and we must have $ID_P = PD_P$ [12, Theorem 17.1(3)]. Hence $PD_P$ is idempotent, and therefore, by the comment above, so is $P$. Now let $M$ be a maximal ideal containing $I$. Then $ID_M$ is idempotent, hence prime (hence radical). It follows (checking locally) that $I$ is a radical ideal.

Conversely, let $I$ be a radical ideal each of whose minimal primes is idempotent. If $M$ is a maximal ideal containing $I$ and $P$ is a minimal prime of $I$ contained in $M$, then $ID_M = PD_M$. Since $P$ is idempotent, this yields $ID_M = I^2D_M$. It follows that $I$ is idempotent. □

We next extend Theorem 2.9 to P⋆MDs.

**Corollary 2.10.** *Let $D$ be a P⋆MD, where $\star$ is a semistar operation on $D$, and let $I$ be a quasi-$\star_f$-ideal of $D$. Then $I$ is $\star_f$-idempotent if and only if $I$ is a radical ideal each of whose minimal primes is $\star_f$-idempotent. (In particular, if $D$ is a PvMD and $I$ is a $t$-ideal of $D$, then $I$ is $t$-idempotent if and only if $I$ is a radical ideal each of whose minimal primes is $t$-idempotent.)*

*Proof.* Suppose that $I$ is $\star_f$-idempotent. Then $I\mathrm{Na}(D, \star)$ is an idempotent ideal in $\mathrm{Na}(D, \star)$ by Lemma 2.2(1). By Theorem 2.9, $I\mathrm{Na}(D, \star)$ is a radical ideal of $\mathrm{Na}(D, \star)$, and hence, by Lemma 2.2(4), $I$ is a radical ideal of $D$. Now let $P$ be a minimal prime of $I$ in $D$. Then $P$ is a quasi-$\star_f$-prime of $D$. By Lemma 1.2(2b) $P\mathrm{Na}(D, \star)$ is minimal over $I\mathrm{Na}(D, \star)$, whence $P\mathrm{Na}(D, \star)$ is idempotent, again by Theorem 2.9. The $\star_f$-idempotence of $P$ now follows from Lemma 2.2(1).

The converse follows by similar applications of Theorem 2.9 and Lemma 2.2. □

Recall that a Prüfer domain is said to be *strongly discrete* (*discrete*) if it has no nonzero (branched) idempotent prime ideals. Since unbranched primes in a Prüfer domain must be idempotent [12, Theorem 23.3(b)], a Prüfer domain is strongly discrete if and only if it is discrete and has no unbranched prime ideals. We have the following straightforward application of Theorem 2.9.

**Corollary 2.11.** *Let D be a Prüfer domain.*

(1) *If D is discrete, then an ideal I of D is idempotent if and only if I is a radical ideal each of whose minimal primes is unbranched.*
(2) *If D is strongly discrete, then D has no proper nonzero idempotent ideals.*

Let us call a P$\star$MD $\star_f$- *strongly discrete* ($\star_f$- *discrete*) if it has no (branched) $\star_f$-idempotent quasi-$\star_f$-prime ideals. From Lemma 2.2(1, 2), we have the usual connection between a property of a P$\star$MD and the corresponding property of its $\star$-Nagata ring.

**Proposition 2.12.** *Let $\star$ be a semistar operation on D. Then D is $\star_f$-(strongly) discrete P$\star$MD if and only if* $\mathrm{Na}(D, \star)$ *is a (strongly) discrete Prüfer domain.*

Applying Corollary 2.10 and Lemma 2.2(1, 2), we have the following extension of Corollary 2.11.

**Corollary 2.13.** *Let D be a domain.*

(1) *Assume that D is a P$\star$MD for some semistar operation $\star$ on D.*
    (a) *If D is $\star_f$-discrete, then a nonzero quasi-$\star_f$-ideal I of D is $\star_f$-idempotent if and only if I is a radical ideal each of whose minimal primes is unbranched.*
    (b) *If D is $\star_f$-strongly discrete, then D has no $\star_f$-proper $\star_f$-idempotent ideals.*
(2) *Assume that D is a PvMD.*
    (a) *If D is t-discrete, then a t-ideal I of D is t-idempotent if and only if I is a radical ideal each of whose minimal primes is unbranched.*
    (b) *If D is t-strongly discrete, then D has no t-proper t-idempotent ideals.*

## 3 Divisoriality

According to [7, Corollary 4.1.14], if $D$ is a doublesharp Prüfer domain and $P$ is a nonzero, nonmaximal ideal of $D$, then $P$ is divisorial. The natural question arises: If $D$ is a $\star_f$-doublesharp P$\star$MD and $P \in \mathrm{QSpec}^{\star_f}(D) \setminus \mathrm{QMax}^{\star_f}(D)$, is $P$ necessarily divisorial? Since $\star$ is an arbitrary semistar operation and divisoriality specifically involves the $v$-operation, one might expect the answer to be negative. Indeed, we give a counterexample in Example 3.4 below. However, in Theorem 3.2 we prove a general result, a corollary of which does yield divisoriality in the "ordinary" P$v$MD case. First, we need a lemma, the first part of which may be regarded as an extension of [14, Proposition 2.2(2)].

**Lemma 3.1.** *Let $\star$ be a semistar operation on $D$. Then*

(1) $(D^{\tilde{\star}} : (D^{\tilde{\star}} : E))\mathrm{Na}(D, \star) = (\mathrm{Na}(D, \star) : (\mathrm{Na}(D, \star) : E))$ *for each* $E \in \overline{\boldsymbol{F}}(D)$, *and*

(2) *if $I$ is a nonzero ideal of $D$, then $I^{\tilde{\star}}$ is a divisorial ideal of $D^{\tilde{\star}}$ if and only if $I\mathrm{Na}(D, \star)$ is a divisorial ideal of* $\mathrm{Na}(D, \star)$.

*In particular, if $D$ is a P$\star$MD, then $(D^{\star} : (D^{\star} : E))\mathrm{Na}(D, \star) = (\mathrm{Na}(D, \star) : (\mathrm{Na}(D, \star) : E))$ for each $E \in \overline{\boldsymbol{F}}(D)$; and, for a nonzero ideal $I$ of $D$, $I^{\star_f}$ is divisorial in $D^{\star}$ if and only if $I\mathrm{Na}(D, \star)$ is divisorial in* $\mathrm{Na}(D, \star)$.

*Proof.* Set $\mathcal{N} = \mathrm{Na}(D, \star)$. For (1), applying Lemma 2.4, we have

$$(D^{\tilde{\star}} : (D^{\tilde{\star}} : E))\mathcal{N} = (\mathcal{N} : (D^{\tilde{\star}} : E)) = (\mathcal{N} : (\mathcal{N} : E)).$$

(2) Assume that $I$ is a nonzero ideal of $D$. If $I^{\tilde{\star}}$ is divisorial in $D^{\tilde{\star}}$, then (using (1))

$$(\mathcal{N} : (\mathcal{N} : I\mathcal{N})) = (D^{\tilde{\star}} : (D^{\tilde{\star}} : I^{\tilde{\star}}))\mathcal{N} = I^{\tilde{\star}}\mathcal{N} = I\mathcal{N}.$$

Now suppose that $I\mathcal{N}$ is divisorial. Then

$$(D^{\tilde{\star}} : (D^{\tilde{\star}} : I^{\tilde{\star}}))\mathcal{N} = (\mathcal{N} : (\mathcal{N} : I)) = I\mathcal{N},$$

whence

$$(D^{\tilde{\star}} : (D^{\tilde{\star}} : I^{\tilde{\star}})) \subseteq I\mathcal{N} \cap K = I^{\tilde{\star}}.$$

The "in particular" statement follows from standard considerations. □

**Theorem 3.2.** *Let $\star$ be a semistar operation on $D$ such that $D$ is a $\star_f$-doublesharp P$\star$MD, and let $P \in \mathrm{QSpec}^{\star_f}(D) \setminus \mathrm{QMax}^{\star_f}(D)$. Then $P^{\star_f}$ is a divisorial ideal of $D^{\star}$.*

*Proof.* Since $\mathrm{Na}(D, \star)$ is a doublesharp Prüfer domain (Lemma 2.2(5)), $P\mathrm{Na}(D, \star)$ is divisorial by [7, Corollary 4.1.14]. Hence $P^{\star_f}$ is divisorial in $D^{\star}$ by Lemma 3.1. □

**Corollary 3.3.** *If $D$ is a $t$-doublesharp P$v$MD, and $P$ is a non-$t$-maximal $t$-prime of $D$, then $P$ is divisorial.*

*Proof.* Take $\star = v$ in Theorem 3.2. (More precisely, take $\star$ to be any extension of the star operation $v$ on $D$ to a semistar operation on $D$, so that $\star_f$ (restricted to $D$) is the $t$-operation on $D$.) Then $P = P^t = P^{\star_f}$ is divisorial by Theorem 3.2. □

**Example 3.4.** *Let $p$ be a prime integer and let $D := \mathrm{Int}(\mathbb{Z}_{(p)})$. Then $D$ is a two-dimensional Prüfer domain by [2, Lemma VI.1.4 and Proposition V.1.8]. Choose a height 2 maximal ideal $M$ of $D$, and let $P$ be a height 1 prime ideal of $D$ contained in $M$. Then $P = q\mathbb{Q}[X] \cap D$ for some irreducible polynomial $q \in \mathbb{Q}[X]$ [2, Proposition V.2.3]. By [2, Theorems VIII.5.3 and VIII.5.15], $P$ is not a divisorial ideal of $D$. Set $E^{\star} = ED_M$ for $E \in \overline{\boldsymbol{F}}(D)$. Then $\star$ is a finite-type semistar operation on $D$.*

*Clearly, $M$ is the only quasi-$\star$-maximal ideal of $D$, and, since $D_M$ is a valuation domain, $D$ is a P$\star$MD by Lemma 1.2. Moreover,* $\text{Na}(D, \star) = D_M(X)$ *is also a valuation domain and hence a doublesharp Prüfer domain, which yields that $D$ is a $\star_f$-doublesharp P$\star$MD (Lemma 2.2). Finally, since $P = PD_M \cap D = P^\star \cap D$, $P$ is a non-$\star_f$-maximal quasi-$\star_f$-prime of $D$.* □

In the remainder of the paper, we impose on Prüfer domains (P$\star$MDs) the finite character (finite $\star_f$-character) condition. As we shall see, this allows improved versions of Theorem 2.9 and Corollary 2.10. It also allows a type of unique factorization for (quasi-$\star_f$-)ideals that are simultaneously ($\star_f$-)idempotent and ($\star_f$-)divisorial.

**Theorem 3.5.** *Let $D$ be a Prüfer domain with finite character, and let $I$ be a nonzero ideal of $D$. Then:*

(1) *$I$ is idempotent if and only if $I$ is a product of idempotent prime ideals.*
(2) *The following statements are equivalent.*
   (a) *$I$ is idempotent and divisorial.*
   (b) *$I$ is a product of non-maximal idempotent prime ideals.*
   (c) *$I$ is a product of divisorial idempotent prime ideals.*
   (d) *$I$ has a unique representation as the product of incomparable divisorial idempotent primes.*

*Proof.* (1) Suppose that $I$ is idempotent. By Theorem 2.9, $I$ is the intersection of its minimal primes, each of which is idempotent. Since $D$ has finite character, $I$ is contained in only finitely many maximal ideals, and, since no two distinct minimal primes of $I$ can be contained in a single maximal ideal, $I$ has only finitely many minimal primes and they are comaximal. Hence $I$ is the product of its minimal primes (and each is idempotent). The converse is trivial.

(2) (a) $\Rightarrow$ (b): Assume that $I$ is idempotent and divisorial. By (1) and its proof, $I = P_1 \cdots P_n = P_1 \cap \cdots \cap P_n$, where the $P_i$ are the minimal primes of $I$. We claim that each $P_i$ is divisorial. To see this, observe that

$$(P_1)^v P_2 \cdots P_n \subseteq (P_1 \cdots P_n)^v = I^v = I \subseteq P_1.$$

Since the $P_i$ are incomparable, this gives $(P_1)^v \subseteq P_1$, that is, $P_1$ is divisorial. By symmetry each $P_i$ is divisorial. It is well known that in a Prüfer domain, a maximal ideal cannot be both idempotent and divisorial. Hence the $P_i$ are non-maximal.

(b) $\Rightarrow$ (c): Since $D$ has finite character, it is a $(d)$-doublesharp Prüfer domain [13, Theorem 5], whence nonmaximal primes are automatically divisorial by [7, Corollary 4.1.14].

(c) $\Rightarrow$ (a): Write $I = Q_1 \cdots Q_m$, where each $Q_j$ is a divisorial idempotent prime. Since $I$ is idempotent (by (1)), we may also write $I = P_1 \cdots P_n$, where the $P_i$ are the minimal primes of $I$. For each $i$, we have $Q_1 \cdots Q_m = I \subseteq P_i$, from which it follows that $Q_j \subseteq P_i$ for some $j$. By minimality, we must then have $Q_j = P_i$. Thus each $P_i$ is divisorial, whence $I = P_1 \cap \cdots \cap P_n$ is divisorial.

Finally, we show that (d) follows from the other statements. We use the notation in the proof of (c) $\Rightarrow$ (a). In the expression $I = P_1 \cdots P_n$, the $P_i$ are (divisorial, idempotent, and) incomparable, and it is clear that no $P_i$ can be omitted. To see that this is the only such expression, consider a representation $I = Q_1 \cdots Q_m$, where the $Q_i$ are divisorial, idempotent, and incomparable. Fix a $Q_k$. Then $P_1 \cdots P_n = I \subseteq Q_k$, and we have $P_i \subseteq Q_k$ for some $i$. However, as above, $Q_j \subseteq P_i$ for some $j$, whence, by incomparability, $Q_k = P_i$. The conclusion now follows easily. □

We note that incomparability is necessary for uniqueness above, for example, if $D$ is a valuation domain and $P \subsetneq Q$ are non-maximal (necessarily divisorial) primes, then $P = PQ$.

We close by extending Theorem 3.5 to P$\star$MDs and then to "ordinary" P$v$MDs. We omit the (by now) straightforward proofs.

**Corollary 3.6.** *Let $\star$ be a semistar operation on $D$ such that $D$ is a P$\star$MD with finite $\star_f$-character, and let $I$ be a quasi-$\star_f$-ideal of $D$. Then:*

(1) *$I$ is $\star_f$-idempotent if and only if $I^{\star_f}$ is a $\star_f$-product of $\star_f$-idempotent quasi-$\star_f$-prime ideals in $D$, that is, $I^{\star_f} = (P_1 \cdots P_n)^{\star_f}$, where the $P_i$ are $\star_f$-idempotent quasi-$\star_f$-primes of $D$.*

(2) *The following statements are equivalent.*

   (a) *$I$ is $\star_f$-idempotent and $\star_f$-divisorial ($I^{\star_f}$ is divisorial in $D^\star$).*
   (b) *$I$ is a $\star_f$-product of non-quasi-$\star_f$-maximal idempotent quasi-$\star_f$-prime ideals.*
   (c) *$I$ is a $\star_f$-product of $\star_f$-divisorial $\star_f$-idempotent prime ideals.*
   (d) *$I$ has a unique representation as a $\star_f$-product of incomparable $\star_f$-divisorial $\star_f$-idempotent primes.*

**Corollary 3.7.** *Let $D$ be a P$v$MD with finite $t$-character, and let $I$ be a nonzero $t$-ideal of $D$. Then:*

(1) *$I$ is $t$-idempotent if and only if $I$ is a $t$-product of $t$-idempotent $t$-prime ideals in $D$.*

(2) *The following statements are equivalent.*

   (a) *$I$ is $t$-idempotent and divisorial.*
   (b) *$I$ is a $t$-product of non-$t$-maximal $t$-idempotent $t$-primes.*
   (c) *$I$ is a $t$-product of divisorial $t$-idempotent $t$-primes.*
   (d) *$I$ has a unique representation as a $t$-product of incomparable divisorial $t$-idempotent $t$-primes.*

## References

1. Arnold, J.: On the ideal theory of the Kronecker function ring and the domain D(X). Can. J. Math. **21**, 558–563 (1969)
2. Cahen, P.-J., Chabert, J.-L.: Integer-Valued Polynomials, vol. 48. Providence (1997) (Amer. Math. Soc. Surv. Monogr.)

3. Fontana, M., Houston, E., Lucas, T.: Toward a classification of prime ideals in Prüfer domains. Forum Math. **22**, 741–766 (2010)
4. Fontana, M., Houston, E., Lucas, T.: Factoring Ideals in Integral Domains. Lectures Notes of U.M.I. Springer, Berlin (2013)
5. Fontana, M., Houston, E., Park, M.H.: Sharpness and semistar operations in Prüfer-like domains. Commun. Algebra **47**, 1478–1489 (2019)
6. Fontana, M., Huckaba, J.A.: Localizing systems and semistar operations. In: Chapman, S.T., Glaz, S. (eds.) Non-Noetherian Commutative Ring Theory. Kluwer Academic Publishers, pp. 169–198 (2000)
7. Fontana, M., Huckaba, J.A., Papick, I.J.: Prüfer Domains. Marcel Dekker Inc., New York (1997)
8. Fontana, M., Jara, P., Santos, E.: Prüfer $\star$-multiplication domains and semistar operations. J. Algebra Appl. **2**, 21–50 (2003)
9. Fontana, M., Loper, K.A.: Nagata rings, Kronecker function rings and related semistar operations. Commun. Algebra **31**, 4775–4805 (2003)
10. Gilmer, R.: Integral domains which are almost Dedekind. Proc. Am. Math. Soc. **15**, 813–818 (1964)
11. Gilmer, R.: Overrings of Prüfer domains. J. Algebra **4**, 331–340 (1966)
12. Gilmer, R.: Multiplicative Ideal Theory. Marcel Dekker, New York (1972)
13. Gilmer, R., Heinzer, W.: Overrings of Prüfer domains, II. J. Algebra **7**, 281–302 (1967)
14. Kang, B.G.: Prüfer $v$-multiplication domains and the ring $R[X]_{N_v}$. J. Algebra **123**, 151–170 (1989)
15. Okabe, A., Matsuda, R.: Semistar operations on integral domains. Math. J. Toyama Univ. **17**, 1–21 (1994)
16. Zafrullah, M.: Some polynomial characterizations of Prüfer $v$-multiplication domains. J. Pure Appl. Algebra **32**, 231–237 (1984)

# Simultaneous Interpolation and P-adic Approximation by Integer-Valued Polynomials

**Sophie Frisch**

**Abstract** Let $D$ be a Dedekind domain with finite residue fields and $\mathcal{F}$ a finite set of maximal ideals of $D$. Let $r_0, \ldots, r_n$ be distinct elements of $D$, pairwise incongruent modulo $P^{k_P}$ for each $P \in \mathcal{F}$, and $s_0, \ldots, s_n$ arbitrary elements of $D$. We show that there is an interpolating $P^{k_P}$-congruence preserving integer-valued polynomial, that is, $f \in \mathrm{Int}(D) = \{g \in K[x] \mid g(D) \subseteq D\}$ with $f(r_i) = s_i$ for $0 \le i \le n$, such that, moreover, the function $f : D \to D$ is constant modulo $P^{k_P}$ on each residue class of $P^{k_P}$ for all $P \in \mathcal{F}$.

**Keywords** Interpolation · Polynomials · Congruence preserving · $P$-adic approximation · $P$-adic Lipschitz functions · Lipschitz maps · Integer-valued polynomials · Polynomial functions · Polynomial mappings · Dedekind domains · Commutative rings · Integral domains

**Mathematics Subject Classification 2020** Primary 13B25; Secondary 13F20, 13M10, 11C08, 13F05.

## 1 Introduction

Let $D$ be a Dedekind domain with finite residue fields, $K$ its quotient field, and

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

the ring of integer-valued polynomials on $D$.

This research was supported by the Austrian Science Fund FWF grant P30934-N35.

S. Frisch (✉)
Institute of Analysis and Number Theory, Technische Universität Graz, Kopernikusgasse 24, 8010 Graz, Austria
e-mail: frisch@math.tugraz.at



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*, Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_10

We will show that two different feats that can each be accomplished separately by integer-valued polynomials, namely, interpolation of arbitrary functions on $D$, and, representation of arbitrary functions on $D/P^n$, where $P^n$ is a power of a maximal ideal $P$, can actually be accomplished by one and the same polynomial, simultaneously.

We recall some well-known facts. First, about interpolation by integer-valued polynomials: Newton already used polynomials in $\mathrm{Int}(\mathbb{Z})$ to interpolate functions on $\mathbb{Z}$, cf. [1]. More generally, when $D$ is a Dedekind domain with finite residue fields, then, given $r_0, \ldots, r_n \in D$ (distinct) and arbitrary $s_0, \ldots, s_n \in D$, we can find $f \in \mathrm{Int}(D)$ with $f(r_i) = s_i$ for $0 \leq i \leq n$ [3]. If this holds for a domain $D$, we say that $D$ has the interpolation property. The domains having the interpolation property have been characterized among Noetherian domains and among Prüfer domains [2], and include, as mentioned, all Dedekind domains with finite residue fields.

It turned out that the interpolation property is relevant to the question whether $\mathrm{Int}(D)$ is a Prüfer domain. If $D$ is Prüfer (a necessary condition for $\mathrm{Int}(D)$ to be Prüfer) then $\mathrm{Int}(D)$ is Prüfer if and only if $\mathrm{Int}(D)$ has the interpolation property [2].

Second, about the representation of functions on $D/I$, where $I$ is an ideal of $D$: Let $f \in \mathrm{Int}(D)$. We say that $f$ is $I$-congruence preserving, if, for all $a, b \in D$,

$$a \equiv b \mod I \quad \Longrightarrow \quad f(a) \equiv f(b) \mod I.$$

In that case, $f$ induces a well-defined function on $D/I$ by $f(a + I) = f(a) + I$. Let $D$ be a Dedekind domain with finite residue fields. If $I$ is a power of a maximal ideal of $D$ (and only if $I$ is a power of a maximal ideal), every function on $D/I$ arises from an $I$-congruence preserving polynomial in $\mathrm{Int}(D)$ in this way. This was shown for $D = \mathbb{Z}$ by Skolem [7] (in the "if" direction) and Rédei and Szele [5, 6] (in the "only if" direction), and later generalized to Dedekind domains [4].

If $D$ is a Dedekind domain with finite residue fields, we will show that, given $r_0, \ldots, r_n \in D$ (distinct) and arbitrary $s_0, \ldots, s_n \in D$, and a finite set of powers $P^{k_P}$ of maximal ideals such that the $r_i$ are pairwise incongruent modulo each $P^{k_P}$, we can find a polynomial $f \in \mathrm{Int}(D)$ with $f(r_i) = s_i$ for $0 \leq i \leq n$ and such that

$$a \equiv b \mod P^{k_P} \quad \Longrightarrow \quad f(a) \equiv f(b) \mod P^{k_P}.$$

for each $P^{k_P}$, cf. Theorem 1.

A note on terminology: if $R$ is any ring and $f \in R[x]$ a polynomial, $f = \sum_k c_k x^k$ induces a function by substitution of elements of $R$ for the variable: $r \mapsto \sum_k c_k r^k$. A function $\varphi\colon R \to R$ thus arising from a polynomial $f \in R[x]$ is called a polynomial function on $R$.

When $R$ is an infinite domain, then the polynomial $f$ inducing a polynomial function is uniquely determined by its values on an infinite subset of $R$. Relying on this one-to-one correspondence between polynomials and polynomial functions, in the case where $R = K$ is an infinite field, we will not be as pedantic about the distinction between polynomials and polynomial functions as would be necessary if we were dealing with finite rings or rings with zero-divisors.

In what follows, when we talk about the function associated to an integer-valued polynomial $f \in \mathrm{Int}(D)$, we always mean the function $f\colon D \to D$ (as opposed to $f\colon K \to K$).

## 2 Notation and Definitions

We let $\mathbb{N}$ denote the positive integers (natural numbers) and $\mathbb{N}_0$ the non-negative integers. We use "additive" terminology for Lipschitz functions:

**Definition 1.** *Let $R$ be a commutative ring, $f\colon R \to R$ a function, $I$ an ideal of $R$, and $n \in \mathbb{N}_0$. We say that $f$ is $I$-adically $n$-Lipschitz if, for all $m \in \mathbb{N}$ and all $a, b \in R$*

$$a \equiv b \mod I^{m+n} \quad \Longrightarrow \quad f(a) \equiv f(b) \mod I^m$$

*When $D$ is a domain, $g \in \mathrm{Int}(D)$, and $I$ an ideal of $D$, we will say that $g$ is $I$-adically $n$-Lipschitz if the associated function $g\colon D \to D$ is $I$-adically $n$-Lipschitz.*

We summarize some elementary consequences of this definition.

*Remark 1.* Let $R$ be a commutative ring, $f\colon R \to R$ a function, and $I$ an ideal of $R$.

1. $I$-adically $n$-Lipschitz implies $I$-adically $N$-Lipschitz for all $N \geq n$.
2. If $f\colon R \to R$ is a function induced by a polynomial in $R[x]$ by substitution of the variable, then $f$ is $I$-adically 0-Lipschitz for all ideals $I$ of $R$.
3. For fixed $I$ and $n$, the set of $I$-adically $n$-Lipschitz functions on $R$ is closed under addition, subtraction and multiplication and, therefore, forms a subring of the set of all functions $R^R$.
4. If $D$ is a domain, $I$ an ideal of $D$ and $n \in \mathbb{N}_0$, then the set of $g \in \mathrm{Int}(D)$ that are $I$-adically $n$-Lipschitz is a subring of $\mathrm{Int}(D)$.

In what follows, $D$ is always a Dedekind domain with quotient field $K$, and we always assume $D \neq K$. For such a Dedekind domain, we denote by $\mathrm{Spec}^1(D)$ the set prime ideals of height one, which coincides with the set of maximal ideals of $D$. For $P \in \mathrm{Spec}^1(D)$, we use $v_P$ to denote the normalized discrete valuation on $K$ associated with $P$; that is, for $d \in D \setminus \{0\}$, $v_P(d)$ is the maximal exponent $v$ such that $d \in P^v$, and, for an element of $K \setminus \{0\}$ expressed as a fraction $a/b$ with $a, b \in D \setminus \{0\}$, $v_P(a/b) = v_P(a) - v_P(b)$.

*Remark 2.* Let $D$ a Dedekind domain, $f \in \mathrm{Int}(D)$, and $P$ a maximal ideal of $D$. If we express $f$ as a fraction $f = g/d$ with $g \in D[x]$ and $d \in D \setminus \{0\}$, we see that $f$ is $P$-adically $v_P(d)$-Lipschitz. In particular, if $f \in D_P[x]$, then $f$ is $P$-adically 0-Lipschitz. More generally, if $f \in \mathrm{Int}(D)$ is expressed as a fraction $f = g/d$ with $g \in D_P[x]$ and $d \in D \setminus \{0\}$, then, also, $f$ is $P$-adically $v_P(d)$-Lipschitz.

Note that $v_P(d)$, in the above remark, is not necessarily the minimal $n$ for which $f$ is $P$-adically $n$-Lipschitz (not even if $d$ is relatively prime to the content of $g$). For instance, when $f$ is a product $f = f_1 \dots f_n$ with $f_i = g_i/d$, $g_i \in D[x]$, then the denominator of $f$ is $d^n$, but $f$ is $P$-adically $v_P(d)$-Lipschitz, not just $v_P(d^n)$-Lipschitz, by Remark 1 (3).

We use $\|I\|$ for the norm of an ideal $I$ of $D$, that is $\|I\| = |D/I|$.

## 3 *P*-adic Lipschitz Constants of Interpolating Integer-Valued Polynomials

We recall a Lemma from an earlier paper that we will need for the proof of Lemma 2.

**Lemma 1** **([3], [Lemma 6.1]).** *Let $v$ be a discrete valuation on a field $K$ and $R_v$ its valuation ring. Suppose $g = \sum_{k=0}^{n} d_k x^k$ in $K[x]$ splits over $K$ as*

$$g(x) = d_n(x - b_1) \dots (x - b_m)(x - c_1) \dots (x - c_l),$$

*where $v(b_i) < 0$ and $v(c_i) \geq 0$.*

*Let $\mu = \min_{0 \leq k \leq n} v(d_k)$ and set $g_+(x) = (x - c_1) \dots (x - c_l)$ then, for all $r \in R_v$,*

$$v\big(g(r)\big) = \mu + v\big(g_+(r)\big).$$

**Definition 2.** *For $q, m$ integers with $q > 1$ and $m \geq 0$ define*

$$L(q, m) := \frac{1 - q^m}{1 - q}$$

**Lemma 2.** *Let $D$ be a Dedekind domain with finite residue fields and $a_0$, $a_1$ distinct elements of $D$. For $P \in \mathrm{Spec}^1(D)$, let $m_P = v_P(a_1 - a_0)$.*

*For any finite set $\mathcal{F}$ of maximal ideals of $D$ there exists $f \in \mathrm{Int}(D)$ with $f(a_1) = 0$ and $f(a_0) = 1$, and such that $f$ is $P$-adically $L(\|P\|, m_P)$-Lipschitz for all $P \in \mathcal{F}$.*

*Proof.* By linear substitution we may assume, w.l.o.g., that $a_0 = 0$. Also, we assume w.l.o.g. that $\mathcal{F}$ contains the set

$$\mathcal{P} = \{P \in \mathrm{Spec}^1(D) \mid a_1 \in P\} = \{P \in \mathrm{Spec}^1(D) \mid m_P > 0\}.$$

The case $\mathcal{P} = \emptyset$ is trivial. Assume $\mathcal{P} \neq \emptyset$. We set $\mathcal{F}_0 = \{P \in \mathcal{F} \mid m_P = 0\}$; such that $\mathcal{F}$ is the disjoint union of $\mathcal{P}$ and $\mathcal{F}_0$.

We will construct a polynomial $g \in K[x]$ with $g(a_1) = 0$, such that for every essential valuation $v$ of $D$ and every $r \in D$, $v\big(g(r)\big) \geq v\big(g(0)\big)$; and then set $f(x) = g(x)/g(0)$.

Let $N = \max_{P \in \mathcal{P}} \|P\|^{m_P}$. Using the Chinese Remainder Theorem modulo $P^{m_P+1}$ for $P \in \mathcal{F}$, we produce a sequence $(b_i)_{i=1}^{N}$ in $D$ with the properties:

1. $b_1 = a_1$
2. For all $P \in \mathcal{F}$, the $b_i$ with $1 \leq i \leq \|P\|^{m_P}$ form a complete system of residues modulo $P^{m_P}$.
3. For all $P \in \mathcal{F}$, for all $i > \|P\|^{m_P}$, $b_i \equiv 1$ modulo $P^{m_P+1}$.

Note that no $b_i$ is in $P^{m_P+1}$ for any $P \in \mathcal{F}$, and, in particular, that no $b_i$ is in $P$ for any $P \in \mathcal{F}_0$.

Let $P \in \mathcal{P}$ and $1 \leq k \leq m_P$. For any given $r \in D$, the number of $b_i$ with $1 \leq i \leq \|P\|^{m_P}$ in the residue class $r + P^k$ is the same, namely,

$$\gamma_k(P) := \|P\|^{m_P - k}\,.$$

Note that, therefore, for all $P \in \mathcal{P}$ and $1 \leq k \leq m_P$,

$$\forall r \in D \quad \left|\{i \mid v_P(r - b_i) \geq k\}\right| \geq \gamma_k(P),$$

with equality holding for all $r \in D \setminus (1 + P)$ (and, actually, for all $r \in D$ in the case where $\|P\|^{m_P} = N$).

Let $\mathcal{Q} = \{Q \in \mathrm{Spec}^1(D) \setminus \mathcal{P} \mid \exists i \;\; b_i \in Q\}$ and for $Q \in \mathcal{Q}$ let $k_Q = \max_i v_Q(b_i)$. Note that $\mathcal{Q} \cap \mathcal{F} = \emptyset$.

Let $c \in D$ with $v_Q(c) = k_Q + 1$ for all $Q \in \mathcal{Q}$, and $c \equiv 1 \mod P^{m_P+1}$ for all $P \in \mathcal{F}$. Let $\mathcal{Q}' = \{Q \in \mathrm{Spec}^1(D) \mid v_Q(c) > 0\}$. Then $\mathcal{Q} \subseteq \mathcal{Q}'$ and $\mathcal{Q}' \cap \mathcal{F} = \emptyset$.

Let $c_1 = a_1$ and for $1 < i \leq N$ let $c_i = c^{-1} b_i$. Then, for every $P \in \mathrm{Spec}^1(D) \setminus \mathcal{Q}'$, and, in particular, for every $P \in \mathcal{F}$, $(c_i)_{i=1}^N$ is a sequence in $D_P$. Also, for every maximal ideal $Q$ of $D$ that is neither in $\mathcal{Q}'$ nor in $\mathcal{P}$, $v_P(c_i) = 0$ for all $i$.

We set

$$g(x) = \prod_{i=1}^{N} (x - c_i) = (x - a_1) \prod_{i=2}^{N} (x - c^{-1} b_i)$$

and show that for all essential valuations $v$ of $D$ and all $r \in D$, $v(g(r)) \geq v(g(0))$.

First, assume $P \in \mathcal{P}$. The sequence $(c_i)_{i=1}^N$ enjoys the same properties with respect to $PD_P$ that the sequence $(b_i)_{i=1}^N$ enjoys with respect to $P$, namely, those $c_i$ with $1 \leq i \leq \|P\|^{m_P}$ form a complete system of residues modulo $(PD_P)^{m_P}$ and $c_i \equiv 1$ modulo $(PD_P)^{m_P+1}$ for all $i > \|P\|^{m_P}$. Also, no $c_i$ is in $P^{m_P+1}$.

Consequently, for all $r \in D$, and $1 \leq k \leq m_P$

$$\left|\{i \mid v_P(r - c_i) \geq k\}\right| = \left|\{i \mid v_P(r - b_i) \geq k\}\right| \geq \gamma_k(P).$$

Let $\gamma_P := \sum_{k=1}^{m_P} \gamma_k(P)$. Then

$$v_P\big(g(r)\big) = \sum_{i=1}^{N} v_P(r - c_i) = \sum_{k=1}^{\infty} \left|\{i \mid v_P(r - c_i) \geq k\}\right| \geq$$

$$\geq \sum_{k=1}^{m_P} \left|\{i \mid v_P(r - c_i) \geq k\}\right| = \sum_{k=1}^{m_P} \left|\{i \mid v_P(r - b_i) \geq k\}\right| \geq \gamma_P,$$

while $v_P(g(0)) =$

$$= \sum_{k=1}^{\infty} \left|\{i \mid v_P(c_i) \geq k\}\right| = \sum_{k=1}^{m_P} \left|\{i \mid v_P(c_i) \geq k\}\right| = \sum_{k=1}^{m_P} \left|\{i \mid v_P(b_i) \geq k\}\right| = \gamma_P.$$

Now consider $Q \in \mathcal{Q}'$. Here $v_Q(c_1) = v_Q(a_1) = 0$ and, for all $i > 1$, $v_Q(c_i) < 0$. Let $d_k$ be the coefficient of $x^k$ in $g$ and $\mu = \min_k v_Q(d_k)$. Using Lemma 1, we see that for all $r \in D$,

$$v_Q\big(g(r)\big) = \mu + v_Q(r - a_1) \geq \ \mu \ = \mu + v_Q(a_1) = v_Q\big(g(0)\big).$$

For the remaining essential valuations $v$ of $D$, $v(c_i) = 0$ for all $i$, and, therefore, for all $r \in D$, $v\big(g(r)\big) = \sum_i v(r - c_i) \geq 0 = \sum_i v(c_i) = v\big(g(0)\big)$.

Now let $f(x) = g(x)/g(0)$. Then $f(a_1) = 0$, and $f(0) = 1$. Also, $f \in \mathrm{Int}(D)$, because for all $r \in D$ and every essential valuation $v$ of $D$, $v\big(g(r)\big) \geq v\big(g(0)\big)$ and therefore $v\big(f(r)\big) \geq 0$.

As for the Lipschitz properties: for those $P \in \mathrm{Spec}^1(D)$ for which $v_P(c) = 0$, and, in particular, for all $P \in \mathcal{F}$, $g$ is in $D_P[x]$. $f$ is, therefore, $P$-adically $v_P(g(0))$-Lipschitz for all $P \in \mathcal{F}$ by Remark 2.

For $P \in \mathcal{F}_0$, $v_P(g(0)) = 0$ and hence $f$ is $P$-adically 0-Lipschitz for all $P \in \mathcal{F}_0$.

For $P \in \mathcal{P}$,

$$v_P(g(0)) = \gamma_P = \sum_{k=1}^{m_P} \gamma_k(P) = \sum_{k=1}^{m_P} \|P\|^{m_P - k} = \sum_{j=0}^{m_P - 1} \|P\|^j = \frac{1 - \|P\|^{m_P}}{1 - \|P\|}.$$

$f$ is, therefore, $P$-adically $l_P$-Lipschitz for all $P \in \mathcal{F}$, for the values of $l_P$ stated in the Lemma. □

**Corollary 1.** *Let $D$ be a Dedekind domain with finite residue fields, $\mathcal{F}$ a finite set of maximal ideals, and $a_0, \ldots, a_n$ distinct elements of $D$. For each $P \in \mathcal{F}$, let $m_P \geq \max_{1 \leq i \leq n} v_P(a_i - a_0)$.*

*Then there exists $f \in \mathrm{Int}(D)$ with $f(a_i) = 0$ for $1 \leq i \leq n$, and $f(a_0) = 1$, and such that $f$ is $P$-adically $L(\|P\|, m_P)$-Lipschitz for all $P \in \mathcal{F}$.*

*Proof.* For each $1 \leq i \leq n$ and $P \in \mathcal{F}$, let $m_P(i) = v_P(a_i - a_0)$ and $l_P(i) = L(\|P\|, m_P(i))$. Let $f_i \in \mathrm{Int}(D)$ with $f_i(a_i) = 0$ and $f_i(a_0) = 1$ and such that $f_i$ is $P$-adically $L(\|P\|, m_P(i))$-Lipschitz for each $P \in \mathcal{F}$. Such an $f_i$ exists by Lemma 2, and it is $P$-adically $L(\|P\|, m_P)$-Lipschitz, because $m_P(i) \leq m_P$, and $L(q, m)$ is an increasing function in $m$ for fixed $q$, and $l$-Lipschitz implies $l'$-Lipschitz for all for all $l' \geq l$. Now set $f(x) = \prod_{i=1}^{n} f_i(x)$. □

## 4 Interpolation by Congruence-Preserving Integer-Valued Polynomials

**Lemma 3.** *Let $D$ be a Dedekind domain with finite residue fields and $r_0, \ldots, r_n$ distinct elements of $D$.*

*Let $\mathcal{F}$ be a finite set of maximal ideals of $D$. For each $P \in \mathcal{F}$, let $k_P \in \mathbb{N}$ such that the $r_i$ are pairwise incongruent modulo $P^{k_P}$ and $l_P = L(\|P\|, k_P - 1)$ as in Definition 2.*

*Then there exists $f \in \mathrm{Int}(D)$ such that*

1. *$f(r_0) = 1$ and, for $1 \le i \le n$, $f(r_i) = 0$;*
2. *for each $P \in \mathcal{F}$, for every $r \in D \setminus (r_0 + P^{k_P})$, $f(r) \equiv 0 \mod P^{k_P}$;*
3. *for each $P \in \mathcal{F}$, for every $r \in r_0 + P^{k_P + l_P}$, $f(r) \equiv 1 \mod P^{k_P}$.*

*Proof.* We will first construct a polynomial $f_P \in \mathrm{Int}(D)$ for each $P \in \mathcal{F}$, in several steps. Fix $P \in \mathcal{F}$.

Extend $r_0, \ldots, r_n$ to a complete set of residues $r_0, \ldots, r_{\|P\|^{k_P}-1}$ modulo $P^{k_P}$, such that for all $i > n$ and all $Q \in \mathcal{F} \setminus \{P\}$, $r_i \equiv r_1$ modulo $Q^{k_Q+1}$.

Let $C$ be a finite subset of $\prod_{Q \in \mathcal{F}} Q^{k_Q}$ containing a complete system of residues of the residue classes of $P^{k_P+l_P}$ contained in $P^{k_P}$, and with $0 \in C$.

For each $1 \le i < \|P\|^{k_P}$, and $c \in C$, let $f_{ic}$ a polynomial in $\mathrm{Int}(D)$ with $f_{ic}(r_0) = 1$, $f_{ic}(r_i + c) = 0$, and $Q$-adically $l_Q$-Lipschitz for all $Q \in \mathcal{F}$, such as we know to exist by Lemma 2 and its Corollary. Set $f_i = \prod_{c \in C} f_{ic}$. Then $f_i(r_i) = 0$ and $f_i(r_0) = 1$. Also, since $\bigcup_{c \in C} r_i + c + P^{k_P+l_P} = r_i + P^{k_P}$ and $f_i(r_i + c) = 0$ for all $c \in C$, the $P$-adic Lipschitz property implies that for all $r \in r_i + P^{k_P}$, $f_i(r) \equiv 0$ modulo $P^{k_P}$. Likewise, the Lipschitz properties of the polynomials $f_{ic}$ imply for all $Q \in \mathcal{F}$ that $f_i(r) \equiv 1$ modulo $Q^{k_Q}$ for all $r \in r_0 + Q^{k_Q+l_Q}$.

Let $f_P = \prod_{i=1}^{\|P\|^{k_P}-1} f_i$. Then $f_P$ satisfies

1. $f_P(r_0) = 1$ and $f_P(r_j) = 0$ for $1 \le j \le n$;
2. $f_P(r) \equiv 0$ modulo $P^{k_P}$ for $r \in D \setminus (r_0 + P^{k_P})$;
3. for all $Q \in \mathcal{F}$, for all $r \in r_0 + Q^{k_Q+l_Q}$, $f_P(r) \equiv 1$ modulo $Q^{k_Q}$.

Having constructed $f_P$ for each $P \in \mathcal{F}$, we set $f = \prod_{P \in \mathcal{F}} f_P$, and $f$ has the desired properties. □

**Theorem 1.** *Let $D$ be a Dedekind domain with finite residue fields, $r_0, \ldots, r_n$ distinct elements of $D$ and $s_0, \ldots, s_n$ arbitrary elements of $D$.*

*Let $\mathcal{F}$ be a finite set of maximal ideals of $D$. For each $P \in \mathcal{F}$ let $k_P \in \mathbb{N}$ such that the $r_i$ are pairwise incongruent modulo $P^{k_P}$.*

*Then there exists $f \in \mathrm{Int}(D)$ such that*

1. *for $0 \le i \le n$,*

$$f(r_i) = s_i$$

2. *for all $P \in \mathcal{F}$, for all $a, b \in D$,*

$$a \equiv b \mod P^{k_P} \implies f(a) \equiv f(b) \mod P^{k_P}.$$

3. *for all $P \in \mathcal{F}$, for all $r \in D$ with $(r + P^{k_P}) \cap \{r_0, \ldots, r_n\} = \emptyset$,*

$$f(r) \equiv 0 \mod P^{k_P}.$$

*Proof.* It suffices to show, for each index $i$, the existence of a polynomial $h_i \in \mathrm{Int}(D)$ such that

1. $h_i(r_i) = 1$ and $h_i(r_j) = 0$ for $j \neq i$,
2. for all $P \in \mathcal{F}$, for all $r \in D \setminus (r_i + P^{k_P})$, $h_i(r) \equiv 0 \mod P^{k_P}$, and
3. for all $P \in \mathcal{F}$, for all $r \in r_i + P^{k_P}$, $h_i(r) \equiv 1 \mod P^{k_P}$,

because, then, the polynomial $f = \sum_{i=0}^{n} s_i h_i$ does the job.

W.l.o.g., assume $i = 0$. We construct $h_0$ with the help of Lemma 3:

For each $Q \in \mathcal{F}$, let $l_Q = L(\|Q\|, k_Q - 1)$.

Let $C$ be a subset of $\prod_{Q \in \mathcal{F}} Q^{k_Q}$ containing, for each $Q \in \mathcal{F}$, a complete system of residues of the residue classes of $Q^{k_Q + l_Q}$ contained in $Q^{k_Q}$, and with $0 \in C$.

For each $d \in C$, $r_0 + d, r_1, \ldots, r_n$ satisfy the premises of Lemma 3. Accordingly, let $f_d \in \mathrm{Int}(D)$ such that

1. $f_d(r_0 + d) = 1$ and, for $1 \leq i \leq n$, $f_d(r_i) = 0$;
2. for each $P \in \mathcal{F}$, for every $r \in D \setminus (r_0 + d + P^{k_P})$, $f_d(r) \equiv 0 \mod P^{k_P}$;
3. for each $P \in \mathcal{F}$, for every $r \in r_0 + d + P^{k_P + l_P}$, $f_d(r) \equiv 1 \mod P^{k_P}$.

and set $g_d = 1 - f_d$.

Since $r_0 + d + P^{k_P} = r_0 + P^{k_P}$ for all $P \in \mathcal{F}$ and $d \in C$, each $g_d$ satisfies

1. $g_d(r_0 + d) = 0$ and, for $1 \leq i \leq n$, $g_d(r_i) = 1$;
2. for each $P \in \mathcal{F}$, for every $r \in D \setminus (r_0 + P^{k_P})$, $g_d(r) \equiv 1 \mod P^{k_P}$;
3. for each $P \in \mathcal{F}$, for every $r \in r_0 + d + P^{k_P + l_P}$, $g_d(r) \equiv 0 \mod P^{k_P}$.

Now, set $g = \prod_{d \in C} g_d$.

Considering that, for all $P \in \mathcal{F}$, $\bigcup_{d \in C} r_0 + d + P^{k_P + l_P} = r_0 + P^{k_P}$, we see that the polynomial $g = \prod_{d \in C} g_d$ satisfies

1. $g(r_0) = 0$ and, for $1 \leq i \leq n$, $g(r_i) = 1$;
2. for each $P \in \mathcal{F}$, for every $r \in D \setminus (r_0 + P^{k_P})$, $g(r) \equiv 1 \mod P^{k_P}$;
3. for each $P \in \mathcal{F}$, for every $r \in r_0 + P^{k_P}$, $g(r) \equiv 0 \mod P^{k_P}$.

Finally, we let $h_0 = 1 - g$. □

Recall that a function $f : D \to D$ satisfying

$$a \equiv b \mod I \implies f(a) \equiv f(b) \mod I,$$

where $D$ is a commutative ring and $I$ an ideal of $D$, is called *$I$-congruence preserving*. In this case, $f$ defines a function $\bar{f}_I\colon D/I \to D/I$ by

$$\bar{f}_I(a+I) = f(a) + I.$$

We call $\bar{f}_I$ the function induced by $f$ on $D/I$.

We can now sharpen Theorem 1 some more to obtain a completely general form of simultaneous interpolation and $P$-adic approximation. Given arbitrary arguments and values in $D$ and, for finitely many maximal ideals, a function on the residue class ring modulo a power of the ideal, we can find a polynomial in $\mathrm{Int}(D)$ that interpolates, while simultaneously realizing the given functions on the residue class rings, provided that the requirements are not obviously contradictory.

**Theorem 2.** *Let $D$ be a Dedekind domain with finite residue fields, $r_0, \ldots, r_n$ distinct elements of $D$ and $s_0, \ldots, s_n$ arbitrary elements of $D$.*

*Let $\mathcal{F}$ be a finite set of maximal ideals of $D$. For each $P \in \mathcal{F}$ let $k_P \in \mathbb{N}$ a natural number, and*

$$\varphi_P\colon D/P^{k_P} \to D/P^{k_P}$$

*a function.*

*If, for all $P \in \mathcal{F}$ and for all $0 \le i \le n$,*

$$s_i \in \varphi_P(r_i + P^{k_P})$$

*then there exists $f \in \mathrm{Int}(D)$ such that*

1. *for $0 \le i \le n$,*
$$f(r_i) = s_i$$
2. *for all $P \in \mathcal{F}$, for all $a, b \in D$,*
$$a \equiv b \mod P^{k_P} \quad \Longrightarrow \quad f(a) \equiv f(b) \mod P^{k_P}$$
*and the function $\bar{f}\colon D/P^{k_P} \to D/P^{k_P}$ defined by $\bar{f}(a + P^{k_P}) = f(a) + P^{k_P}$ equals $\varphi_P$.*

*Proof.* We may, w.l.o.g., assume that for all $P \in \mathcal{F}$ the arguments $r_i$ are pairwise incongruent modulo $P^{k_P}$. If they are not, we replace each $k_P$ by a possibly larger $l_P$ such that the $r_i$ are incongruent modulo $P^{l_P}$, and replace each $\varphi_P$ by a function

$$\psi_P\colon D/P^{l_P} \to D/P^{l_P}$$

which preserves congruences modulo $P^{k_P} + P^{l_P}$, induces $\varphi_P$ on $D/P^{k_P}$ and satisfies $\psi_P(r_i + P^{l_P}) = s_i + P^{l_P}$.

Now assume that the $r_i$ are pairwise incongruent modulo $P^{k_P}$. We apply Theorem 1 to produce $g \in \mathrm{Int}(D)$ such that

1. for $0 \le i \le n$, $g(r_i) = s_i$
2. for all $P \in \mathcal{F}$, $g$ is $P^{k_P}$-congruence preserving
3. for all $P \in \mathcal{F}$, for all $r \in D$ such that $(r + P^{k_P})$ contains no $r_i$, we have $g(r) \equiv 0 \mod P^{k_P}$.

Let $\mathcal{F}'$ be the subset of $\mathcal{F}$ consisting of those $P$ for which $r_0, \ldots, r_n$ do not form a complete system of residues modulo $P^{k_P}$. For all $P \in \mathcal{F} \setminus \mathcal{F}'$, $g$ already induces $\varphi_P$ on $D/P^{k_P}$. We now modify $g$ by adding a polynomial $f_Q \in \mathrm{Int}(D)$ for each $Q \in \mathcal{F}'$ to the effect that $\varphi_Q$ is induced on $D/Q^{k_Q}$, without affecting the properties 1 and 2 of $g$ and without changing the function induced on $D/P^{k_P}$ for any $P \in \mathcal{F} \setminus \{Q\}$.

Fix $Q \in \mathcal{F}'$. To construct $f_Q$, first extend $r_0, \ldots, r_n$ to a complete system of residues $r_0, \ldots, r_n, r_{n+1}, \ldots, r_{q-1}$ modulo $Q^{k_Q}$.

Then, for each $i$ with $n < i < q$, use Theorem 1 to find $h_i \in \mathrm{Int}(D)$ which is $Q^{k_Q}$-congruence preserving and satisfies $h_i(r_i) = 1$ and $h_i(r_j) = 0$ for $0 \le j < q$ with $j \ne i$.

Also, for $n < i < q$, let $b_i \in \varphi_Q(r_i + Q^{k_Q})$ such that $b_i \equiv 0 \mod P^{k_P}$ for all $P \in \mathcal{F} \setminus \{Q\}$. Then, set

$$f_Q = \sum_{i=n+1}^{q-1} b_i h_i.$$

Having thus defined $f_Q$ for each $Q \in \mathcal{F}'$, finally, set

$$f = g + \sum_{Q \in \mathcal{F}'} f_Q.$$

□

## References


1. Cahen, P.J., Chabert, J.L.: Integer-Valued Polynomials. Mathematical Surveys and Monographs, vol. 48. American Mathematical Society, Providence, RI (1997)
2. Cahen, P.J., Chabert, J.L., Frisch, S.: Interpolation domains. J. Algebra **225**(2), 794–803 (2000). http://dx.doi.org/10.1006/jabr.1999.8151
3. Frisch, S.: Interpolation by integer-valued polynomials. J. Algebra **211**(2), 562–577 (1999). http://dx.doi.org/10.1006/jabr.1998.7741
4. Frisch, S.: Polynomial functions on finite commutative rings. In: Dobbs, D.E., Fontana, M., Kabbaj, S.E. (eds.) Advances in Commutative Ring Theory (Fez, 1997). Lecture Notes in Pure and Applied Mathematics, vol. 205, pp. 323–336. Dekker, New York (1999)
5. Rédei, L., Szele, T.: Algebraischzahlentheoretische Betrachtungen über Ringe. I. Acta Math. **79**, 291–320 (1947). https://doi.org/10.1007/BF02404701
6. Rédei, L., Szele, T.: Algebraisch-zahlentheoretische Betrachtungen über Ringe. II. Acta Math. **82**, 209–241 (1950). https://doi.org/10.1007/BF02398278
7. Skolem, T.: Einige Sätze über Polynome. Avh. Norske Vid. Akad. Oslo. I. **1940**(4), 16 (1940)

# Length Functions over Prüfer Domains

**Gabriele Fusacchia and Luigi Salce**

**Abstract** The first part of this paper is mostly devoted to survey results by Northcott-Reufel on length functions over commutative domains, specifically over valuation domains and 1-dimensional Prüfer domains of finite character. In the second part we present new results leading to the characterization of length functions over arbitrary Prüfer domains of finite character.

**Keywords** Prüfer domains · Valuation domains · Length functions

**2000 Mathematics Subject Classification** Primary: 13F05, 13F30, 13G05. Secondary: 13C60

## 1 Introduction

An intriguing feature in mathematical research arises when papers dating from the same time and dealing with completely different arguments are found, after many years, to have a strict connection, when new researches provide a unifying point of view or unforeseeable relationships. An example of this situation is offered by two papers on different subjects that appeared in 1965.

The first paper by Northcott and Reufel [16], which is the source of the present paper, dealt with suitable generalizations of the notion of the classical composition length for modules over a commutative ring, called *length functions*. They were able

Research supported by the Department of Mathematics "Tullio Levi-Civita" of the University of Padova.

G. Fusacchia · L. Salce (✉)
Dipartimento di Matematica "Tullio Levi-Civita", Università di Padova,
Via Trieste 63, 35121 Padua, Italy
e-mail: salce@math.unipd.it

G. Fusacchia
e-mail: gabfus@gmail.com

 
A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_11

to characterize all length functions over valuation domains and over 1-dimensional Prüfer domains of finite character. The latter paper, by Adler, Konheim and McAndrew [1], introduced and investigated the notion of topological entropy and, at the very end, gave a sketch definition of *algebraic entropy* for endomorphisms of Abelian groups. At that time it was impossible to realize, or even suspect, a connection between the two papers [1, 16].

After almost half a century, the generalization of the algebraic entropy from Abelian groups (in the meanwhile deeply investigated in [6] and elsewhere) to the more general setting of modules over arbitrary rings presented in [18] used the notion of sub-additive invariant as a crucial tool for the definition of entropy. Furthermore, important theorems for this entropy were proved in [17] when the sub-additive invariant is, indeed, a length function, thus establishing a strict connection between length functions and algebraic entropy.

Length functions have been investigated in the late '60's by Peter Vámos in [20, 21], who obtained their complete classification over Noetherian commutative rings. In recent years the renewed interest in length functions came as a sub-product of the investigation of the algebraic entropy for endomorphisms of modules over arbitrary rings (the second author is indebted to Peter Vámos for addressing him to length functions as a privileged tool in this investigation). However, in the authors' opinion, length functions are a subject which deserve independent interest, especially for people working in commutative algebra.

This opinion motivates the present paper, whose goal is to investigate length functions over Prüfer domains; we must restrict to domains of finite character, since our actual knowledge is confined to this class of domains. Our starting point is the following characterization, due to Northcott and Reufel [16, Theorem 14], of length functions over 1-dimensional Prüfer domains of finite character; note that these domains are, in particular, $h$-local, i.e., beside finite character, they have the property that every non-zero prime ideal is contained in a unique maximal ideal.

**Theorem 1.1.** (Northcott-Reufel) *Let $R$ be a 1-dimensional Prüfer domain of finite character and $L : Mod(R) \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ a length function such that $L(R) = \infty$. Then there exists a unique family $\{L^{(P)}\}_{P \in Max(R)}$ of local length functions for $R$ such that $L^{(P)}(R_P) = \infty$, with the property that $L(M) = \sum_{P \in Max(R)} L^{(P)}(M_P)$ for every $R$-module $M$. The length functions $L^{(P)}$ coincide with the localizations $L_P$ of $L$ for each $P \in Max(R)$.*

For the notions of local length function and of localization of a length function see the following Section 2, where we provide the general information, mostly borrowed from [16], concerning length functions over commutative rings. The hypothesis that $L(R) = \infty$ in Theorem 1.1 is not restrictive, since length functions satisfying $L(R) < \infty$ are easily classifiable, as we will see in Section 2.

In Section 3 we survey the characterization obtained by Northcott and Reufel in [16] for length functions over valuation domains; it is worth recalling that this classification has been obtained using a different multiplicative approach by Zanardo in [24]. In Section 4 we collect some properties of Prüfer domains used in the sequel of the paper and introduce the notion of their meet-spectrum.

The extension of Theorem 1.1 from 1-dimensional to arbitrary Prüfer domains of finite character, where the structure of the prime spectrum is more complicated, presents problems for representing a length function as sum of its localizations at maximal ideals, as well as for the uniqueness of its representation. These problems are solved in Section 5 where, after an example which makes evident the problems mentioned above and revisiting unpublished notes by the first author [11], we present the most relevant new results leading to the characterization of length functions over semilocal Prüfer domains. These results are based on the ad hoc notions of compatible families of local length functions and of their balanced sum.

Once this step is accomplished, its transfer to general Prüfer domains of finite character follows easily in the final Section 6, where we present the main theorem of the paper (Theorem 6.2). Theorem 1.1, as well as its extension to arbitrary $h$-local domains, are derived as simple corollaries of the main theorem.

For completeness of information on what is at our knowledge on length functions, we must mention that recently Virili [22] surveyed Vámos' results on length functions over Noetherian commutative rings, retracing complete proofs different in many parts from the original ones. The main goal of Virili's survey was the description of algebraic entropies induced by these length functions. A further investigation by Virili [23] concerns length functions on Grothendieck categories.

Finally, very recently Spirito [19] studied decompositions of length functions over integral domains as sums of length functions constructed from overrings. He found standard representations when the integral domain admits a Jaffard family of flat overrings, and when it is a Prüfer domain such that every ideal has only finitely many minimal primes. His paper has some overlaps with the present paper.

## 2 Generalities on Length Functions

The starting point which originated the notion of length function is the classical notion of composition length: given a commutative ring $R$ and an $R$-module $M$, its *composition length* $l(M)$ is the maximum of the lengths of chains of submodules $0 < M_1 < M_2 < \cdots < M_n = M$ such that each factor $M_{i+1}/M_i$ $(0 \leq i \leq n-1)$ is a simple module, if such a maximum exists, otherwise it is $\infty$. It is clear that $l(0) = 0$ and that, given a short exact sequence of $R$-modules $0 \to M' \to M \to M'' \to 0$, $l(M) = l(M') + l(M'')$; furthermore, it is easy to prove that, for each module $M$, $l(M)$ is the supremum of the composition lengths of its finitely generated submodules.

The idea behind the notion of length function, introduced by Northcott and Reufel [16] in order to generalize the composition length, is to measure the size of modules by associating with each module a "quantity" consisting either of a non-negative real number or $\infty$. They axiomatized this notion imposing the three conditions satisfied by the composition length recalled above.

Let $R$ be a commutative unitary ring and $Mod(R)$ the category of $R$-modules. We denote by $\mathbb{R}^*$ the totally ordered set of the non-negative real numbers with the symbol $\infty$ adjoint, which is strictly bigger than any real number: $\mathbb{R}^* = \mathbb{R}_{\geq 0} \cup \{\infty\}$;

obviously $\infty + \infty = \infty + r = \infty$ for each $r \in \mathbb{R}_{\geq 0}$. A *length function* over $Mod(R)$ (or simply over $R$) is a map $L : Mod(R) \to \mathbb{R}^*$ which satisfies the following three conditions:

(i) $L(0) = 0$;

(ii) (additivity) $L(M) = L(M') + L(M'')$ if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence in $Mod(R)$;

(iii) (upper continuity) for every $M \in Mod(R)$, $L(M) = sup_X L(X)$, where $X$ ranges over the set of the finitely generated submodules of $M$.

The first two properties imply that a length function is an invariant, i.e., it assigns the same value to isomorphic modules. Immediate consequences of (ii) are that $M' \leq M$ implies $L(M) = L(M') + L(M/M')$ and that, if $I \leq J$ are ideals of $R$, then $L(R/J) \leq L(R/I)$.

The set of length functions over $R$ may be endowed with a partial order, by saying the $L \leq L'$ if $L(M) \leq L'(M)$ for every $M \in Mod(R)$.

By a *local length function* for $R$ we mean a length function over $Mod(R_P)$, for some $P \in Max(R)$, the maximal spectrum of $R$, where $R_P$ denotes, as usual, the localization of $R$ at $P$. A length function $L$ over $R$ is *discrete* if its finite values form a discrete subset of $\mathbb{R}^*$, necessarily order-isomorphic to $\mathbb{N}$, and it is *faithful* if $L(M) = 0$ implies $M = 0$.

**Example 2.1.** The most common examples of length functions are:

- the classical *composition length* of a module; it is discrete and faithful;

- if $R$ is an integral domain, the *rank* of a module $M$, defined as $rk(M) = dim_K(M \otimes_R K)$, where $K$ is the field of fractions of $R$; it is discrete but not faithful, unless $R$ is a field;

- if $R = \mathbb{Z}$, for every Abelian group $G$ let $L(G) = log|G|$ (obviously setting $L(G) = \infty$ if $G$ is infinite); this is a discrete and faithful length function;

- the *trivial* length functions $L_0$ and $L_\infty$ always exist and are defined as follows: $L_0(M) = 0$ for all $M \in Mod(R)$, and $L_\infty(M) = \infty$ for all $0 \neq M \in Mod(R)$.

The next result says that every length function is completely determined by its action on cyclic modules.

**Proposition 2.2.** ([16, Lemma 1]) *Two length functions $L, L'$ on a commutative ring $R$ coincide if and only $L(R/I) = L'(R/I)$ for every ideal $I$ of $R$.*

*Proof.* The necessity is trivial. The sufficiency depends on the fact that every finitely generated module is the union of a finite chain of submodules with cyclic quotients of two consecutive submodules, to which we can apply the additivity of $L$, and on upper continuity. □

A relevant consequence of Proposition 2.2 is that completion properties of quotients of $R$ in the $R$-topology have no impact on length functions; for instance, a maximal valuation domain and an incomplete non-almost maximal valuation domain with the same value group admit exactly the same length functions, as will be clear in the next section.

The next result shows the relevance of prime ideals in connection with length functions.

**Proposition 2.3.** *Let $P$ be a prime ideal of the commutative ring $R$ and $L$ a length function over $R$ such that $L(R/P) < \infty$. Then $L(R/I) = 0$ for every ideal $I$ strictly containing $P$.*

*Proof.* By additivity, $L(R/P) = L(R/I) + L(I/P)$, hence $L(R/P) \geq L(I/P)$. Choosing $x \in I \setminus P$ provides an embedding $R/P \to I/P$ through the multiplication by $x$. This gives $L(R/P) \leq L(I/P)$, therefore $L(R/P) = L(I/P)$ and consequently $L(R/I) = 0$. □

Since we will focus on modules over integral domains, the next consequence of Proposition 2.3 is crucial. It tells us that a length function on a domain $R$ taking positive finite value on $R$ coincides with the rank function, up to a positive real multiple.

**Corollary 2.4.** ([16, Theorem 2]) *Let $L$ be a length function over an integral domain $R$ satisfying $0 < L(R) < \infty$. Then, for every module $M \in Mod(R)$, $L(M) = L(R) \cdot rk(M)$.*

*Proof.* As $rk(R) = 1$, the equality $L(M) = L(R) \cdot rk(M)$ holds for $M = R$. If $0 < I < R$, then $rk(R/I) = 0$, so, in view of Proposition 2.2, it is enough to prove that $L(R/I) = 0$. But this immediately follows from Proposition 2.3, since 0 is a prime ideal. □

If a length function $L$ satisfies $L(R) = 0$, then obviously it coincides with the trivial length function $L_0$. So, by Corollary 2.4, the investigation of length functions over an integral domain $R$ may be confined to those $L$ such that $L(R) = \infty$.

Localizations at multiplicatively closed subsets of the commutative ring $R$ and length functions have strict relationships. First, any length function $L$ on $R$ determines a multiplicatively closed set $S_L$, defined as

$$S_L = \{a \in R : L(R/aR) = 0\}.$$

In fact, it is clear that $1 \in S_L$ and, if $a, b \in S_L$, then $L(R/aR) = 0 = L(R/bR)$, hence from the exact sequence

$$0 \to aR/abR \to R/abR \to R/aR \to 0$$

we deduce that $L(R/abR) = L(aR/abR) + L(R/aR)$. But $aR/abR$ is an epic image of $R/bR$, hence $L(aR/abR) = 0$, consequently $L(R/abR) = 0$ and $ab \in S_L$.

Recall that the $S_L$-torsion submodule of an $R$-module $M$ consists of those elements $x \in M$ such that $ax = 0$ for some $a \in S_L$.

**Lemma 2.5.** ([16, Lemmas 3 and 4]) *Let $L$ be a length function over the commutative ring $R$. Let $M \in Mod(R)$ and $T$ its $S_L$-torsion submodule. Then $L(M) = L(M/T) = L(M_{S_L})$.*

*Proof.* If $R/I$ is a cyclic $S_L$-torsion module, then $I$ contains an element $a \in S_L$, so that $L(R/I) \leq L(R/aR) = 0$. It follows that $L(T) = 0$ and, by additivity, $L(M) = L(M/T)$. Since $M/T$ embeds into $M_{S_L}$ with $S_L$-torsion cokernel, the additivity of $L$ also implies that $L(M/T) = L(M_{S_L})$. □

On the other hand, starting with a multiplicatively closed subset $S$ of $R$, a length function $L$ over $R$ is said to be *localized at S* if it satisfies $L(M) = L(M_S)$ for every $R$-module $M$, that is, if the length of each $R$-module is the same as the length of its localization at $S$, so that $L$ can be viewed as a length function on $Mod(R_S)$. The next result tells in particular that a length function $L$ is always localized at $S_L$.

**Proposition 2.6.** *Let L be a length function over the commutative ring R, and $S \subseteq T$ two multiplicatively closed subsets of R. Then:*
(1) *if L is localized at T, then it is localized at S;*
(2) *L is localized at S if and only if $S \subseteq S_L$.*

*Proof.* (1) Since $S \subseteq T$, for every module $M$ we have $M_T = (M_S)_T$. Then $L(M_S) = L((M_S)_T)$, since $L$ is localized at $T$, therefore $L(M_S) = L(M_T) = L(M)$.

(2) The same argument as in point (1) proves the sufficiency, once we have shown that $L$ is localized at $S_L$; this follows by Lemma 2.5. For the necessity, if $S$ is not contained in $S_L$, there exists $s \in S$ such that $L(R/sR) > 0$. On the other hand, $L(R_S/sR_S) = L(0) = 0$, hence $L$ cannot be localized at $S$. □

We describe some methods to obtain new length functions from pre-assigned ones. We leave as an exercise for the reader to check the details of the straightforward proofs. It is worthwhile to remark that the first example, with the two lemmas and the proposition following it, provide a crucial tool in the development of the paper, notably, in Definition 5.6 and in the proofs of the main Theorems 5.7 and 6.2.

**Example 2.7.** (Difference) Let $L \geq L'$ be two length functions over $Mod(R)$ and denote by $\mathcal{F}G(R)$ the class of finitely generated $R$-modules. The function $L - L' : \mathcal{F}G(R) \to \mathbb{R}^*$ defined by setting

$$(L - L')(F) = \begin{cases} L(F) - L'(F) & \text{if } L(F) < \infty \\ \infty & \text{if } L(F) = \infty \end{cases}$$

is additive on short exact sequences of finitely generated modules, as it is easy to check. Extend this function to the whole category $Mod(R)$ by setting, for every $R$-module $M$:

$$(L - L')(M) = sup\{(L - L')(F) | F \in \mathcal{F}G(R), F \leq M\}.$$

Then $L - L' : Mod(R) \to \mathbb{R}^*$ is upper continuous by definition, but in general it is not a length function, since it is not additive. As a counter-example, take $R = K(+)V$, where $K$ is a field, $V$ an infinite dimensional $K$-vector space, and $(+)$ the idealization. Taking $L = dim_K$ it is easy to see that the function $L - L$ as defined above is not additive on the exact sequence $0 \to V \to R \to K \to 0$ (we thank the referee for suggesting us such a counter-example).

We look for properties of $L$ and $L'$ ensuring that $L - L'$ is additive, hence a length function.

**Lemma 2.8.** *Let $L$ and $L'$ be two length functions over $Mod(R)$ satisfying the inequality $L \geq L'$. If $L(A) < \infty$ for a module $A$, then $(L - L')(A) = L(A) - L'(A)$.*

*Proof.* All the involved quantities are finite, so we must equivalently prove that $(L - L')(A) + L'(A) = L(A)$, that is, $sup_{F \leq A}(L - L')(F) + sup_{F' \leq A} L'(F') = sup_{F'' \leq A} L(F'')$, where $F, F', F''$ are finitely generated modules. If $F'' \leq A$, then $L(F'') = (L - L')(F'') + L'(F'')$, hence $L(A) \leq (L - L')(A) + L'(A)$. Conversely, $(L - L')(F) + L'(F') \leq (L - L')(F + F') + L'(F' + F) = L(F + F')$, hence the converse inequality $(L - L')(A) + L'(A) \leq L(A)$ also holds. □

**Lemma 2.9.** *Let $L$ and $L'$ be two length functions over $Mod(R)$ satisfying the inequality $L \geq L'$. If $0 \to A \to B \to C \to 0$ is an exact sequence such that $B$ is finitely generated and $L(A) < \infty$, then $L - L'$ is exact on it.*

*Proof.* If $L(B) < \infty$, then $(L - L')(B) = L(B) - L'(B) = L(A) + L(C) - L'(A) - L'(C) = L(A) - L'(A) + (L - L')(C)$. But $(L - L')(A) = L(A) - L'(A)$, by Lemma 2.8, so the claim follows. If $L(B) = \infty$, then necessarily $L(C) = \infty$, hence $(L - L')(B) = \infty = (L - L')(C)$, thus additivity follows also in this case. □

If in the preceding lemma we drop the hypothesis that $L(A) < \infty$, the claim is no more true, as the counter-example above shows. The next result provides a sufficient condition in order that the difference of two length functions is again a length function.

**Proposition 2.10.** *Let $L$ and $L'$ be two length functions over $Mod(R)$ satisfying the inequality $L \geq L'$. If for every submodule $A$ of a finitely generated $R$-module the equality $L(A) = \infty$ implies $(L - L')(A) = \infty$, then $L - L'$ is a length function over $Mod(R)$*

*Proof.* Since $L - L'$ is upper continuous by definition, it is enough to prove that it is additive. It is immediate to check that $L - L'$ is additive on short exact sequences $0 \to A \to B \to C \to 0$, with $A, B, C$ finitely generated. If it is additive on $0 \to A \to B \to C \to 0$ when only $B$, and consequently $C$, are finitely generated, arguing as in the proof of Lemma 3.14 in [22], one can show that $L - L'$ is additive on any type of short exact sequence. So we must check the additivity of $L - L'$ on $0 \to A \to B \to C \to 0$, assuming $B$ finitely generated. If $L(A) < \infty$, then $L - L'$

is additive without any additional hypothesis by Lemma 2.8. If $L(A) = \infty$, then the hypothesis ensures that $(L - L')(A) = \infty$. As $L(B) = \infty = (L - L')(B)$, the additivity of $L - L'$ holds also in this case. □

We continue with four more examples of length functions.

**Example 2.11.** (Sum) If $\{L_\sigma\}_{\sigma\in\Lambda}$ is a family of length functions over $Mod(R)$, their sum $\sum_\sigma L_\sigma$ is the length function defined by setting, for each $M \in Mod(R)$:

$$\sum_{\sigma\in\Lambda} L_\sigma(M) = sup\{\sum_{\sigma\in F} L_\sigma(M) \ : \ F \text{ finite subset of } \Lambda\}.$$

**Example 2.12.** (Scalar multiple) Let $L$ be a length function over $Mod(R)$ and $\lambda$ a positive real number. The scalar multiple $\lambda \cdot L$, defined by setting $(\lambda \cdot L)(M) = \lambda L(M)$ for every $R$-module $M$, is a length function as well.

**Example 2.13.** (Contraction; see [16, Proposition 2]) Let $S$ be a multiplicatively closed subset of $R$ and $H : Mod(R_S) \to \mathbb{R}^*$ a length function. Then $H^c : Mod(R) \to \mathbb{R}^*$, defined by $H^c(M) = H(M_S)$ for each $M \in Mod(R)$, is a length function on $Mod(R)$. Thus $H^c$ is just the composition of $H$ with the localization map $- \otimes_R R_S$.

**Example 2.14.** (Localization; see [16, Proposition 3]) Let $S$ be a multiplicatively closed subset of $R$ and $L : Mod(R) \to \mathbb{R}^*$ a length function. Then $L_S : Mod(R_S) \to \mathbb{R}^*$ defined by $L_S(M) = L(M)$ for each $M \in Mod(R_S)$ is a length function as well. Thus $L_S$ is just the restriction of $L$ to $R_S$-modules. When $S$ is the complement set of a prime ideal $P$, the localization of $L$ at $P$ is simply denoted by $L_P$.

## 3 Length Functions over Valuation Domains

In this section we survey the classification obtained by Northcott and Reufel in [16] for length functions over valuation domains. Recall that an integral domain $R$ is a valuation domain if its ideals are linearly ordered by the inclusion. For terminology, notation and basic facts concerning these domains and their modules, we refer to [9, 10]. In particular, we denote by $v : Q(R) \to \Gamma \cup \{\infty\}$ the valuation of $R$, where $Q(R)$ is the field of fractions of $R$, $\Gamma$ is its value group, and $R = \{x \in Q(R) \ : \ v(x) \geq 0\}$.

Excluding the trivial length function on $Mod(R)$ which sends all modules to 0, characterized by the property that $L(R) = 0$, the length functions may be distinguished in three different types:

- $0/\infty$-type, (I) and (II)
- Rank-type
- Valuation-type.

These types depend on two subsets of $R$, which are associated with the length function $L$:

$$P_\infty = \{a \in R \;:\; L(R/aR) = \infty\} \subseteq P_+ = \{a \in R \;:\; L(R/aR) > 0\}.$$

Note that $L(R) = \infty \Leftrightarrow 0 \in P_\infty \Leftrightarrow P_\infty \neq \emptyset$, and $L(R) > 0 \Leftrightarrow 0 \in P_+ \Leftrightarrow P_+ \neq \emptyset$.

It is easy to check that, if $P_\infty$ and $P_+$ are non-empty, then they are prime ideals, and that $P_+$ is the complement of the multiplicatively closed set $S_L$ defined in the previous section.

We have seen that we can exclude from our classification also length functions satisfying $0 < L(R) < \infty$, since, from Corollary 2.4, we know this condition implies that $L = L(R) \cdot rk$. So the classification of length functions will concern only those $L$ such that $L(R) = \infty$, in which case $P_\infty \subseteq P_+$ are prime ideals. The next result shows that idempotency of these prime ideals plays a role in a crucial way.

**Lemma 3.1.** *If* $L(R) = \infty$ *and* $L(R/P_\infty) < \infty$*, then* $0 < P_\infty^2 = P_\infty = P_+$.

*Proof.* Clearly $0 < P_\infty$. Assume by way of contradiction that $P_\infty^2 < P_\infty$. Take $b \in P_\infty \setminus P_\infty^2$ and consider $bR/bP_\infty$. Then

$$L(bR/P_\infty^2) \leq L(bR/bP_\infty) = L(R/P_\infty) \Rightarrow L(P_\infty/P_\infty^2) = sup_{b \in P_\infty \setminus P_\infty^2} L(bR/P_\infty^2) \leq L(R/P_\infty) < \infty.$$

From the exact sequence:

$$0 \to P_\infty/P_\infty^2 \to R/P_\infty^2 \to R/P_\infty \to 0$$

we deduce that $L(R/P_\infty^2) < \infty$. But this is absurd, since $P_\infty^2 < aR < P_\infty$ implies that $L(R/P_\infty^2) \geq L(R/aR) = \infty$. Thus $P_\infty^2 = P_\infty$. If $a \in R \setminus P_\infty$, then $a^k \in R \setminus P_\infty$ for all positive integers $k$, hence

$$k \cdot L(R/aR) = L(R/a^k R) \leq L(R/P_\infty) < \infty \Rightarrow L(R/aR) = 0 \Rightarrow a \in R \setminus P_+$$

that is, $P_\infty = P_+$. □

We describe now the three different types of length functions and their relationship with the prime ideals $P_\infty$ and $P_+$. The first type, which is called "$0/\infty$-*type*", splits in two sub-types, according as we start with an arbitrary or an idempotent prime ideal $P$ and we set $L(R/P) = \infty$ (first sub-type), or $L(R/P) = 0$ (second sub-type).

## $\mathbf{0/\infty}$ – type (I)

Fixed a prime ideal $P$ of $R$, for an ideal $I$ of $R$ and a module $M \in Mod(R)$, we set

$$L(R/I) = \begin{cases} 0 & \text{if } P < I \\ \infty & \text{if } I \leq P \end{cases} \qquad L(M) = \begin{cases} 0 & \text{if } PM = 0 \text{ and } M_P = 0 \\ \infty & \text{otherwise} \end{cases}$$

If $P = 0$, $L(M) = 0$ for every torsion module $M$, and $L(M) = \infty$ for all other modules.

If $P$ is the maximal ideal, $L(M) = \infty$ for every module $M \neq 0$. In each case $L(R) = \infty$.

In this case $P = P_\infty = P_+$ and P can be idempotent or non-idempotent.

**$0/\infty$ − type (II)**

Fixed an idempotent prime ideal $P = P^2$ of $R$, for an ideal $I$ of $R$ and a module $M \in Mod(R)$, we set

$$L(R/I) = \begin{cases} 0 & \text{if } P \leq I \\ \infty & \text{if } I < P \end{cases} \qquad L(M) = \begin{cases} 0 & \text{if } PM = 0 \\ \infty & \text{if } PM \neq 0 \end{cases}$$

We must exclude $P = 0$ that gives the trivial function, so we have $L(R) = \infty$.

If $P$ is the maximal ideal, then $L(M) = 0$ for $M$ semisimple, otherwise $L(M) = \infty$.

In this case $P = P_\infty = P_\infty^2 = P_+$. The idempotency of $P$ excludes the possibility that $P$ is maximal and principal (if $P = pR$ is maximal, $L(R/pR) = 0$ and $L(R/p^2R) = \infty$, absurd).

**Rank − type**

Given an idempotent prime ideal $P = P^2$ of $R$, and fixed a real number $\lambda > 0$, set:

$$L(R/I) = \begin{cases} 0 & \text{if } P < I \\ \lambda & \text{if } I = P \\ \infty & \text{if } I < P \end{cases} \qquad L(M) = \begin{cases} \lambda \cdot rk_{R/P}(M) & \text{if } PM = 0 \\ \infty & \text{if } PM \neq 0 \end{cases}$$

If $P = 0$, then $L(R) = \lambda$, which implies, by Corollary 2.4, that $L$ coincides with the rank function up to the multiple $\lambda$. We have excluded this case from our classification.

Thus in this case also we have $L(R) = \infty$; furthermore $P = P_\infty = P_\infty^2 = P_+$. The idempotency of $P$ excludes the possibility that $P$ is maximal and principal (if $P = pR$ is maximal, $L(R/pR) = \lambda$ and $L(R/p^2R) = \infty$, absurd). Note that a rank-type length function is discrete.

**Valuation − type**

Given two adjacent prime ideals $P' \subset P$, the valuation domain $S = R_P/P'$ obtained by localizing $R$ at $P$ and factorizing over $P'$ is archimedean, with a valuation:

$$w \;:\; Q(S) \to \mathbb{R} \cup \{\infty\}$$

which is discrete if and only if $S$ is a DVR.

Fixed a real number $\lambda > 0$, we have the induced length function

$$L_w : Mod(S) \to \mathbb{R}^*$$

defined by setting, for every ideal $J$ of $S$:

$$L_w(S/J) = \lambda \cdot inf_{x \in J} w(x).$$

Note that $L_w(S) = \infty$, and, if $S$ is not a DVR, $0 < L_w(S/J) < \infty$ if and only if $0 < J < PR_P/P'$.

From the length function $L_w : Mod(S) \to \mathbb{R}^*$ we derive a length function $L : Mod(R) \to \mathbb{R}^*$ as follows: given an $R$-module $M$, set

$$L(M) = \begin{cases} L_w(M_{PR_P/P'}) & \text{if } P'M = 0 \\ \infty & \text{otherwise} \end{cases}$$

Length functions of this type are the significant ones, since they are related to the valuation of the domain $R$, and are the only non-discrete length functions provided $S = R_P/P'$ is a non-discrete archimedean domain.

If $P' = 0$, then $P$ is the maximal ideal of $R$ and $w = v$ is the valuation of the archimedean valuation domain $R$. If furthermore $\lambda = 1$, $L$ is denoted by $L_v$ and is called the *valuation length*. In this case, for every ideal $I \leq R$ we have:

$$L_v(R/I) = inf_{a \in I} v(a).$$

$L_v$ is non-discrete if and only if $P$ is not principal, equivalently, if $P = P^2$.

To sum up, we have seen that if $L$ is a non-trivial length function on $Mod(R)$ and $L(R) < \infty$, then $L$ is essentially the rank function, while every non-discrete length function $L$ satisfying if $L(R) = \infty$ is essentially a valuation length on a non-discrete archimedean factor of a suitable localization of $R$ at a prime ideal. The composition length is of rank-type if the maximal ideal is idempotent, of valuation type otherwise.

As an immediate application of the above results, we conclude this section with the description of the length functions over two simple types of valuation domains, namely, the archimedean ones (i.e., 1-dimensional), and the strongly discrete ones, i.e., without non-zero idempotents prime ideals (see [10, II.8.3] for their characterization).

**Corollary 3.2.** *Let $R$ be valuation domain. Then*

(1) *if $R$ is 1-dimensional, then the only non-trivial length functions on $R$ are of $0/\infty$-type or, up to a positive real multiple: the composition length and the rank function if $R$ is discrete; the valuation length and the rank function if $R$ is non-discrete;*

(2) *if $R$ is strongly discrete, then the only non-trivial length functions on $R$ are of $0/\infty$-type (I) and of discrete valuation-type.*

# 4 Properties of Prüfer Domains and Their Meet-Spectrum

We fix the notation and start with some basic results holding for an arbitrary commutative integral domain $R$. The (prime) spectrum of $R$ is denoted by $Spec(R)$, and the maximal spectrum by $Max(R)$.

If $I$ is an ideal of $R$, we use the standard notation $\Omega(I)$ to denote the set of the maximal ideals containing $I$. If $S$ is multiplicatively closed set of $R$, let $I_{(S)} = I_S \cap R$ be the contraction of the localization of $I$ at $S$; if $S$ is the complement of a prime ideal $P$, then we simply write $I_{(P)} = I_P \cap R$.

If $\Omega$ is a family of maximal ideals of $R$, the localization of $R$ at the multiplicatively closed set

$$\bigcap_{P\in\Omega}(R \setminus P) = R \setminus \bigcup_{P\in\Omega} P$$

is denoted by $R_\Omega$; the corresponding localization of an ideal $I$ is denoted by $I_\Omega$ and we set $I_{(\Omega)} = I_\Omega \cap R$. If $\Omega$ consists of a single maximal ideal $P$, then we write $I_{(\Omega)} = I_{(P)}$. If $\Omega = \Omega(I)$, then clearly $I_{(\Omega)} = I$.

**Lemma 4.1.** *Let $R$ be an integral domain and $I$ be a non-zero ideal of $R$. If $\Omega = \Omega(I)$, then*

$$R/I \cong R_\Omega/I_\Omega.$$

*Proof.* The composition map

$$R \to R_\Omega \to R_\Omega/I_\Omega$$

has kernel $I_{(\Omega)} = I$, thus $R/I$ embeds into $R_\Omega/I_\Omega$. In order to show that this embedding is also epic, we must prove that $R_\Omega = I_\Omega + R$. First we show that $R = I + sR$ for every $s \in \bigcap_{P\in\Omega}(R \setminus P)$. Assume, by way of contradiction, that $I + sR \leq P'$ for some maximal ideal $P'$. Then $P' \in \Omega$ since it contains $I$; on the other hand, $P' \notin \Omega$ since it contains $s$, absurd. As a consequence we have that, if $r/s \in R_\Omega$, since $r = a + sb$ for some $a \in I, b \in R$, then $r/s = a/s + b \in I_\Omega + R$, as desired. □

**Lemma 4.2.** *Let $R$ be an integral domain, $\Omega$ a finite family of maximal ideals of $R$ and $I$ a non-zero ideal of $R$. The maximal ideals of $R_\Omega$ are exactly the extensions of the maximal ideals in $\Omega$. Furthermore, $I_\Omega = \bigcap_{P\in\Omega} I_P$ and $R_\Omega = \bigcap_{P\in\Omega} R_P$.*

*Proof.* An ideal $P \in \Omega$ clearly survives as a maximal ideal in $R_\Omega$. Conversely, if $Q$ is a maximal ideal in $R_\Omega$, then its contraction $P' = Q \cap R$ is a prime ideal contained in $\bigcup_{P\in\Omega} P$. By prime avoidance, $P'$ is contained in some $P \in \Omega$ and equality must hold, since, as we already noted, $P$ extends to a maximal ideal of $R_\Omega$.

Since every $P \in \Omega$ survives in $R_\Omega$, clearly $I_\Omega \leq \bigcap_{P\in\Omega} I_P$. Conversely, let $x \in \bigcap_{P\in\Omega} I_P$. Then, for each $P \in \Omega$, $(I :_R xR)$ is not contained in $P$; therefore, since the maximal ideals of $R_\Omega$ are the extensions of the ideals in $\Omega$, we obtain that $(I :_R xR)_\Omega = R_\Omega$. Moreover, $(I :_R xR)_\Omega = (I_\Omega :_{R_\Omega} xR_\Omega)$, whence $x \in I_\Omega$. □

We restrict now our consideration to Prüfer domains, which may be defined in several different ways; for our purposes, the right definition is that each localization $R_P$ at a maximal (or non-zero prime) ideal $P$ is a valuation domain. For general notion on Prüfer domains and their modules we refer to the monographs [7, 10]. Since there is an ordered bijection between the prime ideals contained in a fixed prime ideal $P$ of $R$ and the prime ideals of the localization $R_P$, which form a totally ordered set, $Spec(R)$ is a rooted tree (the ideal 0 is its root) with the order given by the inclusion, according to the following:

**Definition 4.3.** A tree is a partially ordered set $T$ such that, for every element $t \in T$, the subset $\{t' \in T \mid t' \leq t\}$ is totally ordered.

*Remark 4.4.* Very often the definition of tree requires the stronger assumption that, for every element $t \in T$, the set $\{t' \in T \mid t' \leq t\}$ is well-ordered. The results by Lewis [15] on the characterization of partially ordered sets as spectra of Prüfer (or Bézout) domains uses Definition 4.3 above.

As usual, we denote by $J(R)$ the Jacobson radical of the integral domain $R$, i.e., the intersection of its maximal ideals. The next proposition provides an indispensable tool for comparing the length of cyclic modules and of certain localizations of them.

**Proposition 4.5.** *Let $R$ be a Prüfer domain, $P$ a non-zero prime ideal contained in $J(R)$, and $L$ a length function over $R$. The following facts hold:*

(1) *every ideal $I$ of $R$ is comparable with $P$;*

(2) *if $L(R/P) < \infty$, then $L$ is localized at $P$;*

(3) *if $S$ is a multiplicatively closed set disjoint from $P$, and $I \leq P$, then $L(R/I) = L(R_S/I_S) = L(R_P/I_P)$.*

*Proof.* (1) Suppose the ideal $I$ is not contained in $P$. Then, for each maximal ideal $Q$, $I_Q$ is not contained in $P_Q \neq R_Q$, and since $R_Q$ is a valuation domain, $P_Q$ is strictly contained in $I_Q$, so that $I = \bigcap_{Q \in Max(R)} I_Q$ contains $P = \bigcap_{Q \in Max(R)} P_Q$.

(2) If $x \in R \setminus P$, then point (1) implies that $P < xR$, so that $L(R/xR) = 0$, by Proposition 2.3. Then $x \in S_L$, whence $S_L$ contains $R \setminus P$, showing that $L$ is localized at $P$, by Proposition 2.6.

(3) If $L$ is localized at $P$, then it is localized at $S$ as well, by Proposition 2.6, and the result is true for every $R$-module. On the other hand, if $L$ is not localized at $P$, then point (2) shows that $\infty = L(R/P) \leq L(R/I)$, and the conclusion follows from the existence of canonical inclusions $R/P \leq R_S/P_S \leq R_P/P_P$, and the fact that $L(R/I) \geq L(R/P)$ for every $I \leq P$. □

Given two different non-zero prime ideals $P$ and $P'$ of $R$, their intersection $P \cap P'$ is never a prime ideal and it contains the product $P \cdot P'$; the prime ideals contained in $P \cap P'$ form a chain, hence their union is the biggest prime ideal contained in $P \cap P'$, which is denoted by $P \wedge P'$. The same holds for the intersection of finitely many prime ideals. With this operation $Spec(R)$ is a meet-semilattice.

The next lemma shows that the localization of $R$ at $P \wedge P'$ coincides with the double localization with respect to $P$ and $P'$.

**Lemma 4.6.** *Let $P \neq P'$ be two maximal ideals of the Prüfer domain $R$. Then $(R_P)_{P'} = (R_{P'})_P = R_{P \wedge P'}$.*

*Proof.* $(R_P)_{P'} = R_S$, where $S$ is the multiplicatively closed set generated by $(R \setminus P) \cup (R \setminus P') = R \setminus (P \cap P')$. Since $P \wedge P' \leq P \cap P'$, $R \setminus (P \cap P')$ contains $S$, so $P \wedge P'$ survives in $R_S$. Moreover, every prime ideal not contained in $P \wedge P'$ cannot be contained in $P \cap P'$, hence it must intersect $R \setminus (P \cap P')$, so that $R_S = \bigcap \{R_J \ : \ J \in Spec(R), JR_S < R_S\} = R_{P \wedge P'}$. □

From now on, $R$ will always denote a Prüfer domain of finite character, i.e., every non-zero element (or ideal) is contained only in finitely many maximal ideals. If $R$ is such a domain and the non-zero prime ideal $P$ is contained in the maximal ideals $M_1, \cdots, M_n$, let

$$\bar{P} = M_1 \wedge \cdots \wedge M_n$$

which is a prime ideal containing $P$.

**Definition 4.7.** Let $R$ be a Prüfer domain of finite character. The meet-spectrum of $R$, denoted by $\wedge Max(R)$, is the subset of $Spec(R)$:

$$\wedge Max(R) = \{P \in Spec(R) \mid 0 \neq P = \bar{P}\}.$$

In other words, the meet-spectrum of $R$ contains those non-zero prime ideals which can be written as the meet of finitely many maximal ideals. Obviously the following inclusions hold:

$$Max(R) \setminus \{(0)\} \subseteq \wedge Max(R) \subseteq Spec(R).$$

The equality $Max(R) = Spec(R)$ occurs if and only if $R$ is 1-dimensional; furthermore, the equality $Max(R) \setminus \{(0)\} = \wedge Max(R)$ occurs if and only if every non-zero prime ideal is contained in a unique maximal ideal, hence, under the hypothesis that $R$ has finite character, if $R$ is $h$-local.

For Prüfer domains of finite character we have at disposal the following result, due to Brandal [5], on the structure of torsion cyclic modules (see also [10, V.1.2]).

**Theorem 4.8.** (Brandal [5]) *Let $R$ be a Prüfer domain of finite character and $I$ a non-zero ideal of $R$. Then:*

(1) *the cyclic module $R/I$ is a direct sum of indecomposable cyclic modules;*

(2) *the cyclic module $R/I$ is indecomposable if and only if, for any partition $\{\Omega_1, \Omega_2\}$ of $\Omega(I)$, there exists $M_i \in \Omega_i$ $(i = 1, 2)$ such that $I \leq M_1 \wedge M_2$.*

We will improve this result using the meet-spectrum of $R$ in the next Theorem 4.10, for which we need the following

**Lemma 4.9.** *Let $I$ be a non-zero ideal of the Prüfer domain $R$. If $P \in \Omega(I)$, then $\sqrt{I_{(P)}}$ is the unique minimal prime ideal containing $I_{(P)}$, and $\sqrt{I_{(P)}} \leq P$.*

*Proof.* Since $R_P$ is a valuation domain, $I_P$ has exactly one minimal prime ideal in $R_P$, which coincides with $\sqrt{I_P}$. Now we have:

$$\sqrt{I_{(P)}} = (\sqrt{I})_{(P)} = (\sqrt{I})_P \cap R = \sqrt{I_P} \cap R$$

so that $\sqrt{I_{(P)}}$ is a prime ideal contained in $P$, hence it is the only minimal prime ideal of $I_{(P)}$. □

Given a non-zero ideal $I \leq R$, the meet-spectrum $\wedge Max(R)$ induces a partition on the finite set $\Omega(I)$ as follows. Consider the finite set of the prime ideals of $\wedge Max(R)$ which contain $I$ and are minimal with respect to this containment, denoted by $\wedge Min(I)$. Then clearly $\{\Omega(P) \mid P \in \wedge Min(I)\}$ is a partition of $\Omega(I)$, called the *partition induced by the meet-spectrum*. The following result shows that this partition gives rise to an indecomposable direct decomposition of $R/I$; notice that item (2) improves Lemma 4.1.

**Theorem 4.10.** *Let $R$ be a Prüfer domain of finite character and $I$ a non-zero ideal of $R$. If $\{\Omega_1, \cdots, \Omega_m\}$ is the partition of $\Omega(I)$ induced by the meet-spectrum $\wedge Max(R)$, then:*

(1) $R/I \cong \bigoplus_{1 \leq i \leq m} R/I_{(\Omega_i)}$ *is a direct decomposition with indecomposable direct summands, and*

(2) *for every $i \leq m$ we have the isomorphism $R/I_{(\Omega_i)} \cong R_{\Omega_i}/I_{\Omega_i}$.*

*Proof.* (1) Consider the canonical map $R \to \bigoplus_{1 \leq i \leq m} R/I_{(\Omega_i)}$, whose kernel is $I = \bigcap_{1 \leq i \leq m} I_{(\Omega_i)}$. This map provides an embedding $\epsilon : R/I \to \bigoplus_{1 \leq i \leq m} R/I_{(\Omega_i)}$. For every index $i$, the equality $\Omega(\bigcap_{j \neq i} I_{(\Omega_j)}) = \bigcup_{j \neq i} I_{(\Omega_j)}$ holds, which gives $I_{(\Omega_i)} + \bigcap_{j \neq i} I_{(\Omega_j)} = R$. From this equality the surjectivity of the map $\epsilon$ follows. Finally, each summand $R/I_{(\Omega_i)}$ is indecomposable since it satisfies condition (2) of Theorem 4.8: if $\Omega_i = \Omega(P)$ with $P \in \wedge Min(I)$ and $P \leq M_1, M_2 \in \Omega(P)$, then $I \leq P \leq M_1 \wedge M_2$.

(2) The proof is similar to that of Lemma 4.1. Let us set $\Omega_i = \Omega$. The composition map $R \to R_\Omega \to R_\Omega/I_\Omega$ has kernel $I_{(\Omega)}$, thus $R/I_{(\Omega)}$ embeds into $R_\Omega/I_\Omega$. In order to show that this embedding is also epic, we must prove that $R_\Omega = I_\Omega + R$. First we show that $R = I_{(\Omega)} + sR$ for every $s \in \bigcap_{P \in \Omega}(R \setminus P)$. Assume, by way of contradiction, that $I_{(\Omega)} + sR \leq P'$ for some maximal ideal $P'$. Then $P' \notin \Omega$ since it contains $s$, but $P'$ must contain $I_{(P)}$ for some $P \in \Omega$. Thus both $P$ and $P'$ must contain the single minimal prime of $I_{(P)}$. But then $I \subseteq P \wedge P'$, which is impossible by the current hypothesis. The conclusion is now as in the proof of Lemma 4.1. □

Fixed a prime ideal $P \in \wedge Max(R)$, the set

$$T(P) = \{P' \in \wedge Max(R) \mid P \subseteq P'\}$$

is a finite tree with root $P$, in which the meet of two elements is the same as the meet in $Spec(R)$.

**Definition 4.11.** Let $R$ be a Prüfer domain of finite character and let $P \in \wedge Max(R)$. Then a child of $P$ is a prime ideal $P' \in T(P)$ different from $P$ which is adjacent to $P$.

Clearly, every element of the meet-spectrum is either a maximal ideal (with no children), or it is the meet of at least two maximal ideals, hence it has at least two children.

If the ring $R$ is semilocal, so in particular of finite character, then the meet-spectrum of $R$ enjoys nice properties.

**Lemma 4.12.** *Let $R$ be a semilocal Prüfer domain, then:*

(1) $\wedge Max(R)$ *is a finite set;*

(2) $\wedge Max(R)$ *is a disjoint union of a finite number of rooted trees $T(P)$, ranging $P$ over the set of the minimal elements of $\wedge Max(R)$;*

(3) $\wedge Max(R)$ *is a rooted tree if and only if the largest prime ideal contained in the Jacobson radical is non-zero.*

*Proof.* (1) and (2) are obvious.

(3) The largest prime ideal contained in the Jacobson radical is the meet of all maximal ideals, so it is the unique minimal element of $\wedge Max(R)$ exactly if it is non-zero. □

We prove now a technical result needed in the proof of the main Theorem 5.7, concerning the meet-spectrum of a semilocal Prüfer domain $R$ in case it is rooted, relating the number of children of the non-maximal elements to the number of the maximal ideals.

For this purpose, we introduce the following notation: let $k_P$ be the number of children of a prime ideal $P \in \wedge Max(R)$, and denote by $\mathcal{C}$ the complement of $Max(R)$ in $\wedge Max(R)$:

$$\mathcal{C} = \wedge Max(R) \setminus Max(R).$$

We exclude the trivial case of $R$ local, so that $\mathcal{C} \neq \emptyset$.

**Proposition 4.13.** *Let $R$ be a semilocal non-local Prüfer domain with maximal ideals $M_1, \cdots, M_n$ and suppose that the meet-spectrum $\wedge Max(R)$ is a rooted tree. Then the following formula holds:*

$$\sum_{Q \in \mathcal{C}} (k_Q - 1) = n - 1.$$

*Proof.* Since every element of $\wedge Max(R)$ is a child, except the root, the following equality holds: $\sum_{Q \in \mathcal{C}} k_Q = | \wedge Max(R)| - 1$. Therefore we get:

$$\sum_{Q \in \mathcal{C}} k_Q = |\mathcal{C}| + |Max(R)| - 1 \Rightarrow \sum_{Q \in \mathcal{C}} k_Q - |\mathcal{C}| = |Max(R)| - 1$$

from which the equality $\sum_{Q \in \mathcal{C}} (k_Q - 1) = n - 1$ immediately follows. □

## 5 Length Functions over Semilocal Prüfer Domains

A semilocal Prüfer domain is trivially of finite character; it is a classical result due to Hinohara in 1962 that it is also a Bézout domain, that is, finitely generated ideals are principal (see [10, III, 5.1]).

In this and in the next section, in order to simplify the notation, we set $\mathcal{M} = Max(R)$ and $\wedge\mathcal{M} = \wedge Max(R)$. Recall that a *local length function for R* is a length function on $Mod(R_P)$ for some $P \in \mathcal{M}$. Since with the symbol $L_P$ we denote the localization at $P$ of a length function $L : Mod(R) \to \mathbb{R}^*$, we will indicate an arbitrary local length function for $R$ with the symbol $L^{(P)}$.

A close inspection to the proof of Theorem 1.1 shows that it is based on the following facts, holding for every ideal $I \neq 0$ of a 1-dimensional Prüfer domain of finite character $R$: if $\Omega(I) = \{P_1, \cdots, P_n\}$, then

$$R/I \cong R/I_{(P_1)} \oplus \cdots \oplus R/I_{(P_n)}$$

is an indecomposable direct decomposition; and, if $P \in \Omega(I)$, then $R/I_{(P)} \cong R_P/I_P$.

These two facts imply that

$$L(R/I) = \sum_{1 \le i \le n} L(R_{P_i}/I_{P_i}) = \sum_{1 \le i \le n} L_{P_i}(R_{P_i}/I_{P_i});$$

furthermore, if $P \in \mathcal{M}$ and $J$ is a non-zero proper ideal of $R_P$, then $J = (J \cap R)_P$ (see [9, p. 6, (D)] and $J \cap R$ is $\sqrt{J \cap R}$-primary, therefore $R_P/J \cong R/(J \cap R)$; consequently $L^{(P)}(R_P/J) = L(R/(J \cap R))$, so that $L^{(P)} = L_P$ for every $P \in \mathcal{M}$.

When we try to extend Theorem 1.1 from 1-dimensional to arbitrary Prüfer domains of finite character, the more complex structure of the meet-spectrum $\wedge\mathcal{M}$ creates problems in the decomposition of $L$ as sum of its localizations at maximal ideals and also in the uniqueness of its representation, due to the fact that the action of local length functions can overlap, as the next example shows.

**Example 5.1.** Let $V = \mathbb{Q}[[X]]$ be the 1-dimensional valuation domain of the rational power series. If $P = X\mathbb{Q}[[X]]$ denotes its maximal ideal, then the residue field $V/P$ is isomorphic to $\mathbb{Q}$. Fixed a prime number $p \in \mathbb{N}$, let $W_p = \mathbb{Z}_p + X\mathbb{Q}[[X]]$ be the subring of $V$ consisting of the power series with constant term in $\mathbb{Z}_p$, the localization at the prime ideal $p\mathbb{Z}$ of the ring of the integers $\mathbb{Z}$. $W_p$ is the pullback of the canonical surjection $V \to \mathbb{Q}$ and the inclusion $\mathbb{Z}_p \to \mathbb{Q}$. Clearly $W_p$ is a 2-dimensional strongly discrete valuation domain, with the same quotient field as $V$. Its non-zero prime ideals are $P$ and $pW_p = p\mathbb{Z}_p + P$; moreover, $(W_p)_P = V$.

Let now $q$ be a prime number different from $p$ and consider the valuation domain $W_q$ obtained in a similar way as before. The ring $R = W_p \cap W_q$ is a Bézout domain with exactly two maximal ideals (see [10, III, 5.1]). Its spectrum is given by the two maximal ideals $pR$ and $qR$, the prime ideal $pR \wedge qR = P$, and the null ideal. In particular, $R_{pR} = W_p$, $R_{qR} = W_q$ and $R_P = (W_p)_P = (W_q)_P = V$.

In order to obtain a length function over $Mod(R)$, in view of Example 2.11 one can simply add together two local length functions $L^{(pR)}$ and $L^{(qR)}$ chosen over the two localizations at maximal ideals $R_{pR} = W_p$ and $R_{qR} = W_q$, respectively. Looking at Section 3 and taking care that we don't have non-zero idempotent prime ideals, we have, up to positive multiples, only three cases for a non-trivial length function $L^{(pR)} : W_p \to \mathbb{R}^*$ such that $L^{(pR)}(W_p) = \infty$.

Case 1. $L^{(pR)}$ is of $0/\infty$-type (I), so that $L^{(pR)}(W_p/I) = 0$ or $\infty$, according as $P < I$ or $I \leq P$;

Case 2. $L^{(pR)}$ is of valuation-type associated with the pair of prime ideals $(P < pW_p)$, so that $L^{(pR)}(W_p/I) = k$ if $I = p^k W_p$ for some $k \geq 0$, and $L^{(pR)}(W_p/I) = \infty$ otherwise;

Case 3. $L^{(pR)}$ is of valuation-type associated with the pair of prime ideals $(0 < P)$, so that $L^{(pR)}(W_p/I) = 0$ if $P \leq I$, and $L^{(pR)}(W_p/I) = k$ if $I = X^k\mathbb{Q}[[X]]$.

We have a similar situation for $W_q$. Now if we choose $L^{(pR)}$ as in Case 2 above, and we add it to a local length function $L^{(qR)}$ as in Case 1 or Case 3, we always have the same length function $L = L^{(pR)} + L^{(qR)}$; in fact, in both cases we have $L(R/I) = k + 0 = k$, for a certain $k \in \mathbb{N}$, if $P < I$, and $L(R/I) = \infty$ otherwise. So uniqueness is lost.

Let now $L : Mod(R) \to \mathbb{R}^*$ be the length function which is the contraction of the valuation length $H : R_P = V \to \mathbb{R}*$ (see Example 2.13). Then the localizations $L_{pR}$ and $L_{qR}$ both coincide with $H$, so the equality $L = L_{pR} + L_{qR}$ cannot hold. In fact, $L(R/P) = H(R_P/P) = 1$, while we get

$$L_{pR}(R/P) + L_{qR}(R/P) = L(R_{pR}/P_{pR}) + L(R_{qR}/P_{qR}) = H(R_P/P) + H(R_P/P) = 1 + 1 = 2.$$

So also the decomposition of $L$ as sum of its localizations at maximal ideals is lost.

If we want to express a length function $L$ by means of a sum $\sum_{P\in\mathcal{M}} L^{(P)}$ of local length functions such that each $L^{(P)}$ coincides with the localization of $L$ at $P$, we must ask that the given family satisfies a certain compatibility condition, according with the following

**Definition 5.2.** A family of local length functions $\{L^{(P)}\}_{P\in\mathcal{M}}$ is compatible if $L^{(P)}(R_P) = \infty$ for all $P \in \mathcal{M}$ and, for each pair $P, P' \in \mathcal{M}$, $(L^{(P)})_{P\wedge P'} = (L^{(P')})_{P\wedge P'}$.

In fact, the family of the localizations $L_P$ $(P \in \mathcal{M})$ of a length function $L$ such that $L(R) = \infty$ is compatible, since for each pair of maximal ideals $P$ and $P'$, $(L_P)_{P\wedge P'} = (L_{P'})_{P\wedge P'}$, both being equal to $L_{P\wedge P'}$. Note that for a 1-dimensional Prüfer domain the compatibility condition is trivially satisfied.

Another problem is made evident by the final part of Example 5.1, which indicates that $\sum_{P\in\mathcal{M}} L_P$ is strictly larger in general than $L$, so we must subtract something from it. This problem arises since the meet-spectrum $\wedge\mathcal{M}$ is larger than the maximal spectrum $\mathcal{M}$. Recall that we denoted by $\mathcal{C}$ the complement of $\mathcal{M}$ in $\wedge\mathcal{M}$, that is, $\mathcal{C} = \wedge\mathcal{M} \setminus \mathcal{M}$. If $\{L^{(P)}\}_{P\in\mathcal{M}}$ is a compatible family of local length functions, and if $Q \in \mathcal{C}$, we denote by $L^{(Q)}$ the common localization at $Mod(R_Q)$ of all $L^{(P)}$ such that $P \in \Omega(Q)$. In order to state our main theorem, we introduce the following

**Definition 5.3.** Given a compatible family $\mathcal{L} = \{L^{(P)}\}_{P\in\mathcal{M}}$ of local length functions, we call $L'_{\mathcal{L}}$ and $L''_{\mathcal{L}}$ the maximal sum and the complement sum of $\mathcal{L}$, respectively, where

$$L'_{\mathcal{L}} = \sum_{P\in\mathcal{M}} L^{(P)} \quad , \quad L''_{\mathcal{L}} = \sum_{Q\in\mathcal{C}} (k_Q - 1)L^{(Q)}.$$

Using this definition and the notation in it, we have the following

**Lemma 5.4.** *If $\mathcal{L} = \{L^{(P)}\}_{P\in\mathcal{M}}$ is a compatible family of local length functions, then its maximal sum $L'_{\mathcal{L}}$ and complement sum $L''_{\mathcal{L}}$ satisfy the inequality $L'_{\mathcal{L}} \geq L''_{\mathcal{L}}$.*

*Proof.* It is enough to prove that, for every ideal $I$ of $R$, $L'_{\mathcal{L}}(R/I) \geq L''_{\mathcal{L}}(R/I)$. If $I = 0$, then all the involved length functions assign value $\infty$ to $R$, so the above inequality is verified. Assume that $I \neq 0$ and let $\{Q_1, \cdots, Q_m\} = \wedge Min(I)$. The sets $\Omega_i = \Omega(Q_i)$ form a partition of $\Omega(I)$. Denote by $\mathcal{Q}_i$ the subset of $\wedge\mathcal{M}$ consisting of the elements containing $Q_i$; then $\mathcal{Q}_i$ is a rooted tree with root $Q_i$, which is order-isomorphic to the meet-spectrum of $R_{\Omega_i}$, and the $\mathcal{Q}_i$ are disjoint sets. Denoting by $n_i$ the cardinality of $\Omega_i$, we have for each $i$:

$$\sum_{P\in\Omega_i} L^{(P)}(R_P/I_P) = n_i\alpha_i$$

where $\alpha_i = L^{(Q_i)}(R_{Q_i}/I_{Q_i})$, since $L^{(P)}(R_P/I_P) = L^{(Q_i)}(R_{Q_i}/I_{Q_i})$ for all $P \in \mathcal{Q}_i$. Applying Proposition 4.13 to $R_{\Omega_i}$ we get:

$$\sum_{Q\in\mathcal{Q}_i\setminus\Omega_i} (k_Q - 1)L^{(Q)}(R_Q/I_Q) = \sum_{Q\in\mathcal{Q}_i\setminus\Omega_i} (k_Q - 1)\alpha_i = (n_i - 1)\alpha_i.$$

We can now conclude that:

$$L'_{\mathcal{L}}(R/I) = \sum_{P\in\mathcal{M}} L^{(P)}(R_P/I_P) = \sum_{P\in\Omega(I)} L^{(P)}(R_P/I_P) = \sum_i n_i\alpha_i$$

$$\geq \sum_i (n_i - 1)\alpha_i = \sum_{Q\in\mathcal{C}} (k_Q - 1)L^{(Q)}(R_Q/I_Q) = L''_{\mathcal{L}}(R/I).$$

□

We can now prove the following result.

**Proposition 5.5.** *Let $R$ be a semilocal Prüfer domain and $\mathcal{L} = \{L^{(P)}\}_{P\in\mathcal{M}}$ a compatible family of local length functions over $Mod(R)$. Let $L'_{\mathcal{L}}$, $L''_{\mathcal{L}}$ be the maximal sum and the complement sum of $\mathcal{L}$, respectively. Then the difference $L'_{\mathcal{L}} - L''_{\mathcal{L}}$ is a length function.*

*Proof.* In view of Proposition 2.10, it is enough to prove that, if $A$ is a submodule of a finitely generated $R$-module satisfying $L'_{\mathcal{L}}(A) = \infty$, then $(L'_{\mathcal{L}} - L''_{\mathcal{L}})(A) = \infty$. If there exists a finitely generated submodule $F$ of $A$ such that $L'_{\mathcal{L}}(F) = \infty$, then $(L'_{\mathcal{L}} - L''_{\mathcal{L}})(F) = \infty$, hence $(L'_{\mathcal{L}} - L''_{\mathcal{L}})(A) = \infty$. Suppose on the contrary that all the finitely generated submodules $F \leq A$ satisfy $L'_{\mathcal{L}}(F) < \infty$. These finitely generated modules $F$ are unions of finite chains of submodules with cyclic sections $R/I$ which satisfy also $L'_{\mathcal{L}}(R/I) < \infty$, since $L'_{\mathcal{L}}(F)$ is the sum of the lengths of these sections. Using the notation in the proof of Lemma 5.4 and denoting by $N$ the number of the maximal ideals of $R$, we have:

$$L'_{\mathcal{L}}(R/I) = \sum_i n_i \alpha_i \leq N \sum_i \alpha_i$$

hence

$$L'_{\mathcal{L}}(R/I) - L''_{\mathcal{L}}(R/I) = \sum_i \alpha_i \geq N^{-1} L'_{\mathcal{L}}(R/I).$$

Therefore $L'_{\mathcal{L}}(F) - L''_{\mathcal{L}}(F)) \geq N^{-1} L'_{\mathcal{L}}(F)$ for all finitely generated modules $F$. Since $L'_{\mathcal{L}}(F)$ is unbounded, so is $L'_{\mathcal{L}}(F) - L''_{\mathcal{L}}(F))$. □

In view of Proposition 5.5, we can give the following definition.

**Definition 5.6.** Let $\mathcal{L} = \{L^{(P)}\}_{P \in \mathcal{M}}$ be a compatible family of local length functions for $R$. The balanced sum of this family is the length function defined as the difference $L_{\mathcal{L}} = L'_{\mathcal{L}} - L''_{\mathcal{L}}$.

We can now state our main theorem, which says that the balanced sums of compatible families of length functions over a semilocal Prüfer domain $R$ represent all the length functions $L$ such that $L(R) = \infty$, and that this representation is unique. Keeping in mind that the involved local length functions are defined over valuation domains, hence covered by the classification illustrated in Section 3, we obtain an unambiguous classification.

**Theorem 5.7.** *Let $R$ be a semilocal Prüfer domain. Given a length function $L$ over $R$ such that $L(R) = \infty$, there exists a unique compatible family $\{L^{(P)}\}_{P \in \mathcal{M}}$ of local length functions for $R$ such that $L$ equals their balanced sum, and $L^{(P)}$ coincides with the localization $L_P$ for each $P \in \mathcal{M}$.*

*Proof.* First we prove that $L$ coincides with the balanced sum of its localizations at maximal ideals. So let $\mathcal{L} = \{L_P\}_{P \in \mathcal{M}}$ and $L' = L'_{\mathcal{L}}$, $L'' = L''_{\mathcal{L}}$. Let $I$ be a non-zero ideal of $R$, $\Omega = \Omega(I)$, $\wedge Min(I) = \{Q_1, \cdots, Q_m\}$ and $\Omega_i = \Omega(I_i)$ for $i = 1, \cdots, m$. By Theorem 4.10 and Lemma 4.1 we get:

$$R/I \cong \bigoplus_{1 \leq i \leq m} R_{\Omega_i}/I_{\Omega_i}.$$

First suppose that $L(R/I) = \infty$. Then, for some index $k$, $\infty = L(R_{\Omega_k}/I_{\Omega_k}) = L(R_{Q_k}/I_{Q_k}) = \alpha_k$, where the last equality follows from Proposition 4.5 applied to $Mod(R_{\Omega_k})$. Using the notation in the proof of Lemma 5.4, we get:

$$L'(R/I) = \sum_{1 \le i \le m} n_i \alpha_i \ge \alpha_k = \infty.$$

Therefore, by definition, $(L' - L'')(R/I) = \infty$. Suppose now that $L(R/I) < \infty$. Then $\alpha_i < \infty$ for all $i$ and, by additivity and by the proof of Lemma 5.4, we get:

$$L(R/I) = \sum_{1 \le i \le m} L(R_{\Omega_i}/I_{\Omega_i}) = \sum_{1 \le i \le m} \alpha_i$$

$$= \sum_{1 \le i \le m} n_i \alpha_i - \sum_{1 \le i \le m} (n_i - 1)\alpha_i = (L' - L'')(R/I).$$

The case $I = 0$ being trivial, since all the involved length functions assume infinite value on the ground ring, we have proved that $L$ coincides on cyclic modules with the balanced sum $L'_{\mathcal{L}} - L''_{\mathcal{L}}$ of its localizations at maximal ideals, so they are equal.

In order to prove uniqueness, given a compatible family $\{\mathcal{L}\} = \{L^{(P)}\}_{P \in \mathcal{M}}$ of local length functions for $R$ such that $L = L'_{\mathcal{L}} - L''_{\mathcal{L}}$, we must prove that, for every $P \in \mathcal{M}$, $L^{(P)} = L_P$. Let $0 \neq I$ be an ideal of $R$ and let $P \in \Omega(I)$. In order to simplify notation, let $W = R_P/I_P$; we may assume, without loss of generality, that $I = I_{(P)}$, so that $\sqrt{I}$ is the only minimal prime ideal containing it. Consider the prime ideal:

$$Q = \bigwedge_{P' \in \Omega(I)} P' = \bigwedge_{P' \in \Omega(\sqrt{I})} P'$$

which is the smallest element of $\mathcal{C}$ containing $I$. Therefore, if $I \le N \in \mathcal{C}$ and $I \le P' \in \mathcal{M}$, we have:

$$L^{(P)}(W) = L^{(P')}(W_{P'}) = L^{(P \wedge P')}(W_{P \wedge P'}) = L^{(N)}(W_N) = L^{(Q)}(W_Q) = \alpha.$$

Then we get:

$$L'_{\mathcal{L}}(W) = \sum_{P' \in \mathcal{M}} L^{(P')}(W_{P'}) = \sum_{P' \in \Omega(I)} L^{(P')}(W_{P'}) = |\Omega(I)| \cdot \alpha.$$

On the other hand, we get:

$$L''_{\mathcal{L}}(W) = \sum_{N \in \mathcal{C}} (k_N - 1) L^{(N)}(W_N) = \sum_{N \in \mathcal{C}} (k_N - 1)\alpha = (|\Omega(I)| - 1) \cdot \alpha$$

where the last equality follows by Proposition 4.13 applied to the domain $R_{\Omega(I)}$. Now, if $L_P(W) = \infty$, then $\infty = L_{\mathcal{L}}(W) = L'_{\mathcal{L}}(W) = |\Omega(I)| \cdot \alpha$, so $L^{(P)}(W) = \alpha = \infty$. On the other hand, if $L^{(P)}(W) = \alpha < \infty$, then $L_P(W) = L_{\mathcal{L}}(W) = L'_{\mathcal{L}}(W) - L''_{\mathcal{L}}(W) = \alpha = L^{(P)}(W)$.

In conclusion, since $L^{(P)}(R_P) = \infty = L_P(R_P)$, the two length functions $L_P$ and $L^{(P)}$ agree on all cyclic $R_P$-modules, hence $L_P = L^{(P)}$ is uniquely determined by $L$. □

## 6 Length Functions over Prüfer Domains of Finite Character

In this section we extend Theorem 5.7 to Prüfer domains of finite character. This class of rings is of central importance among Prüfer domains; it includes Dedekind domains (the Noetherian case) and semilocal Prüfer domains. An example of Prüfer domain of finite character which is neither Dedekind nor semilocal can be found in [12], while an example of Prüfer (actually, Bézout) domain which fails to be of finite character is the ring of entire functions investigated by Helmer in [13]. For an extensive treatment of these domains and their modules we refer to [10].

In order to underline the importance of these domains, it is worth recalling that Bazzoni proved that their class semigroup is a Clifford semigroup, determining the idempotents, the constituent groups and the bonding homomorphisms (see [2–4, 8] and [10, Chapter III, Sections 2, 3]). Furthermore, in [14] it was proved, solving a conjecture posed by Bazzoni in [2], that a Prüfer domain with the property that every locally finitely generated ideal is finitely generated is, in fact, of finite character.

We will need the following

**Lemma 6.1.** *Let $R$ be a Prüfer domain of finite character and $\{L^{(P)}\}_{P\in\mathcal{M}}$ a family of compatible local length functions for $R$. If $\Omega \subseteq \mathcal{M}$, then $\{L^{(P)}\}_{P\in\Omega}$ is a family of compatible local length functions for $R_\Omega$.*

*Proof.* The proof follows immediately from the observation that every localization $R_P$ at a maximal ideal $P \in \Omega$ coincides with $(R_\Omega)_P$. □

Theorem 5.7 can now be extended *verbatim* to Prüfer domains of finite character, but the proof of its extension requires some additional argument for the reduction to the semilocal case.

**Theorem 6.2.** *Let $R$ be a Prüfer domain of finite character. Given a length function $L$ over $R$ such that $L(R) = \infty$, there exists a unique compatible family $\{L^{(P)}\}_{P\in\mathcal{M}}$ of local length functions for $R$ such that $L$ equals their balanced sum, and $L^{(P)}$ coincides with the localization $L_P$ for each $P \in \mathcal{M}$.*

*Proof.* First we show that the balanced sum of a compatible family $\mathcal{L} = \{L^{(P)}\}_{P\in\mathcal{M}}$ of length functions over $R$ is still a well defined length function. Write $L' = L'_{\mathcal{L}}$ and

$L'' = L''_{\mathcal{L}}$. Let $I$ be a non-zero ideal of $R$ and set $\Omega = \Omega(I)$. The elements $Q \in \wedge\mathcal{M}$ containing $I$ are in finite number, an this subset of $\wedge\mathcal{M}$ is order-isomorphic to the meet-spectrum of the semilocal Prüfer domain $R_\Omega$. Denote by $E$ the cyclic module $R/I$. Then by Lemma 4.1 we have:

$$L'(E) = L'(E_\Omega) = \sum_{P\in\mathcal{M}} L^{(P)}(E_P) = \sum_{P\in\Omega} L^{(P)}(E_P)$$

and similarly

$$L''(E) = L''(E_\Omega) = \sum_{I\subseteq Q\in\mathcal{C}} (k_Q - 1)L^{(Q)}(E_Q).$$

Now, by Lemma 6.1, $\{L^{(P)}\}_{P\in\Omega}$ is a family of compatible length functions for $R_\Omega$, hence we can apply Theorem 5.7 to this semilocal domain, ensuring that $L'(E) \geq L''(E)$. The analogue for $I = 0$ is trivial. We can now extend the proof of Proposition 5.5 to the present situation, taking care that finitely generated torsion $R$-modules $B$ and their submodules are modules over a suitable localization of $R$ which is semilocal. So we deduce that $L' - L''$ is a length function.

Now we deal with the existence part. We reduce to the semilocal case, by localizing at the finite set of maximal ideals $\Omega = \Omega(I)$. We have that $L(E) = L(E_\Omega) = L_\Omega(E_\Omega)$, and $L_\Omega$ is a length function over $R_\Omega$, hence by Theorem 5.7 we have

$$L_\Omega = \sum_{P\in\Omega}(L_\Omega)_P - \sum_{I\subseteq Q\in\mathcal{C}} (k_Q - 1)(L_\Omega)_Q.$$

Clearly, the summands $(L_\Omega)_P$ and $(L_\Omega)_Q$ in the above equation coincide, respectively, with $L_P$ and $L_Q$, so that:

$$L(E) = (\sum_{P\in\Omega} L_P - \sum_{I\subseteq Q\in\mathcal{C}} (k_Q - 1)L_Q)(E_\Omega)$$

$$= (\sum_{P\in\Omega} L_P - \sum_{I\subseteq Q\in\mathcal{C}} (k_Q - 1)L_Q)(E) = (\sum_{P\in\mathcal{M}} L_P - \sum_{Q\in\mathcal{C}}(k_Q - 1)L_Q)(E).$$

Since $\{L_P\}_{P\in\mathcal{M}}$ is a compatible family, and being the case $I = 0$ trivial, this proves that $L = L_{\{L_P\}}$.

The proof of the uniqueness is identical to the one given in Theorem 5.7 for the semilocal case. □

As an easy consequence of Theorem 6.2, we obtain the characterization of length functions over $h$-local Prüfer domains, which extends Theorem 1.1.

**Corollary 6.3.** *Let $R$ be a $h$-local Prüfer domain and $L : Mod(R) \to \mathbb{R}^*$ a length function such that $L(R) = \infty$. Then there exists a unique family $\{L^{(P)}\}_{P\in\mathcal{M}}$ of local length functions for $R$ such that $L = \sum_{P\in\mathcal{M}} L^{(P)}$, and $L^{(P)}$ coincides with the localization $L_P$ of $L$ for each $P \in \mathcal{M}$.*

*Proof.* It is enough to recall that for a $h$-local domain $R$, $\wedge\mathcal{M} = \mathcal{M}$, hence the balanced sum of $\{L^{(P)}\}_{P\in\mathcal{M}}$ coincides with the usual sum, and the compatibility condition for a family of local length functions is always trivially satisfied. □

As a natural conclusion of this paper we pose the following:

**Problem 6.4.** *Characterize length functions over arbitrary Prüfer domains.*

**Acknowledgements** We would like to thank the referee for the numerous remarks that improved the presentation of our paper.

## References


1. Adler, R.L., Konheim, A.G., McAndrew, M.H.: Topological entropy. Trans. Am. Math. Soc. **114**, 309–319 (1965)
2. Bazzoni, S.: Class semigroups of Prüfer domains. J. Algebra. **184**, 613–631 (1996)
3. Bazzoni, S.: Idempotents of the class semigroup of a Prüfer domain of finite character, LNPAM, vol. 201, pp. 79-89. Marcel Dekker (1998)
4. Bazzoni, S.: Groups in the class semigroup of a Prüfer domain of finite character. Commun. Algebra **28**(11), 5157–5167 (2000)
5. Brandal, W.: On $h$-local integral domains. Trans. Am. Math. Soc. **206**, 201–212 (1975)
6. Dikranjan, D., Goldsmith, B., Salce, L., Zanardo, P.: Algebraic entropy of endomorphisms of abelian groups. Trans. Am. Math. Soc. **361**, 3401–3434 (2009)
7. Fontana, M., Huckaba, J.A., Papick, I.J.: Prüfer Domains. Pure Appl. Math. (1997) (Marcel Dekker)
8. Fuchs, L.: On the class semigroups of Prüfer domains. In: Abelian Groups and Modules. Birkhäuser, pp. 319–326 (1999)
9. Fuchs, L., Salce, L.: Modules over Valuation Domains. Marcel Dekker, New York (1985)
10. Fuchs, L., Salce, L.: Modules over Non-Noetherian Domains. Mathematical Surveys and Monographs. Providence, vol. 84 (2001) (Am. Math. Soc.)
11. Fusacchia, G.: Length Functions Over Prüfer Domains of Finite Character, unpublished notes
12. Heinzer, W.: Quotient overrings of integral domains. Mathematika **17**, 139–148 (1970)
13. Helmer, O.: Divisibility properties of integral functions. Duke Math. J. **6**, 351–000 (1940)
14. Holland, W.C., Martinez, J., McGovern, W.W., Tesemmad, M.: Bazzoni's conjecture. J. Algebra **320**(4), 1764–1768 (2008)
15. Lewis, W.J.: The spectrum of a ring as a partially ordered set. J. Algebra **25**, 419–434 (1973)
16. Northcott, D.G., Reufel, M.: A generalization of the concept of length. Q. J. Math. (Oxford) (2), **16**, 297–321 (1965)
17. Salce, L., Vámos, P., Virili, S.: Length functions, multiplicities and algebraic entropy. Forum Math. **25**(2), 255–282 (2013)
18. Salce, L., Zanardo, P.: A general notion of algebraic entropy and the rank-entropy. Forum Math. **21**(4), 579–599 (2009)
19. Spirito, D.: Decomposition and Classification of Length Functions, preprint
20. Vámos, P.: Length functions on modules, Ph.D. thesis, University of Sheffield (1968)
21. Vámos, P.: Additive functions and duality over Noetherian rings. Q. J. Math. (Oxford) (2) **19**, 43–55 (1968)
22. Virili, S.: Length functions and algebraic entropy over commutative Noetherian rings, Internal report, Universitá de Castellon (2012)
23. Virili, S.: Length Functions of Grothendieck Categories with Applications to Infinite Group Representations, preprint (2014). arxiv:1410.8306
24. Zanardo, P.: Multiplicative invariants and additive functions over valuation domains. J. Commut. Algebra. **3**(4), 561–587 (2011)

# On Some Arithmetical Properties of Noetherian Domains

**Florian Kainrath**

**Abstract** We give a characterization of those noetherian domains, such that for all non zero $a \in R$ there are only (up to associates) finitely many irreducibles, that divide some power of $a$. In turns out, that a necessary condition for that, is that the integral closure of $R$ is a root extension of $R$. We also give a description of noetherian domains with this property.

**Keywords** Quasi finitely · Generated monoid · Root extension · Associated prime

## 1 Introduction

Let $R$ be a noetherian domain. For a non-zero non-unit $a \in R$ let $f(a) \in \mathbb{N} \cup \{\infty\}$ be the number of essentially different factorizations of $a$, and $N(a) \in \mathbb{N} \cup \{\infty\}$ the number (up to associates) of irreducibles dividing some power of $a$. The behaviour of $f(a^n)$ as $n \to \infty$ depends on the number $N(a)$ in the following way:

$$f(a^n) \quad \begin{cases} = An^s + O(n^{s-1}) & \text{if } N(a) < \infty \\ \gg n^r \quad \text{for all integers } r & \text{if } N(a) = \infty, \end{cases}$$

for some $A \in \mathbb{Q}_{>0}$ and some $s \in \mathbb{N}$ (see [6] Theorems 1 and 2). We will give a description of those $R$, such that $N(a) < \infty$ for all $a$. As we will see, a necessary condition for that, is that the integral closure $\bar{R}$ of $R$ is a root extension of $R$, i.e. for all $x \in \bar{R}$ there exists some $m \in \mathbb{N}$, such that $x^m \in R$. We will also give a characterization of noetherian domains having this property. This answers a question, that remained open in the description of tamely inside factorial, noetherian domains, achieved in [1] (Corollary 6).

F. Kainrath (✉)
Institut für Mathematik, Karl-Franzens-Universität Graz,
Heinrichstraße 36, 8010 Graz, Austria
e-mail: florian.kainrath@uni-graz.at



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_12

## 2 Quasi Finitely Generated Monoids

In this paper a monoid is commutative, cancellative monoid with unit 1. We let $Q(H)$ be the quotient group of a monoid $H$, and let $H^\times$ be its group of units. $H$ is called reduced, if $H^\times = \{1\}$. The monoid $H_{\text{red}} = H/H^\times$ is reduced.

Let $D$ be a monoid and $H \subset D$ a submonoid. $H$ is called to be saturated in $D$, if for all $h_1, h_2 \in H$ we have $h_1 \mid_H h_2 \iff h_1 \mid_D h_2$, or equivalently if $Q(H) \cap D = H$.

For a subset $A$ of $H$, let $[A]_H$ be the submonoid generated by $A$ in $H$ and let $[[A]]_H$ be the divisor-closed submonoid of $H$ generated by $A$, i.e. $[[A]]_H$ consists of all $h \in H$ dividing some $a \in [A]_H$. $H$ is called finitely generated, if $H = [A]_H$ for some finite subset $A \subset H$. $H$ is called quasi finitely generated, if $H_{\text{red}}$ is finitely generated. Note that this will be so, if and only if every element is a product of irreducibles and $H$ has (up to associates) only finitely many irreducibles. We call $H$ locally finitely generated, if for all $a \in H$ the monoid $[[a]]_H := [[\{a\}]]_H$ is quasi finitely generated.

An extension $H \subset D$ of monoids or rings is called a root extension, if for all $d \in D$, there is some $m \in \mathbb{N}^+$ such that $d^m \in H$. The monoid $\widetilde{H} = \{x \in Q(H) \mid x^m \in H \text{ for some } m \in \mathbb{N}^+\}$ is called the root closure of $H$. It is contained in the complete integral closure $\widehat{H}$, which consists of all $x \in Q(H)$, such that there exists some $c \in H$ with $cx^n \in H$ for all $n \in \mathbb{N}$. If $H = R\backslash\{0\}$ for some noetherian domain $R$, then $\widehat{H} = \bar{R}\backslash\{0\}$, where $\bar{R}$ is the integral closure of $R$.

Finally, if $R$ is a domain and $a \in R\backslash\{0\}$, then let $R_a$ be the ring of fractions $\{x/a^n \mid x \in R \text{ and } n \in \mathbb{N}\}$. Note that $[[a]]_R$ $(= [[a]]_{R\backslash\{0\}}) = R \cap R_a^\times$ and $Q([[a]]_R) = R_a^\times$.

**Lemma 1.** *Let $H$ be a monoid. Then $H$ is quasi finitely generated if and only if $\widehat{H}$ is quasi finitely generated, $\widetilde{H} = \widehat{H}$ and $\widehat{H}^\times/H^\times$ is finite.*

*Proof.* We may suppose that $H$ is reduced. Suppose first that $H$ is finitely generated. From Proposition 2.7.11 and Lemma 2.7.12 in [4] we get that $\widetilde{H} = \widehat{H}$ is finitely generated. It remains to show that $\widetilde{H}^\times$ is finite. Clearly it is finitely generated, since $\widetilde{H}$ is so. From the definition of $\widetilde{H}$ and $H \cap \widetilde{H}^\times = H^\times = \{1\}$ (Lemma 5.4 in [3]) we get that $\widetilde{H}^\times$ is a torsion group and hence is finite.

Conversely, assume that $\widehat{H} = \widetilde{H}$ is quasi finitely generated and that $\widetilde{H}^\times = \widehat{H}^\times$ is finite. Then clearly $\widetilde{H}$ is finitely generated, which implies that $H$ is finitely generated by Proposition 6.1 in [3].

**Lemma 2.** *Let $R$ be a noetherian domain and $a \in R$, $a \neq 0$. Then:*

1. $\widehat{[[a]]_R} = R_a^\times \cap \bar{R}$.
2. $\widehat{[[a]]_R}$ *is a saturated submonoid of* $[[a]]_{\bar{R}}$.
3. $\widehat{[[a]]_R}$ *is quasi finitely generated.*

*Proof.* (1) and (2) follow from Lemma 3.6 in [5].

(3) follows now from (2) and Propositions 2.7.5.1 and 2.7.8.3 in [4].

**Theorem 1.** *Let $R$ be a noetherian domain. Then the following are equivalent:*

1. *$R\backslash\{0\}$ is locally finitely generated.*
2. *$R \subset \bar{R}$ is a root extension and for all $a \in R\backslash\{0\}$ the group $(R_a^\times \cap \bar{R}^\times)/R^\times$ is finite.*

*If $\bar{R}$ is a finitely generated $R$-module, then the second condition in (2) is equivalent to the finiteness of the group $\bar{R}^\times/R^\times$.*

*Proof.* We have

$$\bar{R}\backslash\{0\} = \bigcup_{a\in R\backslash\{0\}} R_a^\times \cap \bar{R} = \bigcup_{a\in R\backslash\{0\}} \widehat{[[a]]_R} \quad .$$

Hence the extension $R \subset \bar{R}$ is a root extension if and only if this holds for $[[a]]_R \subset \widehat{[[a]]_R}$ for all $a \in R\backslash\{0\}$. Now the equivalence of 1. and 2. follows from Lemma 1.

Suppose now that $\bar{R}$ is a finitely generated $R$-module. For all $a \in R\backslash\{0\}$ we have $(R_a^\times \cap \bar{R}^\times)/R^\times \subset \bar{R}^\times/R^\times$. So the finiteness of $\bar{R}^\times/R^\times$ implies the finiteness of $(R_a^\times \cap \bar{R}^\times)/R^\times$ for all $a \in R\backslash\{0\}$. Conversely, let us assume that all the groups $(R_a^\times \cap \bar{R}^\times)/R^\times$ ($a \in R\backslash\{0\}$) are finite. Since $\bar{R}$ is a finitely generated $R$-module, there exists some $a \in R\backslash\{0\}$ such that $a\bar{R} \subset R$. Then we have $\bar{R}_a = R_a$ and hence $R_a^\times \cap \bar{R}^\times = \bar{R}^\times$, so that $\bar{R}^\times/R^\times$ is finite.

## 3 Root Extensions of Noetherian Rings

Let $R$ be a (commutative) ring. For a prime ideal $p$ of $R$ we let $k(p)$ be its residue field. If $R \subset S$ is any extension ring of $R$ and if there is only one prime ideal of $S$ lying over $p$, we denote this prime by $p_S$. For any $R$-module $M$ we denote by $\mathrm{Ass}_R(M)$ the set of prime ideals associated to $M$. If $p$ is any prime ideal of $R$ we denote by $R_p$ the ring of fractions $(R\backslash p)^{-1}R$.

The aim of this section is to prove the following theorem:

**Theorem 2.** *Let $R$ be a noetherian ring and $R \subset S$ an integral extension of $R$. Then $R \subset S$ is a root extension if and only if the following holds:*

1. *The induced map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is one to one (and hence bijective).*
2. *For any $p \in \mathrm{Ass}_R(S/R)$ we have either $k(p)$ is an algebraic extension of a finite field or $\mathrm{char}(k(p)) > 0$ and $k(p_S)$ is purely inseparable over $k(p)$.*

For the proof of this theorem we need a series of lemmas.

**Lemma 3.** *Let $R \subset S$ be a root extension of rings. Then the induced map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is one to one.*

*Proof.* Let $R \subset S$ be a root extension of rings and let $p \in \mathrm{Spec}(R)$. Choose any $q \in \mathrm{Spec}(S)$ lying over $p$. Then $q = \{x \in S \mid x^n \in p \text{ for some } n \in \mathbb{N}\}$, so that $q$ is uniquely determined.

**Lemma 4.** *Let $R \subset S$ be a root extension of rings and let $T \subset R$ be multiplicatively closed and let $I$ be an ideal of $S$. Then the extensions $T^{-1}R \subset T^{-1}S$ and $R/(I \cap R) \subset S/I$ are root extension, too. In particular for any prime ideal $p$ of $R$ the extension $k(p) \subset k(p_S)$ is a root extension.*

*Proof.* This is obvious.

**Lemma 5.** *Let $k \subset k'$ be an algebraic extension of fields. Then it is a root extension if and only if either $k$ is an algebraic extension of a finite field or the extension is purely inseparable.*

*Proof.* This is well known. See for example Proposition 3.6 in [2].

In the next two Lemmas we consider an extension $R \subset S$ such that $R$ and $S$ are local and noetherian. We denote by $m$ resp. $m_S$ the maximal ideal of $R$ resp. $S$. We assume further that $S$ is a finitely generated $R$-module and that $\mathrm{Ass}_R(S/R) = \{m\}$. In particular $R \neq S$. Note that $S/R$ is an $R$-module of finite length, and hence is annihilated by some power of $m$. Therefore there is some integer $n$ such that $m^n S \subset R$. Further $m_S$ is the unique prime ideal of $S$ containing $mS$. Hence $\sqrt{mS} = m_S$. Since $S$ is noetherian, there is some integer $k$ such that $m_S^k \subset mS$. We choose $k$ minimal with this property. Putting these two inclusions together, we obtain $m_S^{kn} \subset R$. Note that $1 + m \subset R^\times$ and $1 + mS \subset 1 + m_S \subset S^\times$ are subgroups and that we have two exact sequences of abelian groups

$$1 \longrightarrow \frac{1+m_S}{1+m} \longrightarrow S^\times/R^\times \longrightarrow k(m_S)^\times/k(m)^\times \longrightarrow 1 \tag{1}$$

$$1 \longrightarrow \frac{1+mS}{1+m} \longrightarrow \frac{1+m_S}{1+m} \longrightarrow \frac{1+m_S}{1+mS} \longrightarrow 1 \quad . \tag{2}$$

**Lemma 6.** *The group $(1 + m_S)/(1 + m)$ is a torsion group, if and only if $m = m_S$ or $\mathrm{char}(k(m)) > 0$.*

*Proof.* To begin with let $I \subset J \subset m_S$ be two ideals of $S$ such that $J^2 \subset I$. Then the map $x \mapsto 1 + x$ induces an isomorphism of abelian groups $J/I \to (1 + J)/(1 + I)$. Applying this to $m_S^{l+1} \subset m_S^l$ for $l$=1, ..., $k$, we see that the group $(1+m_S)/(1+m_S^k)$ has a finite filtration, whose quotients are vector spaces over $k(m)$. Hence $(1 + m_S)/(1 + m_S^k)$ is a torsion group if $\mathrm{char}(k(m)) > 0$.

Next consider the group $(1 + m_S)/(1 + mS)$. Suppose that it is a non-trivial torsion group. Then $m_S \neq mS$. Hence $k \geq 2$. Then $(1 + m_S^{k-1})/(1 + m_S^{k-1} \cap mS) \cong (1 + m_S^{k-1})(1 + mS)/(1 + mS)$ is a non-trivial subgroup of $(1 + m_S)/(1 + mS)$. But as we have seen above $(1 + m_S^{k-1})/(1 + m_S^{k-1} \cap mS)$ is isomorphic to $m_S^{k-1}/(m_S^{k-1} \cap mS)$, which is a non-trivial vector space over $k(m)$. Hence $\mathrm{char}(k(m)) > 0$. Conversely suppose that $\mathrm{char}(k(m)) > 0$. Then we already know that $(1 + m_S)/(1 + m_S^k)$ is a torsion group. Since $m_S^k \subset mS$ our group $(1 + m_S)/(1 + mS)$ is a homomorphic image of $(1 + m_S)/(1 + m_S^k)$. Hence it is a torsion group, too. Putting our observations together, we obtain, that $(1 + m_S)/(1 + mS)$ is a torsion group if and only if either $m_S = mS$ or $\mathrm{char}(k(m)) > 0$.

For any integer $l$ let $U_l$ be the image of $1 + m^{l+1}S$ in $(1 + mS)/(1 + m)$. Then the $U_l$ form a filtration of $(1 + mS)/(1 + m)$, whose quotients are again vector spaces over $k(m)$ (see Lemma 2.3 in [7]). Since $m^n S \subset R$ this filtration is finite. So we obtain that $(1 + mS)/(1 + m)$ is a torsion group if and only if either $m = mS$ or $\mathrm{char}(k(m)) > 0$.

The assertion of the Lemma follows now from the exact sequence (2).

**Lemma 7.** *$R \subset S$ is a root extension, if and only if either $k(m)$ is an algebraic extension of a finite field or* char $k(m) > 0$ *and the extension of fields $k(m) \subset k(m_S)$ is purely inseparable.*

*Proof.* From $m_S^{kn} \subset R$ and $S = m_S \cup S^\times$ we conclude that $R \subset S$ is a root extension if and only if $S^\times/R^\times$ is a torsion group. Now the exact sequence (1) tells us, that this will be so if and only if $k(m) \subset k(m_S)$ is a root extension and $(1 + m_S)/(1 + m)$ is a torsion group. Since $R \neq S$ we have $k(m) \neq k(m_S)$ if $m = m_S$. Now the assertion of the lemma follows from Lemmas 5 to 6.

**Lemma 8.** *Let $R \subset S$ be any non-trivial extension of rings and let $T \subset R$ be the set of all non-zero divisors of the $R$-module $S/R$. Then $R \subset S$ is a root extension if and only if $T^{-1}R \subset T^{-1}S$ is a root extension.*

*Proof.* By Lemma 4 we need only show that $R \subset S$ is a root extension if $T^{-1}R \subset T^{-1}S$ is one. So let us assume that $T^{-1}R \subset T^{-1}S$ is a root extension and let $s \in S$. Then there exists some $r \in R$, $t \in T$ and an integer $n \geq 1$ such that $s^n/1 = r/t \in T^{-1}S$. Hence $t'ts^n \in R$ for some $t' \in T$. By definition of $T$ this implies $s^n \in R$.

We are now in the position to prove Theorem 2.

*Proof.* (*Proof of Theorem* 2) Let $R \subset S$ be as in the statement of the Theorem. Let $\Sigma$ be the set of all $R$-subalgebras of $S$, which are finitely generated $R$-modules. Then $S$ is a root extension of $R$ if and only if every member of $\Sigma$ is so. Further we have $\mathrm{Ass}_R(S/R) = \bigcup \mathrm{Ass}_R(S'/R)$ where $S'$ ranges over $\Sigma$. We may therefore assume that $S$ is a finitely generated $R$-module. By Lemma 3 we may further assume that $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is one to one. This implies that $\mathrm{Spec}(S) \to \mathrm{Spec}(R')$, $\mathrm{Spec}(R') \to \mathrm{Spec}(R)$ are one to one, too, for any intermediate ring $R'$ of $R \subset S$.

Suppose first that $R \subset S$ is a root extension and let $p \in \mathrm{Ass}_R(S/R)$. From Lemmas 4 to 5 we already know that either $k(p)$ is an algebraic extension of a finite field or $k(p) \subset k(p_S)$ is purely inseparable. So we are left to show that $\mathrm{char}(k(p)) > 0$. Let $q$ be any minimal member of $\mathrm{Ass}_R(S/R)$ contained in $p$. Then we have an epimorphism $R/q \to R/p$. So if $\mathrm{char}(k(q)) = \mathrm{char}(R/q) > 0$ then $\mathrm{char}(k(p)) = \mathrm{char}(R/p) > 0$, too. Therefore we suppose that $p$ is minimal in $\mathrm{Ass}_R(S/R)$. Then we have $\mathrm{Ass}_{R_p}(S_p/R_p) = \{pR_p\}$. After replacing $R$ and $S$ by $R_p$ and $S_p$ we may assume that $R$ and $S$ are local and $p$ is the maximal ideal of $R$. Now we are in the situation of Lemma 7, which in particular tells us that $\mathrm{char}(k(p)) > 0$.

Next assume that for all $p \in \mathrm{Ass}_R(S/R)$ either $k(p)$ is an algebraic extension of a finite field or $k(p) \subset k(p_S)$ is purely inseparable. Choose any minimal member $p$ of $\mathrm{Ass}_R(S/R)$ and let $R' = \{x \in S \mid sx \in R \text{ for some } s \in R \backslash p\}$ $(= R_p \cap S)$ be the $p$-primary component of $R$ in $S$. Then $R'$ is a subring of $S$ containing $R$, and we have $\mathrm{Ass}_R(R'/R) = \mathrm{Ass}_R(S/R)\backslash\{p\}$ and $\mathrm{Ass}_R(S/R') = \{p\}$. By Proposition 9. A in [8] we have $\{p\} = \mathrm{Ass}_R(S/R') = \{q \cap R \mid q \in \mathrm{Ass}_{R'}(S/R')\}$. It follows, that $\mathrm{Ass}_{R'}(S/R') = \{p_{R'}\}$. Hence using an induction on the cardinality of $\mathrm{Ass}_R(S/R)$, we reduce to the case that $\mathrm{Ass}_R(S/R) = \{p\}$.

Set $T = R\backslash p$. Then $T$ consists exactly of the non-zero divisors of $S/R$. By Lemma 8 we may replace $R \subset S$ by $T^{-1}R \subset T^{-1}S$. But now Lemma 7 shows us that $R \subset S$ is a root extension.

## References

1. Chapman, S.T., Halter-Koch, F., Krause, U.: Inside factorial monoids and integral domains. J. Algebra **252**, 350–375 (2002)
2. Davis, E.D., Maroscia, P.: Affince curves on which every point is a set-theoretic complete intersection. J. Algebra **87**, 113–135 (1984)
3. Geroldinger, A., Halter-Koch, F.: Arithmetical theory of monoid homomorphisms. Semigroup Forum **48**, 333–362 (1994)
4. Geroldinger, A., Halter-Koch, F.: Non-Unique factorizations. Algebraic, combinatorial and analytic theory. Pure and Applied Mathematics, vol. 278. Chapman & Hall/CRC (2006)
5. Geroldinger, A., Hassler, W.: Arithmetic of Mori domains and monoids. J. Algebra **319**, 3419–3463 (2008)
6. Halter-Koch, F.: On the asymptotic behaviour of the number of distinct factorizations into irreducibles. Ark. Mat. **31**, 297–305 (1993)
7. Kainrath, F.: A note on quotients formed by unit groups of semilocal rings. Houst. J. Math **24**, 613–618 (1998)
8. Matsumura, H.: Commutative Algebra, 2nd ed. Benjamin/Cummings (1989)

# Spectral Spaces Versus Distributive Lattices: A Dictionary

**Henri Lombardi**

**Abstract** The category of distributive lattices is, in classical mathematics, antiequivalent to the category of spectral spaces. We give here some examples and a short dictionary for this antiequivalence. We propose a translation of several abstract theorems (in classical mathematics) into constructive ones, even in the case where points of a spectral space have no clear constructive content.

**Keywords** Distributive lattice · Spectral space · Constructive mathematics · Krull dimension · Zariski lattice · Zariski spectrum · Real spectrum · Valuative spectrum · Lying over · Going up · Going down

## Introduction

This paper is written in Bishop's style of constructive mathematics [3, 4, 6, 17, 22]. We give a short dictionary between classical and constructive mathematics w.r.t. properties of spectral spaces and of the associated dual distributive lattices. We give several examples of how this works.

## 1 Distributive Lattices and Spectral Spaces: Some General Facts

References: [7, 10, 19, 20, 23], [1, Chapter 4] and [17, Chapters XI and XIII].

H. Lombardi (✉)
Laboratoire de Mathématiques de Besançon, Université Bourgogne Franche-Comté, Bourgogne Franche-Comté, France
e-mail: henri.lombardi@univ-fcomte.fr
URL: http://hlombardi.free.fr/



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*, Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_13

### 1.1 The Seminal Paper by Stone

In classical mathematics, a *prime ideal* $\mathfrak{p}$ of a distributive lattice $\mathbf{T} \neq \mathbf{1}$ is an ideal whose complement $\mathfrak{f}$ is a filter (*a prime filter*). The quotient lattice $\mathbf{T}/(\mathfrak{p} = 0, \mathfrak{f} = 1)$ is isomorphic to $\mathbf{2}$. Giving a prime ideal of $\mathbf{T}$ is the same thing as giving a lattice morphism $\mathbf{T} \to \mathbf{2}$. We will write $\theta_{\mathfrak{p}} : \mathbf{T} \to \mathbf{2}$ the morphism corresponding to $\mathfrak{p}$.

If $S$ is a system of generators for a distributive lattice $\mathbf{T}$, a prime ideal $\mathfrak{p}$ of $\mathbf{T}$ is characterised by its trace $\mathfrak{p} \cap S$ (cf. [7]).

The (Zariski) *spectrum of the distributive lattice* $\mathbf{T}$ is the set $\mathsf{Spec}\,\mathbf{T}$ whose elements are prime ideals of $\mathbf{T}$, with the following topology: an open basis is provided by the subsets $\mathfrak{D}_{\mathbf{T}}(a) \overset{\text{def}}{=} \{\mathfrak{p} \in \mathsf{Spec}\,\mathbf{T} \mid a \notin \mathfrak{p}\} = \left\{\mathfrak{p} \mid \theta_{\mathfrak{p}}(a) = 1\right\}$. One has

$$\left.\begin{array}{ll} \mathfrak{D}_{\mathbf{T}}(a \wedge b) = \mathfrak{D}_{\mathbf{T}}(a) \cap \mathfrak{D}_{\mathbf{T}}(b), & \mathfrak{D}_{\mathbf{T}}(0) = \emptyset, \\ \mathfrak{D}_{\mathbf{T}}(a \vee b) = \mathfrak{D}_{\mathbf{T}}(a) \cup \mathfrak{D}_{\mathbf{T}}(b), & \mathfrak{D}_{\mathbf{T}}(1) = \mathsf{Spec}\,\mathbf{T}. \end{array}\right\} \tag{1}$$

The complement of $\mathfrak{D}_{\mathbf{T}}(a)$ is a *basic closed set* denoted by $\mathfrak{V}_{\mathbf{T}}(a)$. This notation is extended to $I \subseteq \mathbf{T}$: we let $\mathfrak{V}_{\mathbf{T}}(I) \overset{\text{def}}{=} \bigcap_{x \in I} \mathfrak{V}_{\mathbf{T}}(x)$. If $\mathfrak{I}$ is the ideal generated by $I$, one has $\mathfrak{V}_{\mathbf{T}}(I) = \mathfrak{V}_{\mathbf{T}}(\mathfrak{I})$. The closed set $\mathfrak{V}_{\mathbf{T}}(I)$ is also called *the subvariety of* $\mathsf{Spec}\ \mathbf{T}$ *defined by* $I$.

The adherence of a point $\mathfrak{p} \in \mathsf{Spec}\ \mathbf{T}$ is provided by all $\mathfrak{q} \supseteq \mathfrak{p}$. Maximal ideals are the closed points of $\mathsf{Spec}\ \mathbf{T}$. The spectrum $\mathsf{Spec}\ \mathbf{T}$ is empty iff $0 =_{\mathbf{T}} 1$.

The spectrum of a distributive lattice is the paradigmatic example of a *spectral space*. Spectral spaces can be characterised as the topological spaces satisfying the following properties:

- the space is quasi-compact,[1]
- every open set is a union of quasi-compact open sets,
- the intersection of two quasi-compact open sets is a quasi-compact open set,
- for two distinct points, there is an open set containing one of them but not the other,
- every irreducible closed set is the adherence of a point.

The quasi-compact open sets then form a distributive lattice, the supremum and the infimum being the union and the intersection, respectively. A continuous map between spectral spaces is said to be *spectral* if the inverse image of every quasi-compact open set is a quasi-compact open set.

Stone's fundamental result [23] can be stated as follows. *The category of distributive lattice is, in classical mathematics, antiequivalent to the category of spectral spaces.*

Here is how this works.

1. *The quasi-compact open sets of* $\mathsf{Spec}\ \mathbf{T}$ *are exactly the* $\mathfrak{D}_{\mathbf{T}}(u)$*'s.*
2. *The map* $u \mapsto \mathfrak{D}_{\mathbf{T}}(u)$ *is well-defined and it is an isomorphism of distributive lattices.*

---

[1] The nowadays standard terminology is quasi-compact, as in Bourbaki and Stacks, rather than compact.

In the other direction, if $X$ is a spectral space we let $\mathsf{Oqc}(X)$ be the distributive lattice formed by its quasi-compact open sets. If $\xi : X \to Y$ is a spectral map, the map

$$\mathsf{Oqc}(\xi) : \mathsf{Oqc}(Y) \to \mathsf{Oqc}(X), \quad U \mapsto \xi^{-1}(U)$$

is a morphism of distributive lattices. This defines $\mathsf{Oqc}$ as a contravariant functor.

Johnstone calls *coherent spaces* the spectral spaces [16]. Balbes and Dwinger [1] give them the name *Stone space*. The name *spectral space* is given by Hochster in a famous paper [15] where he proves that all spectral spaces can be obtained as Zariski spectra of commutative rings.

In constructive mathematics, spectral spaces may have no points. So it is necessary to translate the classical stuff about spectral spaces into a constructive rewriting about distributive lattices. It is remarkable that all useful spectral spaces in the literature correspond to simple distributive lattices.

Two other natural spectral topologies can be defined on $\mathsf{Spec}\ \mathbf{T}$ by changing the definition of basic open sets. When one chooses the $\mathfrak{V}(a)$'s as basic open sets, one gets the spectral space corresponding to $\mathbf{T}^{\circ}$ (obtained by reversing the order). When one chooses Boolean combinations of the $\mathfrak{D}(a)$'s as basic open sets one gets the constructible topology (also called the patch topology). This spectral space can be defined as the spectrum of $\mathbb{B}\mathrm{o}(\mathbf{T})$ (the Boolean algebra generated by $\mathbf{T}$).

### 1.1.1 Spectral Subspaces Versus Quotient Lattices

**Theorem 1.** (Subspectral spaces) *Let $\mathbf{T}'$ be a quotient lattice of $\mathbf{T}$ and $\pi : \mathbf{T} \to \mathbf{T}'$ the quotient morphism. Let us write $X' = \mathsf{Spec}\,\mathbf{T}'$, $X = \mathsf{Spec}\,\mathbf{T}$ and $\pi^\star : X' \to X$ the dual map of $\pi$.*

1. *$\pi^\star$ identifies $X'$ with a* topological subspace *of $X$. Moreover $\mathsf{Oqc}(X') = \{\, U \cap X' \mid U \in \mathsf{Oqc}(X)\,\}$. We say that $X'$* is a subspectral space of $X$.
2. *A subset $X'$ of $X$ is a subspectral space of $X$ if and only if*
   *– the induced topology by $X$ on $X'$ is spectral and*
   *– $\mathsf{Oqc}(X') = \{\, U \cap X' \mid U \in \mathsf{Oqc}(X)\,\}$.*
3. *A subset $X'$ of $X$ is a subspectral space if and only if it is closed for the patch topology.*
4. *If $Z$ is an arbitrary subset of $X = \mathsf{Spec}\,\mathbf{T}$, its adherence for the patch topology is given by $X' = \mathsf{Spec}\,\mathbf{T}'$, where $\mathbf{T}'$ is the quotient lattice of $\mathbf{T}$ defined by the following preorder $\preccurlyeq$:*

$$a \preccurlyeq b \iff (\mathfrak{D}_{\mathbf{T}}(a) \cap Z) \subseteq (\mathfrak{D}_{\mathbf{T}}(b) \cap Z). \tag{2}$$

### 1.1.2 Gluing Distributive Lattices and Spectral Subspaces

Let $(x_1, \dots, x_n)$ be a system of comaximal elements in a commutative ring $\mathbf{A}$. Then the canonical morphism $\mathbf{A} \to \prod_{i \in [\![1..n]\!]} \mathbf{A}[1/x_i]$ identifies $\mathbf{A}$ with a finite subproduct of localisations of $\mathbf{A}$.

Similarly a distributive lattice can be recovered from a finite number of good quotient lattices.

**Definition 1.** Let $\mathbf{T}$ be a distributive lattice and $(\mathfrak{a}_i)_{i \in [\![1..n]\!]}$ (resp. $(\mathfrak{f}_i)_{i \in [\![1..n]\!]}$) a finite family of ideals (resp. of filters) of $\mathbf{T}$. We say that the ideals $\mathfrak{a}_i$ *cover* $\mathbf{T}$ if $\bigcap_i \mathfrak{a}_i = \{0\}$. Similarly we say that the filters $\mathfrak{f}_i$ *cover* $\mathbf{T}$ if $\bigcap_i \mathfrak{f}_i = \{1\}$.

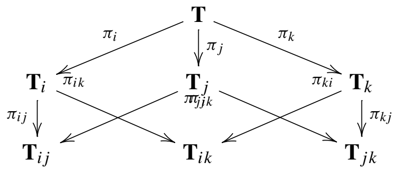
Let $\mathfrak{b}$ be an ideal of $\mathbf{T}$; we write $x \equiv y \mod \mathfrak{b}$ as meaning $x \equiv y \mod (\mathfrak{b} = 0)$. Let us recall that for $s \in \mathbf{T}$ the quotient $\mathbf{T}/(s = 0)$ is isomorphic to the principal filter $\uparrow s$ (one sees this filter as a distributive lattice with $s$ as 0 element).

**Fact 1.** *Let $\mathbf{T}$ be a distributive lattice, $(\mathfrak{a}_i)_{i \in [\![1..n]\!]}$ a finite family of principal ideals ($\mathfrak{a}_i = \downarrow s_i$) and $\mathfrak{a} = \bigcap_i \mathfrak{a}_i$.*

1. *If $(x_i)$ is a family in $\mathbf{T}$ s.t. for each $i, j$ one has $x_i \equiv x_j \mod \mathfrak{a}_i \vee \mathfrak{a}_j$, then there exists a unique $x$ modulo $\mathfrak{a}$ satisfying: $x \equiv x_i \mod \mathfrak{a}_i$ ($i \in [\![1..n]\!]$).*
2. *Let us write $\mathbf{T}_i = \mathbf{T}/(\mathfrak{a}_i = 0)$, $\mathbf{T}_{ij} = \mathbf{T}_{ji} = \mathbf{T}/(\mathfrak{a}_i \vee \mathfrak{a}_j = 0)$, $\pi_i : \mathbf{T} \to \mathbf{T}_i$ and $\pi_{ij} : \mathbf{T}_i \to \mathbf{T}_{ij}$ the canonical maps. If the ideals $\mathfrak{a}_i$ cover $\mathbf{T}$, the system $(\mathbf{T}, (\pi_i)_{i \in [\![1..n]\!]})$ is the inverse limit of the diagram*

$$((\mathbf{T}_i)_{1 \le i \le n}, (\mathbf{T}_{ij})_{1 \le i < j \le n}; (\pi_{ij})_{1 \le i \ne j \le n}).$$

3. *The analogous result works with quotients by principal filters.*




We have also a gluing procedure described in the following proposition.[2]

**Proposition 1.** (Gluing distributive lattices) *Let $I$ be a finite set and a diagram of distributive lattices*

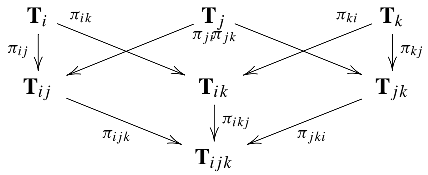
$$\big((\mathbf{T}_i)_{i \in I}, (\mathbf{T}_{ij})_{i < j \in I}, (\mathbf{T}_{ijk})_{i < j < k \in I}; (\pi_{ij})_{i \ne j}, (\pi_{ijk})_{i < j, j \ne k \ne i}\big)$$

*and a family of elements $(s_{ij})_{i \ne j \in I} \in \prod_{i \ne j \in I} \mathbf{T}_i$ satisfying the following properties:*

---

[2]In commutative algebra, a similar procedure works for $\mathbf{A}$-modules [17, XV-4.4]. But in order to glue commutative rings, it is necessary to pass to the category of Grothendieck schemes.

- *the diagram is commutative,*
- *if $i \neq j$, $\pi_{ij}$ is a quotient morphism w.r.t. the ideal $\downarrow s_{ij}$,*
- *if $i, j, k$ are distinct, $\pi_{ij}(s_{ik}) = \pi_{ji}(s_{jk})$ and $\pi_{ijk}$ is a quotient morphism w.r.t. the ideal $\downarrow \pi_{ij}(s_{ik})$.*




*Let $\big(\mathbf{T}\,;\ (\pi_i)_{i\in I}\big)$ be the limit of the diagram. Then there exist $s_i$'s in $\mathbf{T}$ such that the principal ideals $\downarrow s_i$ cover $\mathbf{T}$ and the diagram is isomorphic to the one in Fact 1. More precisely each $\pi_i$ is a quotient morphism w.r.t. the ideal $\downarrow s_i$ and $\pi_i(s_j) = s_{ij}$ for all $i \neq j$.*
*The analogous result works with quotients by principal filters.*

*Remark 1.* The reader can translate the previous result in gluing of spectral spaces.

### 1.1.3 Heitmann Lattice and J-Spectrum

An ideal $\mathfrak{m}$ of a distributive lattice $\mathbf{T}$ is *maximal* when $\mathbf{T}/(\mathfrak{m} = 0) \simeq \mathbf{2}$, i.e. if $1 \notin \mathfrak{m}$ and $\forall x \in \mathbf{T}\ (x \in \mathfrak{m}$ or $\exists y \in \mathfrak{m}\ x \vee y = 1)$.

In classical mathematics we have the following result.

**Lemma 1.** *The intersection of all maximal ideals containing an ideal $\mathfrak{J}$ is called the* Jacobson radical of $\mathfrak{J}$ *and is equal to*

$$\mathrm{J}_{\mathbf{T}}(\mathfrak{J}) = \{ a \in \mathbf{T} \mid \forall x \in \mathbf{T}\ (a \vee x = 1 \Rightarrow \exists z \in \mathfrak{J}\ \ z \vee x = 1) \}. \tag{3}$$

*We write* $\mathrm{J}_{\mathbf{T}}(b)$ *for* $\mathrm{J}_{\mathbf{T}}(\downarrow b)$. *The ideal* $\mathrm{J}_{\mathbf{T}}(0)$ *is the* Jacobson radical of $\mathbf{T}$.

In constructive mathematics, equality (3) is used as definition.

The *Heitmann lattice of* $\mathbf{T}$, denoted by $\mathsf{He}(\mathbf{T})$, is the quotient of $\mathbf{T}$ corresponding to the following preorder $\preccurlyeq_{\mathsf{He}(\mathbf{T})}$:

$$a \preccurlyeq_{\mathsf{He}(\mathbf{T})} b \ \overset{\text{def}}{\Longleftrightarrow}\ \mathrm{J}_{\mathbf{T}}(a) \subseteq \mathrm{J}_{\mathbf{T}}(b) \Longleftrightarrow a \in \mathrm{J}_{\mathbf{T}}(b). \tag{4}$$

Elements of $\mathsf{He}(\mathbf{T})$ can be identified with ideals $\mathrm{J}_{\mathbf{T}}(a)$, via the canonical map

$$\mathbf{T} \longrightarrow \mathsf{He}(\mathbf{T}), \quad a \longmapsto \mathrm{J}_{\mathbf{T}}(a).$$

The next definition follows the remarkable paper by Heitmann [14].

**Definition 2.** Let $\mathbf{T}$ be a distributive lattice.

1. The *maximal spectrum of* $\mathbf{T}$, denoted by $\mathsf{Max}\,\mathbf{T}$, is the topological subspace of $\mathsf{Spec}\,\mathbf{T}$ provided by the maximal ideals of $\mathbf{T}$.
2. The *j-spectrum of* $\mathbf{T}$, denoted by $\mathsf{jspec}\,\mathbf{T}$, is the topological subspace of $\mathsf{Spec}\,\mathbf{T}$ provided by the primes $\mathfrak{p}$ s.t. $\mathrm{J}_{\mathbf{T}}(\mathfrak{p}) = \mathfrak{p}$, i.e. the prime ideals $\mathfrak{p}$ which are intersections of maximal ideals.
3. The *Heitmann* J*-spectrum of* $\mathbf{T}$, denoted by $\mathsf{Jspec}\,\mathbf{T}$, is the adherence of $\mathsf{Max}\,\mathbf{T}$ in $\mathsf{Spec}\,\mathbf{T}$ for the patch topology. It is a spectral subspace of $\mathsf{Spec}\,\mathbf{T}$.
4. The *minimal spectrum of* $\mathbf{T}$, denoted by $\mathsf{Min}\,\mathbf{T}$, is the topological subspace of $\mathsf{Spec}\,\mathbf{T}$ provided by minimal primes of $\mathbf{T}$.

In general, $\mathsf{Max}\,\mathbf{T}$, $\mathsf{jspec}\,\mathbf{T}$ and $\mathsf{Min}\,\mathbf{T}$ are not spectral spaces.

**Theorem 2.** $\mathsf{Jspec}\,\mathbf{T}$ *is a spectral subspace of* $\mathsf{Spec}\,\mathbf{T}$ *canonically homeomorphic to* $\mathsf{Spec}\,(\mathsf{He}(\mathbf{T}))$.

## *1.2 Distributive Lattices and Entailment Relations*

A particularly important rule for distributive lattices, known as *cut*, is

$$\big(x \wedge a \ \leqslant \ b\big) \ \ \& \ \ \big(a \ \leqslant \ x \vee b\big) \quad \Longrightarrow \quad a \leqslant \ b. \tag{5}$$

For $A \in \mathrm{P_{fe}}(\mathbf{T})$ (finitely enumerated subsets of $\mathbf{T}$) we write

$$\bigvee A := \bigvee\nolimits_{x \in A} x \qquad \text{and} \qquad \bigwedge A := \bigwedge\nolimits_{x \in A} x.$$

We denote by $A \ \vdash \ B$ or $A \vdash_{\mathbf{T}} B$ the relation defined as follows over the set $\mathrm{P_{fe}}(\mathbf{T})$:

$$A \vdash B \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \bigwedge A \ \leqslant \ \bigvee B.$$

This relation satisfies the following axioms, in which we write $x$ for $\{x\}$ and $A, B$ for $A \cup B$:

$$\begin{array}{rrcll} & & a & \vdash \ a & (R) \\ A \vdash B & \Longrightarrow & A, A' & \vdash \ B, B' & (M) \\ (A, x \ \vdash \ B) \ \& \ (A \ \vdash \ B, x) & \Longrightarrow & A & \vdash \ B & (T). \end{array}$$

We say that the relation is *reflexive*, *monotone* and *transitive*. The third rule (transitivity) can be seen as a version of rule (5) and is also called the *cut* rule.

**Definition 3.** For an arbitrary set $S$, a relation over $\mathrm{P_{fe}}(S)$ which is reflexive, monotone and transitive is called an *entailment relation*.

The following theorem is fundamental. It says that the three properties of entailment relations are exactly what is needed for the interpretation in the form of a distributive lattice to be adequate.

**Theorem 3.** (Fundamental theorem of entailment relations) *[7], [17, XI-5.3], [21, Satz 7] Let $S$ be a set with an entailment relation $\vdash_S$ on $\mathrm{P_{fe}}(S)$. We consider the distributive lattice* $\mathbf{T}$ *defined by generators and relations as follows: the generators are the elements of $S$ and the relations are*

$$A \ \vdash_{\mathbf{T}} \ B$$

*each time that $A \ \vdash_S \ B$. Then, for all $A$, $B$ in $\mathrm{P_{fe}}(S)$, we have*

$$A \ \vdash_{\mathbf{T}} \ B \implies A \ \vdash_S \ B.$$

# 2 Spectral Spaces in Algebra

The usual spectral spaces in algebra are (always?) understood as spectra of distributive lattices associated to coherent theories describing relevant algebraic structures. We describe this general situation and give some examples.

## *2.1 Dynamical Algebraic Structures, Distributive Lattices and Spectra*

References: [13, 20]. The paper [13] introduces the general notion of "dynamical theory" and of "dynamical proof". See also the paper [2] which illustrates the usefulness of these notions.

### 2.1.1 Dynamical Theories and Dynamical Algebraic Structures

Dynamical theories are a version "without logic, purely computational" of *coherent theories* (we say theory for "first order formal theory").

Dynamical theories use only dynamical rules, i.e. deduction rules of the form

$$\Gamma \ \vdash \ \exists \underline{y}^1 \, \Delta_1 \ \textsf{or} \ \cdots \ \textsf{or} \ \exists \underline{y}^m \, \Delta_m,$$

where $\Gamma$ and the $\Delta_i$'s are lists of atomic formulae in the language $\mathcal{L}$ of the theory $\mathcal{T} = (\mathcal{L}, \mathcal{A})$.

The computational meaning of "$\exists y\, \Delta$" is "**Introduce** $\underline{y}$ **such that** $\Delta$". The computational meaning of "$U$ **or** $V$ **or** $W$" is "open three branches of computations …".

Axioms (elements of $\mathcal{A}$) are dynamical rules and theorems are valid dynamical rules (validity is described in a simple way and uses only a computational machinery).

A *dynamical algebraic structure* for a dynamical theory $\mathcal{T}$ is given through a presentation $(G, R)$ by generators and relations. Generators are the element of $G$ and they are added to the constants in the language. Relations are the elements of $R$. They are dynamical rules without free variables and they are added to the axioms of the theory.

A dynamical algebraic structure is intuitively thought of as an incompletely specified algebraic structure. The notion corresponds to lazy evaluation in Computer Algebra.

Purely equational algebraic structures correspond to the case where the only predicate is equality and the axioms are Horn rules.

Dynamical theories whose axioms contain neither **or** nor $\exists$ are called *Horn theories* (algebraic theories in [13]). For example, theories of absolutely flat rings and of pp-rings can be given as Horn theories.

A coherent theory is a *first order geometric theory*. In non-first order geometric theories we accept dynamical rules that use infinite disjunctions at the right of $\vdash$. In this paper we speak only of first order geometric theories.

A fundamental result about dynamical theories says that adding the classical first order logic to a dynamical theory does not change valid rules: first order classical mathematic is conservative over dynamical theories [13, Theorem 1.1].

#### 2.1.2 Distributive Lattices Associated to a Dynamical Algebraic Structure

Let $\mathbf{A} = \big((G, R), \mathcal{T}\big)$ be a dynamical algebraic structure for $\mathcal{T} = (\mathcal{L}, \mathcal{A})$.

• **First example**. If $P(x, y)$ belongs to $\mathcal{L}$ and if $Clt$ is the set of closed terms of $\mathbf{A}$, we get the following entailment relation $\vdash_{\mathbf{A},P}$ for $Clt \times Clt$:

$$\begin{array}{ccc} (a_1, b_1), \dots, (a_n, b_n) \ \vdash_{\mathbf{A},P} (c_1, d_1), \dots, (c_m, d_m) & \overset{\text{def}}{\Longleftrightarrow} & \\ P(a_1, b_1),\ \dots,\ P(a_n, b_n) \vdash_{\mathbf{A}} P(c_1, d_1) \ \textbf{or}\ \dots\ \textbf{or}\ P(c_m, d_m). & & \end{array} \tag{6}$$

Intuitively the distributive lattice $\mathbf{T}$ generated by this entailment relation represents the "truth values" of $P$ in the dynamical algebraic structure $\mathbf{A}$. In fact to give an element $\alpha : \mathbf{T} \to \mathbf{2}$ of $\mathsf{Spec}\,\mathbf{T}$ amounts to giving the value $\top$ (resp. $\bot$) to $P(a, b)$ when $\alpha(a, b) = 1$ (resp. $\alpha(a, b) = 0$).

• **Second example, the Zariski lattice of a commutative ring**. Let $\mathcal{Al}$ be a dynamical theory of nontrivial local rings, e.g. with signature

$$(\cdot = 0, \mathrm{U}(\cdot)\ ;\ \cdot + \cdot, \cdot \times \cdot, - \cdot, 0, 1\,).$$

This is an extension of the purely equational theory of commutative rings. The predicate $\mathrm{U}(x)$ is defined as meaning the invertibility of $x$,

- $\mathrm{U}(x) \ \vdash \exists y \, xy = 1$
- $xy = 1 \ \vdash \mathrm{U}(x)$

and the axioms of nontrivial local rings are written as

**AL** $\mathrm{U}(x + y) \vdash \mathrm{U}(x)$ **or** $\mathrm{U}(y)$ • $\mathrm{U}(0) \ \vdash \ \bot$

The *Zariski lattice* $\mathsf{Zar}\,\mathbf{A}$ of a commutative ring $\mathbf{A}$ is defined as the distributive lattice generated by the entailment relation $\vdash_{\mathsf{Zar}\,\mathbf{A}}$ for $\mathbf{A}$ defined as

$$\begin{array}{c} a_1, \dots, a_n \ \vdash_{\mathsf{Zar}\,\mathbf{A}} c_1, \dots, c_m \qquad \overset{\text{def}}{\Longleftrightarrow} \\ \mathrm{U}(a_1), \ \dots, \mathrm{U}(a_n) \ \vdash_{\mathcal{Al}(\mathbf{A})} \mathrm{U}(c_1) \ \textbf{or} \ \dots \ \textbf{or} \ \mathrm{U}(c_m). \end{array} \tag{7}$$

Here $\mathcal{Al}(\mathbf{A})$ is the dynamical algebraic structure of type $\mathcal{Al}$ over $\mathbf{A}$.

We get the following equivalence (we call it a *formal Nullstellensatz*):

$$a_1, \dots, a_n \vdash_{\mathsf{Zar}\,\mathbf{A}} c_1, \dots, c_m \Longleftrightarrow \exists k > 0 \ \ (a_1 \cdots a_n)^k \in \langle c_1, \dots, c_m \rangle \,.$$

So, $\mathsf{Zar}\,\mathbf{A}$ can be identified with the set of ideals $\mathrm{D}_{\mathbf{A}}(\underline{x}) = \sqrt[\mathbf{A}]{\langle \underline{x} \rangle}$, with $\mathrm{D}_{\mathbf{A}}(\mathfrak{j}_1) \wedge \mathrm{D}_{\mathbf{A}}(\mathfrak{j}_2) = \mathrm{D}_{\mathbf{A}}(\mathfrak{j}_1\mathfrak{j}_2)$ and $\mathrm{D}_{\mathbf{A}}(\mathfrak{j}_1) \vee \mathrm{D}_{\mathbf{A}}(\mathfrak{j}_2) = \mathrm{D}_{\mathbf{A}}(\mathfrak{j}_1 + \mathfrak{j}_2)$.

Now, the usual Zariski spectrum $\mathsf{Spec}\,\mathbf{A}$ is canonically homeomorphic to $\mathsf{Spec}\,(\mathsf{Zar}\,\mathbf{A})$. Indeed, to give a point of $\mathsf{Spec}\,\mathbf{A}$ (a prime ideal) amounts to giving an epimorphism $\mathbf{A} \to \mathbf{B}$ where $\mathbf{B}$ is a local ring, or also, that is the same thing, to giving a minimal model of $\mathcal{Al}(\mathbf{A})$. This corresponds to the intuition of "forcing the ring to be a local ring".

• **More generally.** Let us consider a set $S$ of closed atomic formulae of the dynamical algebraic structure $\mathbf{A} = \big((G, R), \mathcal{T}\big)$. We define a corresponding entailment relation (with the $A_i$'s and $B_j$'s in $S$):

$$\begin{array}{c} A_1, \dots, A_n \ \vdash_{\mathbf{A},S} B_1, \dots, B_m \qquad \overset{\text{def}}{\Longleftrightarrow} \\ A_1, \ \dots, A_n \ \vdash_{\mathbf{A}} B_1 \ \textbf{or} \ \dots \ \textbf{or} \ B_m. \end{array} \tag{8}$$

We may denote by $\mathsf{Zar}(\mathbf{A}, S)$ this distributive lattice.

• **Points of a spectrum and models in classical mathematics.** With a good choice of predicates in the language, to give a point of the spectrum of the corresponding lattice amounts often to giving a minimal model of the dynamical algebraic structure. This is the case when all existence axioms in the theory imply unique existence. The topology of the spectrum is in any case strongly dependent on the choice of predicates.

• **The complete Zarisiki lattice of a dynamical algebraic structure A** is defined by choosing for $S$ the set $Clat(\mathbf{A})$ of all closed atomic formulas of $\mathbf{A}$. When the theory has no existential axioms, this lattice corresponds to the entailment relation for $Clat(\mathbf{A})$ generated by the axioms of $\mathcal{T}$, replacing the variables by arbitrary closed terms of $\mathbf{A}$.

## 2.2 A Very Simple Case

Let $\mathcal{T}$ be a Horn theory. Any dynamical algebraic structure $\mathbf{A} = ((G, R), \mathcal{T})$ of type $\mathcal{T}$ defines an ordinary algebraic structure $\mathbf{B}$ and there is no significant difference between dynamical algebraic structures and ordinary algebraic structures.

The minimal models of $\mathbf{A}$ are (identified with) the quotient structures $\mathbf{C} = \mathbf{B}/\!\sim$. If we choose convenient predicates for defining a distributive lattice associated to $\mathbf{B}$, the points of the corresponding spectrum are (identified with) these quotient structures.

For example, in the case of the purely equational theory $\mathcal{T} = \mathcal{M}od_{\mathbf{A}}$ (the theory of modules over a fixed ring $\mathbf{A}$), and choosing the predicate $x = 0$ (or the predicate $x \neq 0$), we get the lattice generated by the following entailment relation for an $\mathbf{A}$-module $M$:

- $x_1 = 0, \ldots, x_n = 0 \ \vdash y_1 = 0$ **or** $\ldots$ **or** $y_m = 0$,

or by

- $y_1 \neq 0, \ldots, y_m \neq 0 \ \vdash x_1 \neq 0$ **or** $\ldots$ **or** $x_n \neq 0$,

which means "*one* $y_j$ *is in the submodule* $\langle x_1, \ldots, x_n \rangle$" (formal Nullstellensatz for linear algebra).

Here the points of the spectrum are (identified with) submodules of $M$ and a basic open (or a basic closed) set $\mathfrak{D}(a)$ is the set of submodules containing $a$.

It might be that these kinds of lattices and spectra are too simple to lead to interesting results in algebra.

## 2.3 The Real Spectrum of a Commutative Ring

The real spectrum $\mathsf{Sper}\,\mathbf{A}$ of a commutative ring corresponds to the intuition of "forcing the ring $\mathbf{A}$ to be an ordered (discrete[3])" field.

A point of $\mathsf{Sper}\,\mathbf{A}$ can be given as an epimorphism $\varphi : \mathbf{A} \to \mathbf{K}$, where $(\mathbf{K}, \mathbf{C})$ is an ordered field.[4] Moreover two such morphisms $\varphi : \mathbf{A} \to \mathbf{K}$ and $\varphi' : \mathbf{A} \to \mathbf{K}'$ define the same point of the spectrum if there exists an isomorphism of ordered fields $\psi : \mathbf{K} \to \mathbf{K}'$ making the suitable diagram commutative.

[3] We ask the order relation to be decidable.

[4] $\mathbf{C}$ is the cone of nonnegative elements.

We write "$x \geq 0$" the predicate over $\mathbf{A}$ corresponding to "$\varphi(x) \geq 0$ in $\mathbf{K}$". We get the following axioms:

- $\vdash x^2 \geq 0$
- $x \geq 0, y \geq 0 \ \vdash x + y \geq 0$
- $x \geq 0, y \geq 0 \ \vdash xy \geq 0$
- $-1 \geq 0 \ \vdash \bot$
- $-xy \geq 0 \ \vdash x \geq 0$ **or** $y \geq 0$

This means that $\{ x \in \mathbf{A} \mid x \geq 0 \}$ is a prime cone: to give a model of this theory is the same thing as to give a point of $\mathsf{Sper}\,\mathbf{A}$.

In order to get the usual topology of $\mathsf{Sper}\,\mathbf{A}$, it is necessary to use the opposite predicate $x < 0$. For the sake of comfort, we take $x > 0$. This predicate satisfies the dual axioms to those for $-x \geq 0$:

- $-x^2 > 0 \ \vdash \bot$
- $x + y > 0 \ \vdash x > 0$ **or** $y > 0$
- $xy > 0 \ \vdash x > 0$ **or** $-y > 0$
- $\vdash 1 > 0$
- $x > 0, y > 0 \ \vdash xy > 0$

So the *real lattice* of $\mathbf{A}$, denoted by $\mathsf{Real}(\mathbf{A})$, is the distributive lattice generated by the minimal entailment relation for $\mathbf{A}$ satisfying the following relations (we write $\mathrm{R}(a)$ instead of $a$):

- $\mathrm{R}(-x^2) \vdash$
- $\mathrm{R}(x + y) \vdash \mathrm{R}(x), \mathrm{R}(y)$
- $\mathrm{R}(xy) \vdash \mathrm{R}(x), \mathrm{R}(-y)$
- $\vdash \mathrm{R}(1)$
- $\mathrm{R}(x), \mathrm{R}(y) \vdash \mathrm{R}(xy)$

So $\mathsf{Spec}\,(\mathsf{Real}\,\mathbf{A})$ is isomorphic to $\mathsf{Sper}\,\mathbf{A}$, viewed as the set of prime cones of $\mathbf{A}$. The spectral topology admits the basis of open sets

$$\mathfrak{R}(a_1, \ldots, a_n) = \left\{ \mathfrak{c} \in \mathsf{Sper}\,\mathbf{A} \mid \&_{i=1}^{n} - a_i \notin \mathfrak{c} \right\}.$$

This approach to the real spectrum was proposed in [7].

An important point is the following *formal Positivstellensatz.*

**Theorem 4.** (Formal Positivstellensatz for ordered fields) *T.F.A.E.*

1. *We have* $\mathrm{R}(x_1), \ldots, \mathrm{R}(x_k) \vdash \mathrm{R}(a_1), \ldots, \mathrm{R}(a_n)$ *in the lattice* $\mathsf{Real}\,\mathbf{A}$.
2. *We have* $x_1 > 0, \ldots, x_k > 0 \ \vdash a_1 > 0$ ***or*** $\ldots$ ***or*** $a_n > 0$ *in the theory of ordered fields over* $\mathbf{A}$.
3. *We have* $x_1 > 0, \ldots, x_k > 0, a_1 \leq 0, \ldots, a_n \leq 0 \ \vdash \bot$ *in the theory of ordered fields over* $\mathbf{A}$.
4. *We have an equality* $s + p = 0$ *in* $\mathbf{A}$, *with* $s$ *in the monoid generated by the* $x_i$*'s and* $p$ *in the cone generated by the* $x_i$*'s and the* $-a_j$*'s.*

## 2.4 Linear Spectrum of a Lattice-Group

The theory of lattice-groups, denoted by $\mathcal{L}gr$, is a purely equational theory over the signature $(\cdot = 0; \cdot + \cdot, -\cdot, \cdot \vee \cdot, 0)$. The following rules express that $\vee$ defines a join semilattice and the compatibility of $\vee$ with $+$:

| | | | |
|---|---|---|---|
| **sdt1** | $\vdash x \vee x = x$ | **sdt3** | $\vdash (x \vee y) \vee z = x \vee (y \vee z)$ |
| **sdt2** | $\vdash x \vee y = y \vee x$ | **grl** | $\vdash x + (y \vee z) = (x + y) \ \vee \ (x + z)$ |

We get the theory $\mathcal{L}iog$ by adding to $\mathcal{L}gr$ the axiom $\vdash x \geq 0$ **or** $-x \geq 0$.

The linear spectrum of an $\ell$-group $\Gamma$ corresponds to the intuition of "forcing the group to be linearly ordered". So a point of this spectrum can be given as a minimal model of the dynamical algebraic structure $\mathcal{L}iog(\Gamma)$, or equivalently by a linearly ordered group $G$ quotient of $\Gamma$, or as the kernel $H$ of the canonical morphism $\pi : \Gamma \to G$. This subgroup $H$ is a *prime solid subgroup* of $\Gamma$.

The *linear lattice* of $\Gamma$, denoted by $\mathsf{Liog}(\Gamma)$, is generated by the entailment relation for $\Gamma$ defined in the following way:

$$a_1, \ldots, a_n \ \vdash_{\mathsf{Liog}\,\Gamma} \ b_1, \ldots, b_m \qquad \overset{\text{def}}{\Longleftrightarrow}$$
$$a_1 \geq 0\textbf{,} \ \ldots\textbf{,} \ a_n \geq 0 \ \vdash_{\mathcal{L}iog\,\Gamma} \ b_1 \geq 0 \ \textbf{or} \ \ldots \ \textbf{or} \ b_m \geq 0.$$

The spectral space previously defined is (isomorphic to) $\mathsf{Spec}\,(\mathsf{Liog}\,\Gamma)$. We have a *formal Positivstellensatz* for this entailment relation $(m, n \neq 0)$.

$$a_1, \ldots, a_n \vdash_{\mathsf{Liog}(\Gamma)} b_1, \ldots, b_m \iff \exists k > 0 \ (b_1^- \wedge \ldots \wedge b_m^-) \leq k(a_1^- \vee \ldots \vee a_n^-).$$

## 2.5 Valuative Spectrum of a Commutative Ring

The valuative spectrum $\mathsf{Spev}\,\mathbf{A}$ of a commutative ring corresponds to the intuition of "forcing the ring to be a valued field". A point of this spectrum is given by an epimorphism $\varphi : \mathbf{A} \to \mathbf{K}$ where $(\mathbf{K}, \mathbf{V})$ is a valued field.[5] Moreover two such morphisms $\varphi : \mathbf{A} \to \mathbf{K}$ and $\varphi' : \mathbf{A} \to \mathbf{K}'$ define the same point of the spectrum if there exists an isomorphism of valued fields $\psi : \mathbf{K} \to \mathbf{K}'$ making the suitable diagram commutative.

We denote by $x \mid y$ the predicate over $\mathbf{A} \times \mathbf{A}$ corresponding to "$\varphi(x)$ divides[6] $\varphi(y)$ in $\mathbf{K}$". We get the following axioms:

---

[5] $\mathbf{V}$ is a valuation ring of $\mathbf{K}$.

[6] That is, $\exists z \in \mathbf{V}\ z\varphi(x) = \varphi(y)$.

- $\vdash 1 \mid 0$
- $\vdash -1 \mid 1$
- $a \mid b \ \vdash ac \mid bc$
- $\vdash a \mid b$ **or** $b \mid a$
- $0 \mid 1 \ \vdash \bot$
- $a \mid b, b \mid c \ \vdash a \mid c$
- $a \mid b, a \mid c \ \vdash a \mid b + c$
- $ax \mid bx \ \vdash a \mid b$ **or** $0 \mid x$

Any predicate $x \mid y$ over $\mathbf{A} \times \mathbf{A}$ satisfying these axioms defines a point in $\mathsf{Spev}\,\mathbf{A}$. So we define the *valuative lattice* of $\mathbf{A}$, denoted by $\mathsf{Val}(\mathbf{A})$ as generated by the minimal entailment relation for $\mathbf{A} \times \mathbf{A}$ satisfying the following relations:

- $\vdash (1, 0)$
- $\vdash (-1, 1)$
- $(a, b) \vdash (ac, bc)$
- $\vdash (a, b), (b, a)$
- $(0, 1) \vdash$
- $(a, b), (b, c) \vdash (a, c)$
- $(a, b), (a, c) \vdash (a, b + c)$
- $(ax, bx) \vdash (a, b), (0, x)$

The two spectral spaces $\mathsf{Spec}\,(\mathsf{Val}\,\mathbf{A})$ and $\mathsf{Spev}\,\mathbf{A}$ can be identified. The spectral topology of $\mathsf{Spec}\,(\mathsf{Val}\,\mathbf{A})$ is generated by the basic open sets $\mathfrak{U}\big((a, b)\big) = \{\, \varphi \in \mathsf{Spev}\,\mathbf{A} \mid \varphi(a) \mid \varphi(b) \,\}$.

We have a formal Valuativstellensatz.

**Theorem 5.** (Formal Valuativstellensatz for valued fields) *Let* $\mathbf{A}$ *be a commutative ring, t.f.a.e.*

1. *One has* $(a_1, b_1), \dots, (a_n, b_n) \ \vdash \ (c_1, d_1), \dots, (c_m, d_m)$ *in the lattice* $\mathsf{Val}\,\mathbf{A}$.
2. *Introducing indeterminates* $x_i$*'s* ($i \in [\![1..n]\!]$) *and* $y_j$*'s* ($j \in [\![1..m]\!]$) *we have in the ring* $\mathbf{A}[\underline{x}, \underline{y}]$ *an equality*

$$d\big(1 + \sum\nolimits_{j=1}^{m} y_j P_j(\underline{x}, \underline{y})\big) \in \big\langle (x_i a_i - b_i)_{i \in [\![1..n]\!]}, (y_j d_j - c_j)_{j \in [\![1..m]\!]} \big\rangle,$$

*where* $d$ *is in the monoid generated by the* $d_j$*'s and the* $P_j(x_1, \dots, x_n, y_1, \dots, y_m)$*'s are in* $\mathbb{Z}[\underline{x}, \underline{y}]$.

## *2.6 Heitmann Lattice and J-Spectrum of a Commutative Ring*

In a commutative ring the *Jacobson radical of an ideal* $\mathfrak{J}$ denoted by $\mathrm{J}_{\mathbf{A}}(\mathfrak{J})$ is defined in classical mathematics as the intersection of the maximal ideals containing $\mathfrak{J}$. In constructive mathematics we use the classically equivalent definition

$$\mathrm{J}_{\mathbf{A}}(\mathfrak{J}) \overset{\text{def}}{=} \{\, x \in \mathbf{A} \mid \forall y \in \mathbf{A}, \quad 1 + xy \text{ is invertible modulo } \mathfrak{J} \,\}. \tag{9}$$

We write $\mathrm{J}_{\mathbf{A}}(x_1, \dots, x_n)$ for $\mathrm{J}_{\mathbf{A}}(\langle x_1, \dots, x_n \rangle)$. The ideal $\mathrm{J}_{\mathbf{A}}(0)$ is called *the Jacobson radical of* $\mathbf{A}$.

The *Heitmann lattice of* $\mathbf{A}$ is $\mathsf{He}(\mathsf{Zar}\,\mathbf{A})$, denoted by $\mathsf{Heit}\,\mathbf{A}$; it is a quotient of $\mathsf{Zar}\,\mathbf{A}$. In fact $\mathsf{Heit}\,\mathbf{A}$ can be identified with the set of ideals $\mathrm{J}_{\mathbf{A}}(x_1,\dots,x_n)$, with $\mathrm{J}_{\mathbf{A}}(\mathfrak{j}_1) \wedge \mathrm{J}_{\mathbf{A}}(\mathfrak{j}_2) = \mathrm{J}_{\mathbf{A}}(\mathfrak{j}_1\mathfrak{j}_2)$ and $\mathrm{J}_{\mathbf{A}}(\mathfrak{j}_1) \vee \mathrm{J}_{\mathbf{A}}(\mathfrak{j}_2) = \mathrm{J}_{\mathbf{A}}(\mathfrak{j}_1 + \mathfrak{j}_2)$.

We denote by $\mathsf{Jspec}(\mathbf{A})$ the spectral space $\mathsf{Spec}\,(\mathsf{Heit}\,\mathbf{A})$. In classical mathematics it is the adherence (for the patch topology) of the maximal spectrum in $\mathsf{Spec}\ \mathbf{A}$. We call it the (Heitmann) J-spectrum of $\mathbf{A}$. It is a subspectral space of $\mathsf{Spec}\ \mathbf{A}$. When $\mathbf{A}$ is Noetherian, $\mathsf{Jspec}(\mathbf{A})$ coincides with the subspace $\mathsf{jspec}(\mathbf{A})$ of $\mathsf{Spec}\ \mathbf{A}$ made of the prime ideals which are intersections of maximal ideals.

*Remark.* $\mathrm{J}_{\mathbf{A}}(x_1,\dots,x_n)$ is a radical ideal but not generally the nilradical of a finitely generated ideal. ■

## 3 A Short Dictionary

References: [1, Theorem IV-2.6], [7, 11].

In this section we consider the following context: $f : \mathbf{T} \to \mathbf{T}'$ is a morphism of distributive lattices and $\mathsf{Spec}\,(f)$, denoted by $f^\star : X' = \mathsf{Spec}\,\mathbf{T}' \to X = \mathsf{Spec}\,\mathbf{T}$, is the dual morphism.

### *3.1 Properties of Morphisms*

**Theorem 6.** ([1, Theorem IV-2.6]) *In classical mathematics we have the following equivalences:*

1. *$f^\star$ is onto ($f$ is lying over) $\iff$ $f$ is injective $\iff$ $f$ is a monomorphism $\iff$ $f^\star$ is an epimorphism.*
2. *$f$ is an epimorphism $\iff$ $f^\star$ is a monomorphism $\iff$ $f^\star$ is injective.*
3. *$f$ is onto*[7] *$\iff$ $f^\star$ is an isomorphism on its image, which is a subspectral space of $X$.*

There are bijective morphisms of spectral spaces that are not isomorphisms. For example, the morphism $\mathsf{Spec}\,(\mathbb{B}\mathrm{o}(\mathbf{T})) \to \mathsf{Spec}\,\mathbf{T}$ is rarely an isomorphism and the lattice morphism $\mathbf{T} \to \mathbb{B}\mathrm{o}(\mathbf{T})$ is an injective epimorphism which is rarely onto.

**Lemma 2.** *Let $S$ be a system of generators for $\mathbf{T}$. The morphism $f$ is lying over if and only if for all $a_1,\dots,a_n,b_1,\dots,b_m \in S$ we have*

$$f(a_1),\dots,f(a_n) \ \vdash_{\mathbf{T}'} f(b_1),\dots,f(b_m) \ \ \Rightarrow \ \ a_1,\dots,a_n \ \vdash_{\mathbf{T}} b_1,\dots,b_m.$$

**Proposition 2.** (Going up vs. lying over) *In classical mathematics t.f.a.e. (see [11]):*

1. *For each prime ideal $\mathfrak{q}$ of $\mathbf{T}'$ and $\mathfrak{p} = f^{-1}(\mathfrak{q})$, the morphism $f' : \mathbf{T}/(\mathfrak{p} = 0) \to \mathbf{T}'/(\mathfrak{q} = 0)$ is lying over.*

[7] In other words, $f$ is a quotient morphism.

2. *For each ideal $I$ of $\mathbf{T}'$ and $J := f^{-1}(I)$, the morphism $f_I : \mathbf{T}/(J = 0) \to \mathbf{T}'/(I = 0)$ is lying over.*
3. *For each $y \in \mathbf{T}'$ and $J = f^{-1}(\downarrow y)$, the morphism $f_y : \mathbf{T}/(J = 0) \to \mathbf{T}'/(y = 0)$ is lying over.*
4. *For each $a, c \in \mathbf{T}$ and $y \in \mathbf{T}'$ we have*

$$f(a) \vdash_{\mathbf{T}'} f(c),\ y \quad \Longrightarrow \quad \exists x \in \mathbf{T} \quad a \vdash_{\mathbf{T}} c,\ x \quad \text{and} \quad f(j) \leq_{\mathbf{T}'} x.$$

**Theorem 7.** *In classical mathematics we have the following equivalences [11]:*

1. *$f$ is going up $\Longleftrightarrow$ for each $a, c \in \mathbf{T}$ and $y \in \mathbf{T}'$ we have*

$$f(a) \leq f(c) \vee y \ \Rightarrow\ \exists x \in \mathbf{T}\ (a \leq c \vee x \text{ and } f(x) \leq y).$$

2. *$f$ is going down $\Longleftrightarrow$ for each $a, c \in \mathbf{T}$ and $y \in \mathbf{T}'$ we have*

$$f(a) \geq f(c) \wedge y \ \Rightarrow\ \exists x \in \mathbf{T}\ (a \geq c \wedge x \text{ and } f(x) \geq y).$$

3. *$f$ has the property of incomparability $\Longleftrightarrow$ $f$ is zero-dimensional.*[8]

**Theorem 8.** *In classical mathematics t.f.a.e.*

1. $\mathsf{Spec}\,(f)$ *is an open map.*
2. *There exists a map $\widetilde{f} : \mathbf{T}' \to \mathbf{T}$ with the following properties:*
   (a) *For $c \in \mathbf{T}$ and $b \in \mathbf{T}'$, one has $b \leq f(c) \Leftrightarrow \widetilde{f}(b) \leq c$.*
   *In particular, $b \leq f(\widetilde{f}(b))$ and $\widetilde{f}(b_1 \vee b_2) = \widetilde{f}(b_1) \vee \widetilde{f}(b_2)$.*
   (b) *For $a, c \in \mathbf{T}$ and $b \in \mathbf{T}'$, one has $f(a) \wedge b \leq f(c) \Leftrightarrow a \wedge \widetilde{f}(b) \leq c$.*
   (c) *For $a \in \mathbf{T}$ and $b \in \mathbf{T}'$, one has $\widetilde{f}(f(a) \wedge b) = a \wedge \widetilde{f}(b)$.*
   (d) *For $a \in \mathbf{T}$, one has $\widetilde{f}(f(a)) = \widetilde{f}(1) \wedge a$.*
3. *There exists a map $\widetilde{f} : \mathbf{T}' \to \mathbf{T}$ satisfying property 2b.*
4. *For $b \in \mathbf{T}$ the g.l.b. $\bigwedge_{b \leq f(c)} c$ exists, and if we write it $\widetilde{f}(b)$, the property 2b holds.*

For this result in locales' theory see [5, Section 1.6]. We give now a proof for spectral spaces. Implications concerning item *1* need classical mathematics. The other equivalences are constructive.

**Lemma 3.** *Let $f : A \to A'$ be a nondecreasing map between ordered sets $(A, \leq)$ and $(A', \leq')$ and $b \in A'$. An element $b_1 \in A$ satisfies the equivalence*

$$\forall x \in A \ \ (b \leq' f(x) \iff b_1 \leq x)$$

[8] See Theorem 10.

*if and only if*

- *on the one hand* $b \le' f(b_1)$,
- *and on the other hand* $b_1 = \bigwedge_{x:b \le' f(x)} x$.

*In particular, if* $b_1$ *exists, it is uniquely determined.*

*Proof.* If $b_1$ satisfies the equivalence, one has $b \le' f(b_1)$ since $b_1 \le b_1$. If $z \in A$ satisfies the implication $\forall x \in A\ (b \le' f(x) \Rightarrow z \le x)$, we get $z \le b_1$ since $b \le' f(b_1)$. So when $b_1$ satisfies the equivalence it is the maximum of $S_b \overset{\text{def}}{=} \bigcap_{b \le' f(x)} \downarrow x \subseteq A$, i.e. the g.l.b. of $\{ x \in A \mid b \le' f(x) \}$. Conversely, if such a g.l.b. $b_1$ exists, it satisfies the implication $\forall x \in A\ (b \le' f(x) \Rightarrow b_1 \le x)$ since $b_1 \in S_b$. Moreover, if $b \le' f(b_1)$ we have the converse implication $\forall x \in A\ (b_1 \le x \Rightarrow b \le' f(x))$ because if $b_1 \le x$ then $b \le' f(b_1) \le' f(x)$.

*Proof of Theorem 8. 3* $\Rightarrow$ *2.* The property *2a* is the particular case of *2b* with $a = 1$. The property *2d* is the particular case of *2c* with $b = 1$. It remains to see that *2b* implies *2c*. Indeed

$$\begin{aligned} \widetilde{f}(f(a) \wedge b) &= \bigwedge\nolimits_{c: f(a) \wedge b \le f(c)} c \quad \text{(Lemma 3)} \\ &= \bigwedge\nolimits_{c: a \wedge \widetilde{f}(b) \le c} c \quad \text{(item 2b)} \\ &= a \wedge \widetilde{f}(b) \end{aligned}$$

*1* $\Rightarrow$ *3.* We assume the map $f^\star : \mathsf{Spec}\,\mathbf{T}' \to \mathsf{Spec}\,\mathbf{T}$ to be open. If $b \in \mathbf{T}'$, the quasi-compact open set $\mathfrak{D}_{\mathbf{T}'}(b) = \mathfrak{B}$ has as image a quasi-compact open set of $\mathbf{T}$, written as $f^\star(\mathfrak{B}) = \mathfrak{D}_{\mathbf{T}}(\widetilde{b})$ for a unique $\widetilde{b} \in \mathbf{T}$. We write $\widetilde{b} = \widetilde{f}(b)$ and we get a map $\widetilde{f} : \mathbf{T}' \to \mathbf{T}$.

It remains to see that item *2b* is satisfied. For $a, c \in \mathbf{T}$ let us write $\mathfrak{A} = \mathfrak{D}_{\mathbf{T}}(a)$, $\mathfrak{C} = \mathfrak{D}_{\mathbf{T}}(c)$ and $g = f^\star$. We have to prove the equivalence *2b*, written as

$$g^{-1}(\mathfrak{A}) \cap \mathfrak{B} \subseteq g^{-1}(\mathfrak{C}) \iff \mathfrak{A} \cap g(\mathfrak{B}) \subseteq \mathfrak{C}.$$

For the direct implication, we consider an $x \in \mathfrak{B}$ such that $g(x) \in \mathfrak{A}$. We have to show that $g(x) \in \mathfrak{C}$. But $x \in g^{-1}(\mathfrak{A}) \cap \mathfrak{B}$, so $x \in g^{-1}(\mathfrak{C})$, i.e. $g(x) \in \mathfrak{C}$.

For the converse implication, we transform the r.h.s. by $g^{-1}$. This operation respects inclusion and intersection. We get $g^{-1}(\mathfrak{A}) \cap g^{-1}(g(\mathfrak{B})) \subseteq g^{-1}(\mathfrak{C})$ and we conclude by noticing that $\mathfrak{B} \subseteq g^{-1}(g(\mathfrak{B}))$.

*2* $\Rightarrow$ *1.* We show that $f^\star(\mathfrak{D}_{\mathbf{T}'}(b)) = \mathfrak{D}_{\mathbf{T}}(\widetilde{f}(b))$.
First we show $f^\star(\mathfrak{D}_{\mathbf{T}'}(b)) \subseteq \mathfrak{D}_{\mathbf{T}}(\widetilde{f}(b))$. Let $\mathfrak{p}' \in \mathsf{Spec}\,\mathbf{T}'$ with $b \notin \mathfrak{p}'$ and let

$$\mathfrak{p} = f^\star(\mathfrak{p}') = f^{-1}(\mathfrak{p}').$$

If one had $\widetilde{f}(b) \in \mathfrak{p}$ one would have $f(\widetilde{f}(b)) \in f(\mathfrak{p}) \subseteq \mathfrak{p}'$ and since $b \le f(\widetilde{f}(b))$, $b \in \mathfrak{p}'$. So we have $\mathfrak{p} \in \mathfrak{D}_{\mathbf{T}}(\widetilde{f}(b))$.

For the reverse inclusion, let us consider a $\mathfrak{p} \in \mathfrak{D}_{\mathbf{T}}(\widetilde{f}(b))$. As $\widetilde{f}$ is nondecreasing and respects $\vee$, the inverse image $\mathfrak{q} = \widetilde{f}^{-1}(\mathfrak{p})$ is an ideal.

We have $b \notin \mathfrak{q}$ because if $b \in \mathfrak{q}$ we have $\widetilde{f}(b) \in \widetilde{f}(\widetilde{f}^{-1}(\mathfrak{p})) \subseteq \mathfrak{p}$.
If $y \in \mathfrak{q}$ then $\widetilde{f}(y) = z \in \mathfrak{p}$ so $y \le f(z)$ for a $z \in \mathfrak{p}$ (item *2a*). Conversely if $y \le f(z)$ for a $z \in \mathfrak{p}$, then $\widetilde{f}(y) \le \widetilde{f}(f(z)) \le z$ (item *2d*), so $\widetilde{f}(y) \in \mathfrak{p}$. So we get

$$\mathfrak{q} = \widetilde{f}^{-1}(\mathfrak{p}) = \left\{ y \in \mathbf{T}' \mid \exists z \in \mathfrak{p} \ \ y \le f(z) \right\}.$$

So $f^{-1}(\mathfrak{q}) = \{ x \in \mathbf{T} \mid \exists z \in \mathfrak{p} \ \ f(x) \le f(z) \}$. But $f(x) \le f(z)$ is equivalent to $x \wedge \widetilde{f}(1) \le z$ (item 2b with $b = 1$). Moreover $\widetilde{f}(1) \notin \mathfrak{p}$ since $\widetilde{f}(b) \le \widetilde{f}(1)$ and $\widetilde{f}(b) \notin \mathfrak{p}$. So

$$f^{-1}(\mathfrak{q}) = \left\{ x \in \mathbf{T} \;\middle|\; \exists z \in \mathfrak{p} \ \ x \wedge \widetilde{f}(1) \le z \right\} = \left\{ x \in \mathbf{T} \;\middle|\; x \wedge \widetilde{f}(1) \in \mathfrak{p} \right\} = \mathfrak{p}.$$

Nevertheless it is possible that $\mathfrak{q}$ be not a prime ideal. In this case let us consider an ideal $\mathfrak{q}'$ which is maximal among those satisfying $f^{-1}(\mathfrak{q}') = \mathfrak{p}$ and $\widetilde{f}(b) \notin \mathfrak{q}'$. We want to show that $\mathfrak{q}'$ is prime. Assume we have $y_1$ and $y_2 \in \mathbf{T}' \setminus \mathfrak{q}'$ such that $y = y_1 \wedge y_2 \in \mathfrak{q}'$. By maximality there is an element $z_i \in \mathbf{T} \setminus \mathfrak{p}$ such that $f(z_i)$ is in the ideal generated by $\mathfrak{q}'$ and $y_i$ $(i = 1, 2)$, i.e. $f(z_i) \le x_i \vee y_i$ with $x_i \in \mathfrak{q}'$. Taking $z = z_1 \wedge z_2$ (it is in $\mathbf{T} \setminus \mathfrak{p}$) and $x = x_1 \vee x_2$ we get $f(z_i) \le x \vee y_i$ and $f(z) = f(z_1) \wedge f(z_2) \le x \vee y_i$, so $f(z) \le x \vee y \in \mathfrak{q}'$, and finally $z \in f^{-1}(\mathfrak{q}') = \mathfrak{p}$: a contradiction.
*4* $\Leftrightarrow$ *3*. Use Lemma 3 by noticing that *2b* implies *2a*.

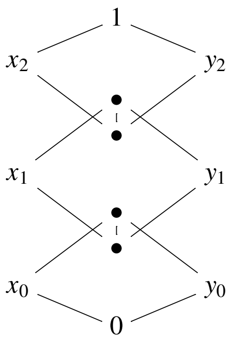
## 3.2 Dimension Properties

**Theorem 9.** (Dimension of spaces, see [12, 18], [17, Chapter XIII]) *In classical mathematics t.f.a.e.*

1. *The spectral space* $\mathsf{Spec}\,(\mathbf{T})$ *is of Krull dimension* $\le n$ *(with the meaning of chains of primes).*
2. *For each sequence* $(x_0, \dots, x_n)$ *in* $\mathbf{T}$ *there exists a* complementary sequence $(y_0, \dots, y_n)$*, which means*

$$\left.\begin{array}{rcl} 1 & \vdash & y_n, x_n \\ y_n, x_n & \vdash & y_{n-1}, x_{n-1} \\ \vdots & \vdots & \vdots \\ y_1, x_1 & \vdash & y_0, x_0 \\ y_0, x_0 & \vdash & 0 \end{array}\right\} \tag{10}$$

For example, for the dimension $n \le 2$, the inequalities in (10) correspond to the following diagram in $\mathbf{T}$:



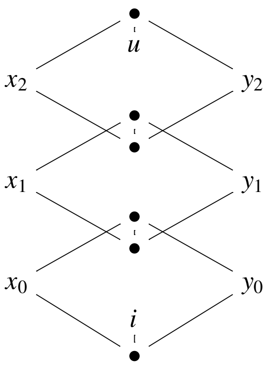

A zero-dimensional distributive lattice is a Boolean algebra.

**Theorem 10.** (Dimension of morphisms, see [11], [17, Section XIII-7]) *Let* $\mathbf{T} \subseteq \mathbf{T}'$ *and* $f$ *be the inclusion morphism. In classical mathematics t.f.a.e.*

1. *The morphism* $\mathsf{Spec}\,(f) : \mathsf{Spec}\,(\mathbf{T}') \to \mathsf{Spec}\,(\mathbf{T})$ *has Krull dimension* $\leq n$.
2. *For any sequence* $(x_0, \dots, x_n)$ *in* $\mathbf{T}'$ *there exists an integer* $k \geq 0$ *and elements* $a_1, \dots, a_k \in \mathbf{T}$ *such that for each partition* $(H, H')$ *of* $\{1, \dots, k\}$*, there exist* $y_0, \dots, y_n \in \mathbf{T}'$ *such that*

$$\begin{array}{rcl} \bigwedge_{j \in H'} a_j & \vdash & y_n,\ x_n \\ y_n,\ x_n & \vdash & y_{n-1},\ x_{n-1} \\ \vdots\ \vdots & & \vdots \\ y_1,\ x_1 & \vdash & y_0,\ x_0 \\ y_0,\ x_0 & \vdash & \bigvee_{j \in H} a_j \end{array} \tag{11}$$

For example, for the relative dimension $n \leq 2$, the inequalities in (11) correspond to the following diagram in $\mathbf{T}$, with $u = \bigwedge_{j \in H'} a_j$ and $i = \bigvee_{j \in H} a_j$:




Note that the dimension of the morphism $\mathbf{T} \to \mathbf{T}'$ is less than or equal to the dimension of $\mathbf{T}'$: take $k = 0$ in item *2*.

The Krull dimension of a ring **A** and of a morphism $\varphi : \mathbf{A} \to \mathbf{B}$ are those of $\mathsf{Zar}\,\mathbf{A}$ and $\mathsf{Zar}\,\varphi$.

A commutative ring **A** is zero-dimensional when for each $a \in \mathbf{A}$ there exist $n \in \mathbb{N}$ and $x \in \mathbf{A}$ such that $x^n(1 - xa) = 0$. A reduced zero-dimensional ring[9] is a ring in which any element $a$ has a *quasi-inverse* $b = a^\bullet$, i.e. such that $aba = a$ and $bab = b$.

Let $\mathbf{A}^\bullet$ the reduced zero-dimensional ring generated by **A**. Then the Krull dimension of a morphism $\rho : \mathbf{A} \to \mathbf{B}$ equals the Krull dimension of the ring $\mathbf{A}^\bullet \otimes_{\mathbf{A}} \mathbf{B}$.

### 3.3 Properties of Spaces

The spectral space $\mathsf{Spec}\ \mathbf{T}$ is said to be *normal* if any prime ideal of **T** is contained in a unique maximal ideal.

**Theorem 11.** *We have the following equivalences:*

1. *The spectral space* $\mathsf{Spec}\,(\mathbf{T})$ *is normal* $\iff$
   *for each* $x \vee y = 1$ *in* **T** *there exist* $a, b$ *such that* $a \vee x = b \vee y = 1$ *and* $a \wedge b = 0$.
2. *In the spectral space* $\mathsf{Spec}\,(\mathbf{T})$ *each quasi-compact open set is a finite union of irreducible quasi-compact open sets* $\iff$
   *the distributive lattice* **T** *is constructed from a dynamical algebraic structure where all axioms are Horn rules (e.g. this is the case for purely equational theories).*

## 4 Some Examples

We give in this section constructive versions of classical theorems. Often, the theorem has exactly the same wording as the classical one. But now, these theorems have a clear computational content, which was impossible when using classical definitions. Sometimes the new theorem is stronger than the previously known classical results (e.g. Theorems 17 or 18 or 19).

### 4.1 Relative Dimension, Lying Over, Going Up, Going Down

See [11] and [17, Section XIII-9].

**Theorem 12.** *Let* $\rho : \mathbf{A} \to \mathbf{B}$ *be a morphism of commutative rings or distributive lattices. If* $\mathsf{Kdim}\ \mathbf{A} \le m$ *and* $\mathsf{Kdim}\ \rho \le n$*, then* $\mathsf{Kdim}\ \mathbf{B} \le (m+1)(n+1) - 1$.

[9] Such a ring is also called absolutely flat or von Neumann regular.

**Theorem 13.** *If a morphism $\alpha : \mathbf{A} \to \mathbf{B}$ of distributive lattices or of commutative rings is lying over and going up (or lying over and going down) one has* $\mathsf{Kdim}(\mathbf{A}) \leq \mathsf{Kdim}(\mathbf{B})$.

**Lemma 4.** *Let $\rho : \mathbf{A} \to \mathbf{B}$ be a morphism of commutative rings. If $\mathbf{B}$ is generated by primitively algebraic elements*[10] *over $\mathbf{A}$, then $\mathsf{Kdim}\,\rho \leq 0$ and so $\mathsf{Kdim}\,\mathbf{B} \leq \mathsf{Kdim}\,\mathbf{A}$.*

**Lemma 5.** *Let $\varphi : \mathbf{A} \to \mathbf{B}$ be a morphism of commutative rings. The morphism $\varphi$ is lying over if and only if for each ideal $\mathfrak{a}$ of $\mathbf{A}$ and each $x \in \mathbf{A}$, one has $\varphi(x) \in \varphi(\mathfrak{a})\mathbf{B} \Rightarrow x \in \sqrt[\mathbf{A}]{\mathfrak{a}}$.*

**Lemma 6.** *Let $\varphi : \mathbf{A} \to \mathbf{B}$ be a morphism of commutative rings. T.F.A.E.*

1. *The morphism $\varphi$ is going up (i.e. the morphism $\mathsf{Zar}\ \varphi$ is going up).*
2. *For any ideal $\mathfrak{b}$ of $\mathbf{B}$, with $\mathfrak{a} = \varphi^{-1}(\mathfrak{b})$, the morphism $\varphi_{\mathfrak{b}} : \mathbf{A}/\mathfrak{a} \to \mathbf{B}/\mathfrak{b}$ is lying over.*
3. *The same thing with finitely generated ideals $\mathfrak{b}$.*
4. *(In classical mathematics) the same thing with prime ideals.*

**Lemma 7.** *Let $\mathbf{A} \subseteq \mathbf{B}$ be a faithfully flat $\mathbf{A}$-algebra. The morphism $\mathbf{A} \to \mathbf{B}$ is lying over and going up. So $\mathsf{Kdim}\ \mathbf{A} \leq \mathsf{Kdim}\ \mathbf{B}$.*

**Lemma 8.** (A classical going up) *Let $\mathbf{A} \subseteq \mathbf{B}$ be commutative rings with $\mathbf{B}$ integral over $\mathbf{A}$. Then the morphism $\mathbf{A} \to \mathbf{B}$ is lying over and going up. So $\mathsf{Kdim}\ \mathbf{A} \leq \mathsf{Kdim}\ \mathbf{B}$.*

**Lemma 9.** *Let $\varphi : \mathbf{A} \to \mathbf{B}$ be a morphism of commutative rings. T.F.A.E.*

1. *The morphism $\varphi$ is going down.*
2. *For $b, a_1, \dots, a_q \in \mathbf{A}$ and $y \in \mathbf{B}$ such that $\varphi(b)y \in \sqrt[\mathbf{B}]{\langle \varphi(a_1, \dots, a_q) \rangle}$, there exist $x_1, \dots, x_p \in \mathbf{A}$ such that*

$$\langle bx_1, \dots, bx_p \rangle \subseteq \sqrt[\mathbf{A}]{\langle a_1, \dots, a_q \rangle} \ \ \textit{and} \ \ y \in \sqrt[\mathbf{B}]{\langle \varphi(x_1), \dots, \varphi(x_p) \rangle}.$$

3. *(In classical mathematics) for each prime ideal $\mathfrak{p}$ of $\mathbf{B}$ with $\mathfrak{q} = \varphi^{-1}(\mathfrak{p})$ the morphism $\mathbf{A}_{\mathfrak{q}} \to \mathbf{B}_{\mathfrak{p}}$ is lying over.*

**Theorem 14.** (Going down) *Let $\mathbf{A} \subseteq \mathbf{B}$ be commutative rings. The inclusion morphism $\mathbf{A} \to \mathbf{B}$ is going down in the following cases:*

1. *$\mathbf{B}$ is flat over $\mathbf{A}$.*
2. *$\mathbf{B}$ is a domain integral over $\mathbf{A}$, and $\mathbf{A}$ is integrally closed.*

---

[10] An element of $\mathbf{B}$ is said to be primitively algebraic over $\mathbf{A}$ if it annihilates a polynomial in $\mathbf{A}[X]$ whose coefficients are comaximal.

### *4.2 Kronecker, Forster–Swan, Serre and Bass Theorems*

References: [8, 9] and [17, Chapter XIV].

**Theorem 15.** (Kronecker–Heitmann theorem, with Krull dimension, without Noetherianity)

1. *Let* $n \geq 0$. *If* $\mathsf{Kdim}\,\mathbf{A} < n$ *and* $b_1, \ldots, b_n \in \mathbf{A}$, *there exist* $x_1, \ldots, x_n$ *such that for all* $a \in \mathbf{A}$, $\mathrm{D}_{\mathbf{A}}(a, b_1, \ldots, b_n) = \mathrm{D}_{\mathbf{A}}(b_1 + ax_1, \ldots, b_n + ax_n)$.
2. *Consequently in a ring with Krull dimension* $\leq n$, *every finitely generated ideal has the same nilradical as an ideal generated by at most* $n + 1$ *elements.*

For a commutative ring $\mathbf{A}$ we define $\mathsf{Jdim}\,\mathbf{A}$ (J-dimension of $\mathbf{A}$) as being $\mathsf{Kdim}(\mathsf{Heit}\,\mathbf{A})$. In classical mathematics it is the dimension of the Heitmann J-spectrum $\mathsf{Jspec}(\mathbf{A})$.

Another dimension, called Heitmann dimension and denoted by $\mathsf{Hdim}(\mathbf{A})$, has been introduced in [8, 9]. One has always $\mathsf{Hdim}(\mathbf{A}) \leq \mathsf{Jdim}(\mathbf{A}) \leq \mathsf{Kdim}(\mathbf{A})$. The following results with $\mathsf{Jdim}$ hold also for $\mathsf{Hdim}$.

**Definition 4.** A ring $\mathbf{A}$ is said to have *stable range (of Bass)* less than or equal to $n$ when unimodular vectors of length $n + 1$ may be shortened in the following meaning:

$$1 \in \langle a, a_1, \ldots, a_n \rangle \implies \exists\, x_1, \ldots, x_n,\ 1 \in \langle a_1 + x_1 a, \ldots, a_n + x_n a \rangle\,.$$

**Theorem 16.** (Bass–Heitmann Theorem, without Noetherianity) *Let* $n \geq 0$. *If* $\mathsf{Jdim}\,\mathbf{A} < n$, *then* $\mathbf{A}$ *has* stable range $\leq n$. *In particular each stably free* $\mathbf{A}$*-module of rank* $\geq n$ *is free.*

A matrix is said to be of rank $\geq k$ when the minors of size $k$ are comaximal.

**Theorem 17.** (Serre's Splitting Off theorem, for $\mathsf{Jdim}$)
*Let* $k \geq 1$ *and* $M$ *be a projective* $\mathbf{A}$*-module of rank* $\geq k$*, or more generally isomorphic to the image of a matrix of rank* $\geq k$.
*Assume that* $\mathsf{Jdim}\,\mathbf{A} < k$. *Then* $M \simeq N \oplus \mathbf{A}$ *for a suitable module* $N$ *isomorphic to the image of a matrix of rank* $\geq k - 1$.

**Corollary 1.** *Let* $\mathbf{A}$ *be a ring such that* $\mathsf{Jdim}\,\mathbf{A} \leq h$ *and* $M$ *be an* $\mathbf{A}$*-module isomorphic to the image of a matrix of rank* $\geq h + s$. *Then* $M$ *has a direct summand which is a free submodule of rang* $s$. *Precisely, if* $M$ *is the image of a matrix* $F \in \mathbf{A}^{n \times m}$ *of rank* $\geq h + s$, *one has* $M = N \oplus L$ *where* $L$ *is a direct summand that is free of rank* $s$ *in* $\mathbf{A}^n$, *and* $N$ *the image of a matrix of rank* $\geq h$.

In the following theorem we use the notion of finitely generated module *locally generated by* $k$ *elements*. In classical mathematics this means that after localisation at any maximal ideal, $M$ is generated by $k$ elements. A classically equivalent constructive definition is that the $k$-th Fitting ideal of $M$ is equal to $\langle 1 \rangle$.

**Theorem 18.** (Forster–Swan *theorem* for Jdim*) If* Jdim $\mathbf{A} \leq k$ *and if the* **A***-module* $M = \langle y_1, \ldots, y_{k+r+s} \rangle$ *is locally generated by* $r$ *elements, then it is generated by* $k + r$ *elements: one can compute* $z_1, \ldots, z_{k+r}$ *in* $\langle y_{k+r+1}, \ldots, y_{k+r+s} \rangle$ *such that* $M$ *is generated by* $(y_1 + z_1, \ldots, y_{k+r} + z_{k+r})$.

**Theorem 19.** (Bass' cancellation *theorem,* with Jdim*)*
*Let* $M$ *be a finitely generated projective* **A***-module of rank* $\geq k$*. If* Jdim $\mathbf{A} < k$*, then* $M$ *is cancellative for every finitely generated projective* **A***-module. That is, if* $Q$ *is finitely generated projective and* $M \oplus Q \simeq N \oplus Q$*, then* $M \simeq N$.

Theorems 17, 18 and 19 were conjectured by Heitmann in [14] (he proved these theorems for the Krull dimension without Noetherianity assumption).

### *4.3 Other Results Concerning Krull Dimension*

In [17] Theorem XII-6.2 gives the following important characterisation. *An integrally closed coherent ring* **A** *of Krull dimension at most* 1 *is a Prüfer domain.* This explains in a constructive way the nowadays classical definition of Dedekind domains as Noetherian, integrally closed domains of Krull dimension 1, and the fact that, from this definition, in classical mathematics, one is able to prove that finitely generated nonzero ideals are invertible.

In [17, Chapter XVI] there is a constructive proof of the Lequain–Simis theorem. This proof uses the Krull dimension.

In [24, Section 2.6] we find the following new result, with a constructive proof. *If* **A** *is a ring of Krull dimension* $\leq d$*, then the stably free modules of rank* $> d$ *over* $\mathbf{A}[X]$ *are free.*

## References

1. Balbes, R., Dwinger, P.: Distributive Lattices. University of Missouri Press, Columbia, Mo (1974)
2. Bezem, M., Coquand, T.: Automating coherent logic. In: Logic for Programming, Artificial Intelligence, and Reasoning. Proceedings of the 12th International Conference, LPAR 2005, Montego Bay, Jamaica, 2–6 Dec 2005. pp. 246–260. Springer, Berlin (2005)
3. Bishop, E., Bridges, D.: Constructive analysis. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 279. Springer, Berlin (1985)
4. Bishop, E.: Foundations of Constructive Analysis. McGraw-Hill, New York (1967)
5. Borceux, F.: Handbook of Categorical Algebra, Encyclopedia of Mathematics and its Applications, vol. 3, no. 52. Cambridge University Press, Cambridge (1994). Categories of sheaves
6. Bridges, D., Richman, F.: Varieties of constructive mathematics. London Mathematical Society Lecture Note Series, vol. 97. Cambridge University Press, Cambridge (1987)
7. Cederquist, J., Coquand, T.: Entailment relations and distributive lattices. In: Logic Colloquium '98 (Prague). Lecture Note in Logic, vol. 13, pp. 127–139. Association for Symbolic Logic, Urbana, IL (2000)

8. Coquand, T., Lombardi, H., Quitté, C.: Dimension de Heitmann des treillis distributifs et des anneaux commutatifs. In: Algèbre et théorie des nombres. Années 2003–2006, pp. 57–100. Laboratoire de Mathématiques de Besançon, Besançon, 2006. Revised version in 2017. http://arxiv.org/abs/1712.01958
9. Coquand, T., Lombardi, H., Quitté, C.: Generating non-Noetherian modules constructively. Manuscripta Math. **115**(4), 513–520 (2004)
10. Coquand, T., Lombardi, H.: A logical approach to abstract algebra. Math. Struct. Comput. Sci. **16**(5), 885–900 (2006)
11. Coquand, T., Lombardi, H.: Constructions cachées en algebre abstraite. Dimension de Krull, Going up, Going down. 2001. Updated version. Technical report, Laboratoire de Mathématiques de l'Université de Franche-Comté (2018). http://hlombardi.free.fr/GoingUpDownFrench-2018.pdf
12. Coquand, T., Lombardi, H.: Hidden constructions in abstract algebra: Krull dimension of distributive lattices and commutative rings. In: Commutative Ring Theory and Applications (Fez, 2001). Lecture Notes in Pure and Applied Mathematics, Dekker, New York, vol. 231, pp. 477–499 (2003)
13. Coste, M., Lombardi, H., Roy, M.-F.: Dynamical method in algebra: effective Nullstellensätze. Ann. Pure Appl. Log. **111**(3), 203–256 (2001)
14. Heitmann, R.: Generating non-Noetherian modules efficiently. Mich. Math. J. **31**, 167–180 (1984)
15. Hochster, M.: Prime ideal structure in commutative rings. Trans. Am. Math. Soc. **142**, 43–60 (1969)
16. Johnstone, P.T.: Stone Spaces. Cambridge studies in Advanced Mathematics, vol. 3. Cambridge University Press, Cambridge (1986). Reprint of the 1982 edition
17. Lombardi, H., Quitté, C.: Commutative algebra: constructive methods. Finite projective modules. Algebra and Applications. Springer, Dordrecht (2015). Translated from the French (Calvage & Mounet, 2011, revised and extended by the authors) by Tania K. Roblot
18. Lombardi, H.: Dimension de Krull, Nullstellensätze et évaluation dynamique. Math. Z. **242**(1), 23–46 (2002)
19. Lombardi, H.: Structures algébriques dynamiques, espaces topologiques sans points et programme de Hilbert. Ann. Pure Appl. Log. **137**(1–3), 256–290 (2006)
20. Lombardi, H.: Théories géométriques pour l'algébre constructive (2018). http://hlombardi.free.fr/Theories-geometriques.pdf
21. Lorenzen, P.: Algebraische und logistische Untersuchungen über freie Verbände. J. Symbol. Log. **16**, 81–106 (1951). Translation by Stefan Neuwirth: Algebraic and logistic investigations on free lattices. http://arxiv.org/abs/1710.08138
22. Mines, R., Richman, F., Ruitenburg, W.: A course in constructive algebra. Universitext. Springer, New York (1988)
23. Stone, M.H.: Topological representations of distributive lattices and Brouwerian logics. Cas. Mat. Fys. **67**, 1–25 (1937)
24. Yengui, I.: Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases. Lecture Notes in Mathematics, vol. 2138. Springer, Cham (2015)

# Valuative Marot Rings

**Thomas G. Lucas**

**Abstract** For a commutative ring $R$ with total quotient ring $T(R)$, $R$ is said to be valuative if for each nonzero $t \in T(R)$ at least one of the extensions $R \subseteq R[t]$ and $R \subseteq R[(R:t)]$ has no proper intermediate rings. There are weak and strong versions: $R$ is weakly valuative if for each pair $s, t \in T(R)\backslash\{0\}$ such that $st \in R$, at least one of $R \subseteq R[t]$ and $R \subseteq R[s]$ has no proper intermediate rings; $R$ is strongly valuative if for each nonzero $t \in T(R)$ at least one of the extensions $R \subseteq R[(R:(R:t))]$ and $R \subseteq R[(R:t)]$ has no proper intermediate rings. There are weakly valuative rings that are not valuative, and valuative rings that are not strongly valuative. In the special case that $R$ is a Marot ring (each regular ideal can be generated by a set of regular elements), $R$ is weakly valuative if and only if it is strongly valuative. Also a valuative Marot ring has at most three regular maximal ideals.

**Keywords** Marot ring · Minimal extension · Valuative domain · Valuative ring

**Subject Classifications [2100]** Primary 13B99 · 13A15; Secondary 13G05 · 13B21

## 1 Introduction

Throughout this article, $R$ denotes a commutative ring with nonzero identity. Also we use $Z(R)$ to denote the set of zero divisors of $R$, $T(R)$ to denote the total quotient ring of $R$, and $R'$ to denote the integral closure of $R$ in $T(R)$. We have $T(R) = \{a/b \mid a, b \in R \text{ with } b \in R\backslash Z(R)\}$. The set $\text{Reg}(R) = R\backslash Z(R)$ denotes the set of regular elements of $R$ and an (fractional) ideal is *regular* if it contains a regular element of $R$ (of $T(R)$). Also, $\text{RMax}(R)$ denotes the set of regular maximal ideals of $R$. We will concentrate on those $R$ that are *Marot rings*, meaning each regular ideal can

T. G. Lucas (✉)
Department of Mathematics and Statistics, University of North Carolina Charlotte, Charlotte, NC 28223, USA
e-mail: tglucas@uncc.edu



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*, Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_14

be generated by a set of regular elements. A related (stronger) condition is that of a *weakly additively regular ring*: $R$ is weakly additively regular if for each pair of elements $f, g \in R$ with $f$ regular, there are elements $s, t \in R$ such that $gs + ft$ is regular and $sR + fR = R$.

An $R$-module $J \subseteq T(R)$ is an $R$-fractional ideal if there is a regular element $r \in R$ such that $rJ \subseteq R$. Also, we use the standard notation of $(R : J)$ to denote the set $\{t \in T(R) \mid tJ \subseteq R\}$ and $(R :_R J) = (R : J) \cap R$ (so the same as $\{r \in R \mid rJ \subseteq R\}$). In the case $R$ is a Marot ring and $J$ is an $R$-fractional ideal that contains a regular element, then $J$ can be generated by regular elements (see Lemma 2.1 below).

As in [13], we say that $R$ is a *weakly valuative* if for each pair of nonzero elements $x, y \in T(R)$ such that $xy \in R$, at least one of $R \subseteq R[x]$ and $R \subseteq R[y]$ has no proper intermediate rings. Also $R$ is *valuative* if for each nonzero $x \in T(R)$ at least one of $R \subseteq R[x]$ and $R \subseteq R[(R : x)]$ has no proper intermediate rings. Finally, $R$ is *strongly valuative* if for each nonzero $x \in T(R)$ at least one of $R \subseteq R[(R : (R : x))]$ and $R \subseteq R[(R : x)]$ has no proper intermediate rings. An alternate (equivalent) definition for weakly valuative is that for each $x \in T(R)$, either $R \subseteq R[x]$ has no proper intermediate rings or for each $y \in (R : x)$, the extension $R \subseteq R[y]$ has no proper intermediate rings. See [3] for a more general notion between comparable pairs of rings $S \subseteq T$.

Clearly a strongly valuative ring is valuative and a valuative ring is weakly valuative, but there are valuative rings that are not strongly valuative and weakly valuative rings that are not valuative [13, Examples 1.5–1.8]. However, if $R$ is integrally closed in $T(R)$, then it is weakly valuative if and only if it is strongly valuative [3, Theorem 2.15]. More recently, it has been shown that if $R$ is a weakly additively regular ring, then it is weakly valuative if and only if it is strongly valuative (see [13, Theorem 3.13] for the case that $R$ is not integrally closed).

A valuative domain has at most three maximal ideals [1, Theorem 2.2] and at most two when it is not integrally closed [1, Theorem 6.2]. Similarly a weakly additively regular weakly valuative ring has at most three regular maximal ideals and at most two when it is not integrally closed [13, Theorem 3.9], but in both cases it may have infinitely many maximal ideals that are not regular. Also an integrally closed valuative Marot ring has at most three regular maximal ideals [13, Theorem 2.10]. Below we show that a weakly valuative Marot ring that is not integrally closed has at most two regular maximal ideals (see Theorem 3.1).

Several results in [1] characterize when an integral domain is valuative. In particular, [1, Theorem 3.7] covers the case that $R$ is integrally closed, [1, Theorems 5.2 and 5.10] is for when $R$ has a unique maximal ideal and is not integrally closed and [1, Theorem 6.2] is for the case $R$ has exactly two maximal ideals and is not integrally closed. In [13], each of these results was extended to weakly additively regular rings, specifically [13, Theorem 3.5], [13, Theorem 3.13], and [13, Theorem 3.17], respectively. Below we give the analogous results for Marot rings: Theorem 2.17 (the same as [13, Theorem 2.10] cited in the previous paragraph), Theorems 3.4 and 3.7.

If $R \subsetneq R[t]$ is a minimal extension for some $t \in T \backslash R$ (i.e., there are no proper intermediate rings), then $M = \sqrt{(R :_R t)}$ is a maximal ideal of $R$ (see, for example, [2]). The maximal ideal $M$ is referred to as the *crucial maximal ideal* of the extension (see, for example, [5, Page 804]). When dealing with a specific ring extension $R \subsetneq T$, if there is an element $s \in T \backslash R$ such that $N = \sqrt{(R :_R s)}$ is a maximal ideal of $R$, then, as in [3], we refer to $N$ as a *maximal $T$-radical ideal* of $R$ (no matter whether the extension $R \subsetneq R[s]$ is minimal or not). It is known that if $R$ is weakly valuative, then there are at most three maximal $T(R)$-radical ideals in $R$ [3, Theorem 5.4]. The ring $R$ in [13, Example 1.9] shows that even if a ring is strongly valuative, it can have infinitely many regular maximal ideals.

For a prime ideal $P$ of $R$, $R_{[P]} = \{t \in T(R) \mid ts \in R$ for some $s \in R\backslash P\}$ and $R_{(P)} = \{t \in T(R) \mid ts \in R$ for some $s \in \mathrm{Reg}(R)\backslash P\}$. The latter is the same ring as $R_H$ where $H = \mathrm{Reg}(R)\backslash P$. If $P$ is not regular, then $\mathrm{Reg}(R) \cap P = \emptyset$ and so $R_{(P)} = T(R)$ in this case. There are different types of extensions of ideals to a ring of the type $R_{[P]}$. For example, one may consider the simple extension $IR_{[P]}$ and the potentially larger extension $[I]R_{[P]} = \{t \in T(R) \mid ts \in I$ for some $s \in R\backslash P\}$ (for example, $[I]R_{[P]} = R_{[P]}$ for each ideal $I$ that is not contained in $P$, but $IR_{[P]}$ is a proper ideal if $I \subseteq Z(R)$). In contrast, $IR_{(P)} = \{t \in T(R) \mid ts \in I$ for some $s \in \mathrm{Reg}(R)\backslash P\}$. If $R$ is a Marot ring and $P$ is regular, then $R_{[P]} = R_{(P)}$ [14, Proposition 6]. Also in this case, if $J$ is a regular ideal, then $JR_{[P]} = [J]R_{[P]}$, with $JR_{[P]} = R_{[P]}$ if $J$ is not contained in $P$.

Recall that a ring $R$ together with a prime ideal $P$ is a *valuation pair* of $T(R)$ if for each $t \in T(R)\backslash R$, there is a $p \in P$ such that $tp \in R\backslash P$ (see, for example, [9, Page 25]). Corresponding to a valuation pair $(R, P)$ is a totally ordered additive Abelian group $G$ and a surjective map $\mathrm{v} : T(R) \to G \cup \{\infty\}$ (with $g < \infty$ for all $g \in G$) such that (i) $\mathrm{v}(ab) = \mathrm{v}(a) + \mathrm{v}(b)$, (ii) $\mathrm{v}(a + b) \geq \min\{\mathrm{v}(a), \mathrm{v}(b)\}$, (iii) $\mathrm{v}(1) = 0$ and $\mathrm{v}(0) = \infty$, and (iv) $R = \{t \in T(R) \mid \mathrm{v}(t) \geq 0\}$ and $P = \{t \in T(R) \mid \mathrm{v}(t) > 0\}$. A related weaker notion is that of a *mock valuation ring* meaning that $R$ is such that $T(R)\backslash R$ is multiplicatively closed [3]. While there are mock valuation rings that are not valuation rings, if $R$ is a Marot ring, it is a mock valuation ring if and only if it has a unique regular maximal ideal $M$ and $M$ is such that $(R, M)$ is a valuation pair of $T(R)$ (see [9, Theorem 7.7] and its proof). Also $R$ is a *Prüfer ring* if each finitely generated regular ideal is invertible. This is equivalent to having $(R_{[M]}, [M]R_{[M]})$ a valuation pair for each (regular) maximal ideal $M$ [7, Theorem 13].

## 2 Preliminary Results

Let $P$ be a prime ideal of a ring $R$ and let $S$ be a proper overring of $R$. Then we let $S_{(P)} = \{t \in T(R) \mid bt \in S$ for some $b \in \mathrm{Reg}(R)\backslash P\}$ and $S_{[P]} = \{t \in T(R) \mid bt \in S$ for some $b \in R\backslash P\}$. As with $R_{(P)}$ and $R_{[P]}$, if $P$ is not a regular ideal of $R$, then $S_{(P)} = T(R) = S_{[P]}$.

**Lemma 2.1.** *Let $R$ be a Marot ring.*

1. *Each regular $R$-fractional ideal can be generated by a set of regular elements.*
2. *If $P$ is a regular prime ideal and $I$ is a regular ideal, then $IR_{[P]} = [I]R_{[P]}$.*

*Proof.* Let $J$ be a regular $R$-fractional ideal. Then there is a regular element $r \in R$ such that $rJ \subseteq R$. Since $R$ is Marot, there is a set of regular elements $X$ in $rJ$ that generates $rJ$ as an (integral) ideal of $R$. The set $r^{-1}X$ is a set of regular elements in $J$ that generate $J$ as an $R$-fractional ideal.

Next suppose $P$ is a regular prime ideal of $R$ and let $I$ be a regular ideal. If $I$ is not contained in $P$, then the Marot property guarantees the existence of a regular element $m \in I\backslash P$. Clearly $m$ is a unit of $R_{[P]}$ and thus $[I]R_{[P]} \subseteq R_{[P]} = mR_{[P]} \subseteq IR_{[P]}$. On the other hand if $I$ is contained in $P$, we at least know that $IR_{[P]} \subseteq [I]R_{[I]}$. For the reverse containment let $q \in [I]R_{[P]}$. Then there is an element $r \in R\backslash P$ such that $rq \in I$. We also have a regular element $p \in R$ such that $pq \in R$ and a regular element $b \in I$. The ideal $J = rR + pbR$ is a regular ideal contained in $(R :_R q)$ but not in $P$. Since $R$ is Marot, $J$ is generated by its regular elements, so there is a regular element $x \in J\backslash P$. As $xq \in I$ and $x$ is a unit of $R_{[P]}$, $q \in IR_{[P]}$ as desired. □

**Lemma 2.2.** *Let $M$ be a regular maximal ideal of a ring $R$ and let $S$ be a ring such that $R \subseteq S \subseteq T(R)$.*

1. *$MR_{[M]}$ is a maximal ideal of $R_{[M]}$, $(R_{[M]})_{[MR_{[M]}]} = R_{[M]}$ and $R_M = (R_{[M]})_{MR_{[M]}}$.*
2. *$(S_{[M]})_{[MR_{[M]}]} = S_{[M]}$ and $S_M = (S_{[M]})_{MR_{[M]}}$.*
3. *If $R$ is a Marot ring, then $S_{[M]} = S_{(M)}$.*

*Proof.* Let $q \in R_{[M]}\backslash MR_{[M]}$. Then there is an element $r \in R\backslash M$ such that $qr \in R$. If $qr \notin M$, then there are elements $a \in R\backslash M$ and $n \in M$ such that $qra + n = 1$. Clearly both $qra$ and $n$ are in $qR_{[M]} + MR_{[M]}$. Thus $qR_{[M]} + MR_{[M]} = R_{[M]}$. In contrast, if $qr \in M$ for each such $r \in R\backslash M$, then for a given $r$ we have elements $c \in R\backslash M$ and $m \in M$ such that $cr + m = 1$ which puts $q = crq + mq \in MR_{[M]}$, a contradiction. Hence $MR_{[M]}$ is a maximal ideal of $R_{[M]}$.

For (2) and the rest of (1), start with an element $i \in (S_{[M]})_{[MR_{[M]}]}$. Then there is an element $j \in R_{[M]}\backslash MR_{[M]}$ such that $ij \in S_{[M]}$. We have elements $k, m \in R\backslash M$ such that $kj \in R\backslash M$ and $mji \in S$. Also $mkji \in S$ with $mkj \in R\backslash M$. Thus $i \in S_{[M]}$. Hence $(S_{[M]})_{[MR_{[M]}]} = S_{[M]}$ and $(R_{[M]})_{[MR_{[M]}]} = R_{[M]}$.

To see that $S_M = (S_{[M]})_{MR_{[M]}}$, suppose $c/d \in (S_{[M]})_{MR_{[M]}}$ with $c \in S$ and $d \in R_{[M]}\backslash MR_{[M]}$. Then we have elements $x, y \in R\backslash M$ such that $xc \in S$ and $yd \in R$. We also have $xy, xyd \in R\backslash M$ and $xyc \in S$. Hence $c/d = xyc/xyd \in S_M$. Thus $S_M = (S_{[M]})_{MR_{[M]}}$ and $R_M = (R_{[M]})_{MR_{[M]}}$.

For (3), assume $R$ is Marot and let $q \in S_{[M]}$. Then there is an element $t \in R\backslash M$ such that $qt \in S$. We also have a regular element $r \in R$ such that $qr \in R$. Thus the (integral) ideal $(S :_R q)$ is a regular ideal of $R$ that is not contained in $M$. Since $R$ is Marot, there is a regular element $x \in (S :_R q)\backslash M$. As $qx \in S$, $q \in S_{(M)}$. □

A more general version of the following lemma appears in [3].

**Lemma 2.3.** (cf. [3, Lemma 2.6]) *Let $R \subsetneq S$ be a minimal extension with corresponding crucial maximal ideal $M \in$* RMax$(R)$ *and $S \subseteq T(R)$. Then $R_{[M]} \subsetneq S_{[M]}$ is also a minimal extension.*

For each $M \in \text{Max}(R)$, $R_{(M)}$ is a regular ring of quotients of $R$ (inside $T(R)$) and thus $R'_{(M)}$ is the integral closure, $(R_{(M)})'$, of $R_{(M)}$ in $T(R)$.

Next we provide a pair of statements equivalent to saying that the integral closure of $R$ is a Prüfer ring. These (and the corollary that follows) will be used to show that the integral closure of a weakly valuative Marot ring is a Prüfer ring.

**Theorem 2.4.** *Let $R$ be a ring with integral closure $R' \supsetneq R$. Then the following are equivalent:*

1. *$R'$ is a Prüfer ring.*
2. *$R'_{(M)}$ is a Prüfer ring for each $M \in \text{RMax}(R)$.*
3. *For each $M \in \text{RMax}(R)$, the integral closure of $R_{(M)}$ is a Prüfer ring.*

*Proof.* If $R'$ is a Prüfer ring, then each ring between $R'$ and $T(R)$ is also a Prüfer ring. Hence $R'_{(M)}$ is a Prüfer ring for each $M \in \text{RMax}(R)$. Thus (1) implies (2).

The equivalence of (2) and (3) follows from the fact that $R'_{(M)}$ is the integral closure of $R_{(M)}$ for each $M \in \text{RMax}(R)$.

To complete the proof we show (2) implies (1).

Let $N'$ be a regular maximal ideal of $R'$. Then $N = N' \cap R$ is a regular maximal ideal of $R$. The ideal $Q = N'R'_{(N)}$ is a regular maximal ideal of $S = R'_{(N)}$. A proof similar to that used to establish statement (2) in Lemma 2.2 shows that $S_{[Q]} = R'_{[N']}$ and $[Q]S_{[Q]} = [N']R'_{[N']}$.

Since $R'_{(P)}$ is a Prüfer ring for each $P \in \text{RMax}(R)$, $(R'_{[M']}, [M']R'_{[M']})$ is a valuation pair for each $M' \in \text{RMax}(R')$. Therefore $R'$ is a Prüfer ring. □

As a corollary we have the following special case.

**Corollary 2.5.** *Let $R$ be a ring that is not integrally closed. If there is a unique (regular) maximal ideal $M$ such that the integral closure of $R_{(M)}$ is a Prüfer ring and $(R_{(N)}, NR_{(N)})$ is a Prüfer valuation ring for all other $N \in \text{RMax}(R)$ (if any), then the integral closure of $R$ is a Prüfer ring.*

We will make use of the following lemma in the proofs of Theorems 2.7 and 3.7.

**Lemma 2.6.** *Let $R$ and $S$ be rings with $R \subsetneq S \subseteq T(R)$. Then $S = \bigcap\{S_{(M)} \mid M \in \text{RMax}(R)\} = \bigcap\{S_{[M]} \mid M \in \text{RMax}(R)\}$.*

*Proof.* The usual conductor argument shows that $S = \bigcap\{S_{(N)} \mid N \in \text{Max}(R)\} = \bigcap\{S_{[N]} \mid N \in \text{Max}(R)\}$. Since $S_{(N)} = S_{[N]} = T(R)$ for all $N \in \text{Max}(R)\backslash\text{RMax}(R)$, we also have $S = \bigcap\{S_{(M)} \mid M \in \text{RMax}(R)\} = \bigcap\{S_{[M]} \mid M \in \text{RMax}(R)\}$. □

**Theorem 2.7.** *Let $R$ and $S$ be rings with $R \subsetneq S \subseteq T(R)$.*

1. *The following are equivalent:*

   a. *$R \subsetneq S$ is a minimal extension.*
   b. *There is a regular maximal ideal $M$ of $R$ such that $R_M \subsetneq S_M$ is minimal and $R_N = S_N$ for all other regular maximal ideals $N \in \text{RMax}(R)\backslash\{M\}$ (if any).*

c. *There is a regular maximal ideal* $M$ *of* $R$ *such that* $R_{[M]} \subsetneq S_{[M]}$ *is minimal and* $R_{[N]} = S_{[N]}$ *for all other regular maximal ideals* $N \in \mathrm{RMax}(R)\backslash\{M\}$ *(if any).*

2. *If* $R$ *is a Marot ring, then* $R \subsetneq S$ *is a minimal extension if and only if there is a regular maximal ideal* $M$ *of* $R$ *such that* $R_{(M)} \subsetneq S_{(M)}$ *is minimal and* $R_{(N)} = S_{(N)}$ *for all other regular maximal ideals* $N \in \mathrm{RMax}(R)\backslash\{M\}$ *(if any).*

*Proof.* To start, if $P$ is a prime ideal of $R$, then $R_P = S_P$ if and only if $R_{[P]} = S_{[P]}$. To see this first suppose $R_P = S_P$ and let $q \in S_{[P]}$. Then by definition, there is an element $r \in R\backslash P$ such that $qr \in S$. From the equality $R_P = S_P$ we then have an element $t \in R\backslash P$ such that $qrt \in R$ and it follows that $q \in R_{[P]}$. Similarly, if $R_{[P]} = S_{[P]}$ and $x/y \in S_P$ with $x \in S$ and $y \in R\backslash P$, then there is an element $z \in R\backslash P$ such that $zx \in R$ and it follows that $x/y = zx/zy \in R_P$.

To establish the equivalence of (a) and (b) in (1), we note that from [6, Lemme 1.2 and Théorème 2.2], $R_M \subsetneq S_M$ is minimal for some (necessarily regular) maximal ideal $M \in \mathrm{Max}(R)$ and $R_P = S_P$ for all other prime ideals $P \in \mathrm{Spec}(R)$ when $R \subsetneq S$ is a minimal extension, so certainly $R_N = S_N$ for all regular maximal ideals $N \in \mathrm{RMax}(R)\backslash\{M\}$.

An observation in [2, Pages 1092 and 1093] is that if there is a maximal ideal $N \in \mathrm{Max}(R)$ such that $R_N \subsetneq S_N$ is minimal and $R_P = S_P$ for all $P \in \mathrm{Spec}(R)\backslash\{N\}$, then $R \subsetneq S$ is a minimal extension. We will start with only assuming we have a regular maximal ideal $M$ of $R$ such that $R_M \subsetneq S_M$ is minimal and $R_N = S_N$ for all $N = \mathrm{RMax}(R)\backslash\{M\}$ (if any). From the observation in [2], it suffices to show $R_P = S_P$ for all $P \in \mathrm{Spec}(R)\backslash\{M\}$. First note that if $P \in \mathrm{Spec}(R)$ is not regular, then $R_P = T(R)_P = S_P$ (as each regular element of $R$ is a unit in $R_P$). For $P$ regular and not contained in $M$, it is contained in some maximal ideal $N \in \mathrm{RMax}(R)$. As $R_N = S_N$, we also have $R_P = (R_N)_P = (S_N)_P = S_P$. Finally for $P$ regular and (properly) contained in $M$, the assumption that $R_M \subsetneq S_M$ is a minimal extension yields that $R_P = (R_M)_P = (S_M)_P = S_P$ (from [6, Théorème 2.2]). Hence (a) and (b) are equivalent.

To see that (a) implies (c), we make use of the observation in the first sentence and Lemma 2.6. Suppose $R \subseteq S$ is minimal with corresponding crucial maximal ideal $M$. Then by Lemma 2.6, $R_{[M]} \subsetneq S_{[M]}$ is minimal. We also have $R_{[N]} = S_{[N]}$ for all $N \in \mathrm{RMax}(R)\backslash\{M\}$.

To complete the proof of (1), we show that (c) implies (a). Suppose we have a regular maximal ideal $M$ of $R$ such that $R_{[M]} \subsetneq S_{[M]}$ is minimal and $R_{[N]} = S_{[N]}$ for all $N \in \mathrm{RMax}(R)\backslash\{M\}$ (if any). From the latter, we have $R_N = S_N$ for all $N \in \mathrm{RMax}(R)\backslash\{M\}$. Let $W$ be a ring such that $R \subsetneq W \subseteq S$. For each $N \in \mathrm{RMax}(R)\backslash\{M\}$, we get $W_{[N]} = R_{[N]}$ as $W_{[P]}$ always lies between $R_{[P]}$ and $S_{[P]}$ for a prime $P$ of $R$. As $M$ is the only other regular maximal ideal of $R$ (and $W$ properly contains $R$), $R_{[M]} \subsetneq W_{[M]}$ since $W = \bigcap\{W_{[Q]} \mid Q \in \mathrm{RMax}(R)\}$. We also have $W_{[M]} \subseteq S_{[M]}$ and so $W_{[M]} = S_{[M]}$ (as $R_{[M]} \subsetneq S_{[M]}$ is minimal) and therefore $W = S$. Hence $R \subsetneq S$ is minimal.

Under the assumption that $R$ is Marot, $R_{[Q]} = R_{(Q)}$ and $S_{[Q]} = S_{(Q)}$ for all regular maximal ideals $Q \in \mathrm{RMax}(R)$ (Lemma 2.2). Thus the equivalence in (2) follows from the equivalence of (a) and (c) in (1). □

The strongly valuative ring $R$ in [13, Example 2.19] has infinitely many regular maximal ideals each of which contains the set of regular nonunits of $R$. Thus $R_{(Q)} = R$ for each regular maximal ideal $Q \in \mathrm{RMax}(R)$. Also the integral closure of $R$ is a minimal extension of $R$. Hence the equivalence in statement (2) of the previous theorem does not hold in general. However, we do have the following.

**Corollary 2.8.** *Let $R$ and $S$ be rings such that $R \subsetneq S \subseteq T(R)$. If there is a regular maximal ideal $M$ of $R$ such that $R_{(M)} \subsetneq S_{(M)}$ is a minimal extension and $R_{(N)} = S_{(N)}$ for all other regular maximal ideals $N$ (if any), then $R \subsetneq S$ is a minimal extension.*

*Proof.* The result follows trivially if $M$ is the only regular maximal ideal of $R$. Suppose we have a ring $W$ such that $R \subsetneq W \subseteq S$. Then we have $R_{(N)} \subseteq W_{(N)} \subseteq S_{(N)} = R_{(N)}$ for each $N \in \mathrm{RMax}(R)\backslash\{M\}$. Since $W$ properly contains $R$, it must be that $W_{(M)}$ properly contains $R_{(M)}$ (by way of Lemma 2.6). As $R_{(M)} \subsetneq S_{(M)}$ is minimal and $R_{(M)} \subsetneq W_{(M)} \subseteq S_{(M)}$ we have $W_{(M)} = S_{(M)}$ and so by Lemma 2.6 $W = S$. Therefore $R \subsetneq S$ is a minimal extension. □

A useful concept when dealing with valuative rings is that of a pointwise minimal extension: a pair of rings $S \subseteq T$ is referred to as a *pointwise minimal extension* if for each $t \in T$, the extension $S \subseteq S[t]$ has no proper intermediate rings. For an integral domain that is not integrally closed, a necessary condition for it to be valuative is that its integral closure is a pointwise minimal extension [1, Proposition 4.1].

**Corollary 2.9.** *Let $R$ be a ring that is not integrally closed and let $S$ be a proper overring that is integral over $R$. If there is a regular maximal ideal $M$ of $R$ such that $R_{(M)} \subsetneq S_{(M)}$ is a pointwise minimal extension and $R_{(N)} = S_{(N)}$ for all regular maximal ideals $N \in \mathrm{RMax}(R)\backslash\{M\}$ (if any), then $R \subsetneq S$ is a pointwise minimal extension.*

*Proof.* Assume there is a regular maximal ideal $M$ of $R$ such that $R_{(M)} \subsetneq S_{(M)}$ is a pointwise minimal extension and $R_{(N)} = S_{(N)}$ for all regular maximal ideals $N \in \mathrm{RMax}(R)\backslash\{M\}$. Then for $t \in S\backslash R$, we have $R_{(N)} = R_{(N)}[t] = R[t]_{(N)}$ for all regular maximal ideals $N$ other than $M$. Thus it must be that $t \in S_{(M)}\backslash R_{(M)}$. Hence $R_{(M)} \subsetneq R_{(M)}[t] = R[t]_{(M)}$ is a minimal integral extension. It follows that $R \subsetneq R[t]$ is minimal and therefore $S$ is a pointwise minimal extension of $R$. □

We recall several basic results that will be useful in our study of valuative Marot rings.

**Lemma 2.10.** [cf. [14, Proposition 5]] *If $R$ is a Marot ring and $R \subseteq S \subseteq T(R)$, then $S$ is a Marot ring.*

**Lemma 2.11.** [13, Lemma 2.2] *Let $S \subsetneq T$ be a ring extension.*

1. *If $t \in T$ is such that $S \subsetneq S[r]$ is a minimal extension for each $r \in (S :_T t)\backslash S$, then there is a unique maximal ideal $M$ of $S$ such that $M = \sqrt{(S :_S r)}$ for each $r \in (S :_T t)\backslash S$.*
2. *If $T$ is a pointwise minimal extension of $S$, then there is a unique maximal ideal $M$ of $S$ such that $M = \sqrt{(S :_S x)}$ for each $x \in T\backslash S$.*

**Lemma 2.12.** [13, Lemma 2.3] *Let $I$ be an invertible ideal of a ring $R$. If $b \in R$ is a nonunit of $R$ such that $bR + I = R$, then $I^{-1} = bI^{-1} + R$.*

**Lemma 2.13.** [13, Lemma 2.4] *Let $I$ and $J$ be invertible comaximal ideals of a ring $R$. If $b \in I$ and $c \in J$ are such that $b + c = 1$, then $(R :_R bJ^{-1}) = J$ and $(R :_R cI^{-1}) = I$.*

**Lemma 2.14.** [13, Lemma 3.2] *Let $R$ be a ring with at least two regular maximal ideals $M$ and $N$. If $R \subsetneq (M : M)$ and $b \in N\backslash M$ and $c \in M\backslash N$ are regular elements, then $R \subsetneq R[b/c]$ is not a minimal extension of $R$.*

**Theorem 2.15.** [13, Theorem 2.5] *Let $R$ be a weakly valuative ring. If $I = bR + rR$ and $J = cR + rR$ are comaximal invertible proper ideals with $b + c = 1$, then at least one of $\sqrt{I}$ and $\sqrt{J}$ is a maximal $T(R)$-radical ideal.*

**Corollary 2.16.** [13, Corollary 2.6] *Let $R$ be a weakly valuative ring with exactly three regular maximal ideals $M_1$, $M_2$, and $M_3$. Also let $r \in M_1 \cap M_2 \cap M_3$ be regular and let $b \in M_1$ and $c \in M_2 \cap M_3$ be such that $b + c = 1$ with $B = bR + rR$ and $C = cR + rR$ invertible. Then $M_1 = \sqrt{B}$ and there is an element $t \in B^{-1}\backslash R$ such that $M_1 = \sqrt{(R :_R t)}$ and $R \subsetneq R[t]$ is a minimal extension.*

The next result from [13] gives a characterization of integrally closed Marot rings that are valuative.

**Theorem 2.17.** [13, Theorem 2.10] *The following are equivalent for an integrally closed Marot ring $R$:*

1. *$R$ is strongly valuative.*
2. *$R$ is valuative.*
3. *$R$ is weakly valuative.*
4. *$R$ is a Prüfer with at most three regular maximal ideals, the set of regular non-maximal prime ideals is linearly ordered under set containment and at most one regular maximal ideal fails to contain each regular nonmaximal prime.*
5. *$R$ is a Prüfer ring with at most three regular maximal ideals and at most one regular maximal ideal fails to contain each regular nonmaximal prime.*

It is convenient to record the following corollary.

**Corollary 2.18.** *Let $R$ be an integrally closed Marot ring with a unique regular maximal ideal. Then $R$ is valuative if and only if it is a Prüfer valuation ring.*

*Proof.* A valuation ring is always valuative. For the converse we have that $R$ is a Marot Prüfer ring with a unique regular maximal ideal $M$. Since $R$ is Marot, $R = R_{(M)} = R_{[M]}$, and thus $(R, M)$ is a valuation pair of $T(R)$ [7, Theorem 13]. □

The ring $R$ in [13, Example 3.4] (and [11, Example 2.4]) is an integrally closed valuative Marot ring that is a Prüfer ring with exactly two regular maximal ideals but is not weakly additively regular. However, it is rather easy to show that a Marot (Prüfer) valuation ring is weakly additively regular.

With regard to the proof of the next result and Theorem 2.21, we define *weakly additively regular ordered pairs* as follows: for $f, g \in R$ with $f$ regular, if there is a pair $s, t \in R$ such that $gs + ft$ is regular and $fR + sR = R$, we say that $(g, f)$ is a *weakly additively regular ordered pair*. Note that if $g \in fR$, then we have $f = g + f(1 - p)$ where $g = fp$. Hence $(g, f)$ is a weakly additively regular ordered pair whenever $f$ divides $g$. In particular, $(h, u)$ is a weakly additively ordered pair for each unit $u$ and element $h \in R$.

**Theorem 2.19.** *Each Marot valuation ring is weakly additively regular.*

*Proof.* Let $V$ be a Marot ring that is also a valuation ring. Then $V$ has a unique regular maximal ideal $M$. Let $\mathrm{v} : T(V) \to G \cup \{\infty\}$ be a valuation map corresponding to the valuation pair $(V, M)$ where $G$ is the corresponding value group. Since $V$ is a Marot ring, the regular nonunits of $V$ map onto the positive elements of $G$ [9, Theorem 7.9]. Let $f, g \in V$ with $f$ regular. As noted above, if $f$ divides $g$ in $V$, then $(g, f)$ is a weakly additively regular ordered pair.

To complete the proof, consider the case that $f$ does not divide $g$. Then $f$ is not a unit. Since $f$ is regular, $g/f \in T(V)$ with $\mathrm{v}(g/f) = \mathrm{v}(g) - \mathrm{v}(f)$. As we are assuming $f$ does not divide $g$, it must be that $0 \le \mathrm{v}(g) < \mathrm{v}(f)$. The ideal $gV + fV$ is regular and thus is generated by regular elements. Moreover, there must be a regular element $h \in gV + fV$ such that $\mathrm{v}(h) = \mathrm{v}(g)$. We have $h = gb + fc$ for some $b, c \in V$. With regard to v, we have $\mathrm{v}(h) = \mathrm{v}(gb + fc) \ge \min\{\mathrm{v}(g) + \mathrm{v}(b), \mathrm{v}(f) + \mathrm{v}(c)\}$. As $\mathrm{v}(h) = \mathrm{v}(g) < \mathrm{v}(f)$, it must be that $\mathrm{v}(b) = 0$. Since $M$ is the only regular maximal ideal and $b \notin M$, we have $bV + fV = V$. Hence we again have that $(g, f)$ is a weakly additively regular ordered pair. Therefore $V$ is weakly additively regular. □

**Lemma 2.20.** *Let $R$ be a ring with a regular element $f$ that is contained in each regular maximal ideal. Then $R$ is weakly additively regular if and only if $(g, k)$ is a weakly additively regular ordered pair for each $g \in R$ and each $k \in fR \cap \mathrm{Reg}(R)$.*

*Proof.* Suppose $(g, k)$ is a weakly additively regular ordered pair for each $g \in R$ and each $k \in fR \cap \mathrm{Reg}(R)$. For each $r \in \mathrm{Reg}(R)$, $rf \in fR \cap \mathrm{Reg}(R)$ and thus there are elements $m, n \in R$ (depending on $g$ and $rf$) such that $gm + rfn$ is regular with $mR + rfR = R$. Since $f$ is contained in each regular maximal ideal, no regular maximal ideal contains $m$ and thus $mR + rR = R$. Hence $R$ is weakly additively regular. The converse is trivial. □

**Theorem 2.21.** *Let $R$ be a Marot ring with integral closure $R' \supsetneq R$. If $R'$ is a valuation ring and $(R : R')$ is a regular ideal of $R$, then $R$ is weakly additively regular.*

*Proof.* Assume $R'$ is a valuation ring and $(R : R')$ is a regular ideal of $R$. Since $R$ is a Marot ring, so is $R'$. Hence $R'$ is also a Prüfer ring with unique regular maximal ideal $M'$. In addition, for the corresponding valuation map v and value group $G$, $M' = \{r \in T(R) \mid \mathrm{v}(r) > 0\}$ and the regular elements of $M'$ map onto the set of positive elements of $G$. The ideal $M = M' \cap R$ is the unique regular maximal ideal of $R$.

Let $I = (R : R')$. Then $I$ is also a regular ideal of $R'$, necessarily proper and thus contained in $M'$. Let $f' \in I$ and $f \in f'R$ be regular. Also let $k \in R'$ be such that $\mathrm{v}(k) \geq \mathrm{v}(f)$. Since $f$ is regular, $k/f \in T(R)$ with $\mathrm{v}(k/f) \geq 0$. Hence $k/f \in R'$. As $I$ is an ideal of $R'$, $k = f(k/f) \in I$.

Next let $g \in R$. To see that $(g, f)$ is a weakly additively regular ordered pair, first consider the case $\mathrm{v}(g) \geq 2\mathrm{v}(f)$. Then $\mathrm{v}(g/f) \geq \mathrm{v}(f)$ so that $g/f \in I$. In this case $f$ divides $g$ in $R$ and thus $(g, f)$ is a weakly additively regular ordered pair. Next suppose $\mathrm{v}(g) < 2\mathrm{v}(f)$. The ideal $gR + f^2R$ is regular and so is generated by regular elements $f^2, d_1, d_2, \ldots, d_n$. By properties of v, at least one $d_i$ is such that $\mathrm{v}(d_i) = \mathrm{v}(g)$. Without loss of generality we may assume $\mathrm{v}(d_1) = \mathrm{v}(g)$. We also have $d_1 = gs + f^2t = gs + f(ft)$ for some $s, t \in R$. Since $\mathrm{v}(g) < 2\mathrm{v}(f)$, it must be that $\mathrm{v}(s) = 0$ and thus $sR' + fR' = R'$. By integrality we also have $sR + fR = R$. Hence $(g, f)$ is weakly additively regular ordered pair for each $g \in R$ and each regular element $f \in f'R$. Therefore $R$ is weakly additively regular by Lemma 2.20. □

## 3 Valuative Marot Rings

The first result of this section extends several from [1] that deal with valuative domains that are not integrally closed and some from [13] that deal with weakly additively regular rings that are not integrally closed.

**Theorem 3.1.** *Let $R$ be a Marot ring that is not integrally closed. If $R$ is weakly valuative, then*

1. *the set of regular nonmaximal primes is linearly ordered (under set containment),*
2. *there is a unique regular maximal ideal $M$ such that $R_{(M)}$ is not a mock valuation ring and for all other regular prime ideals $P$, $R_{(P)}$ is a Prüfer valuation ring,*
3. *the ideal $M$ is a maximal $T(R)$-radical ideal with $R \subsetneq (M : M)$,*
4. *the ring $R$ has at most two regular maximal ideals,*
5. *if $R$ has (exactly) two regular maximal ideals, then both are maximal $T(R)$-radical ideals, and*
6. *the ideal $M$ contains each regular nonmaximal prime.*

*Proof.* We establish the six conclusions in the order they appear. The proof that the set of regular nonmaximal prime ideals is linearly ordered is only slightly different than the one for valuative domains. By way of contradiction, suppose $P$ and $Q$ are incomparable regular prime ideals with neither a maximal ideal. Since $R$ is Marot, there is a regular element $r \in P\backslash Q$ and a regular element $s \in Q\backslash P$. Then neither $r/s$ nor $s/r$ is in $R$. Clearly, $r/s \in (R : s/r)$ and $s/r \in (R : r/s)$. Hence at least one of $R \subsetneq R[r/s]$ and $R \subsetneq R[s/r]$ is a minimal extension. But $P \supseteq (R :_R s/r)$ and $Q \supseteq (R :_R r/s)$ are not maximal ideals. So we have a contradiction by way of [2, Theorems 2.3 and 3.4].

For (2) and (3), [3, Theorem 5.10] yields that $R$ has a unique regular maximal ideal $M$ such that $R_{(M)}$ is not a mock valuation ring. In addition, $R_{(P)}$ is a mock valuation ring for all other regular prime ideals $P$ (if any). As $R$ is Marot, each $R_{(P)}$ is a Prüfer valuation ring with unique regular maximal ideal $PR_{(P)}$ [9, Theorem 7.7]. Hence each $R_{(P)}$ contains $R'$. We also have an element $t \in R'\backslash R$ such that $R \subsetneq R[t]$ is a minimal extension with $M = (R :_R t)$ and $R[t] \subseteq (M : M)$. Thus $M$ is a maximal $T(R)$-radical ideal and $R \subsetneq (M : M)$.

To see that $R$ has at most two regular maximal ideals, suppose that there are at least two regular maximal ideals $N_1$ and $N_2$ other than $M$. Since $R$ is a Marot ring, there is a regular element $r \in N_1 \cap N_2$ that is not in $M$. Also there is a regular element $s \in M$ that is not in $N_1$. By Lemma 2.14, $R \subsetneq R[r/s]$ is not a minimal extension. Thus since $R$ is weakly valuative $R \subsetneq R[s/r]$ is a minimal extension. But both $N_1$ and $N_2$ contain $(R :_R s/r)$ and so $R \subsetneq R[s/r]$ cannot be minimum either. Hence $R$ has at most two regular maximal ideals.

For (5), suppose $R$ has a regular maximal ideal $N$ other than $M$. Since $R$ is a Marot ring there are regular elements $r \in N\backslash M$ and $s \in M\backslash N$. As above, we again have that $R \subsetneq R[r/s]$ is not minimal and thus $R \subsetneq R[s/r]$ is minimal, necessarily with $N = \sqrt{(R :_R s/r)}$. Thus both $N$ and $M$ are maximal $T(R)$-radical ideals in this case.

Finally, if $M$ is the only regular maximal ideal, then it trivially contains all regular nonmaximal primes. So suppose we have a second regular maximal ideal $N$ and, by way of contradiction, also suppose $N$ contains a regular nonmaximal prime $P$ that is not contained in $M$. Since $R$ is a Marot we can choose a regular element $b \in P\backslash M$ and a regular element $c \in M\backslash P$. We will also have $b \in N$ and thus by Lemma 2.14, $R \subsetneq R[b/c]$ is not minimal. As above we obtain a contradiction since $P$ contains $(R :_R c/b)$ but $R \subsetneq R[c/b]$ must be minimal since $R$ is weakly valuative. Therefore $M$ contains each regular nonmaximal prime. □

Recall from above that for a pair of rings $S \subsetneq T$, $T$ is referred to as a *pointwise minimal extension* of $S$ if for each $t \in T\backslash S$, the extension $S \subsetneq S[t]$ is minimal. We will find this notion to be quite useful in characterizing Marot rings that are valuative. Another useful concept is to extend the definition of the types of valuative rings to individual elements: $x \in T(R)$ is (i) *valuative over* $R$ if at least one of $R \subseteq R[x]$ and $R \subseteq R[(R : x)]$ has no proper intermediate rings, (ii) *weakly valuative over* $R$ if either $R \subseteq R[x]$ has no proper intermediate rings or for each $y \in (R : x)$, $R \subseteq R[y]$ has no proper intermediate rings, and (iii) *strongly valuative over* $R$ is at least one of $R \subseteq R[(R : (R : x))]$ and $R \subseteq R[(R : x)]$ has no proper intermediate rings.

**Lemma 3.2.** *Let $R$ be a Marot ring that is weakly valuative. If $R$ is not integrally closed, then there is a regular element $t \in R'\backslash R$ such that $R \subsetneq R[t]$ is a minimal extension.*

*Proof.* If $R$ is not integrally closed, there is an element $b \in R'\backslash R$. The $R$-fractional ideal $bR + R$ is regular, so it contains a regular element $t \in R'\backslash R$ since $R$ is a Marot ring. Since $t$ is integral over $R$ (and regular), it is contained in $R[t^{-1}]$. That $R \subsetneq R[t]$ is minimal follows from the assumption that $R$ is weakly valuative. □

**Theorem 3.3.** *Let $R$ be a Marot ring with integral closure $R' \supsetneq R$. If $R$ is weakly valuative, then $R'$ is a Prüfer ring and $R$ and $R'$ have the same number of regular maximal ideals (exactly one, or exactly two).*

*Proof.* Assume $R$ is weakly valuative. Then it has at most two regular maximal ideals. In the case $R$ has (exactly) two regular maximal ideals, one of these, say $M$ is such that $R_{(M)}$ is not integrally closed and for the other one $N$, $R_{(N)}$ is a Prüfer valuation ring with a unique regular maximal ideal $NR_{(N)}$. By way of Corollary 2.5, we may conclude that $R'$ is a Prüfer ring by showing the integral closure of $R_{(M)}$ is a Prüfer valuation ring.

The ring $R_{(M)}$ is weakly valuative with unique regular maximal ideal $MR_{(M)}$. Hence we may reduce to the case $M$ which is the unique regular maximal ideal of $R$.

By Lemma 3.2 there is a regular element $t \in R'\backslash R$ such that $R \subsetneq R[t]$ is a minimal extension. As $M$ is the unique regular maximal ideal of $R$, we have $M = (R :_R t)$ with $t \in (M : M)$. Thus by [3, Lemma 3.7], there is no $b \in T(R)\backslash R$ such that $R \subsetneq R[b]$ is a closed minimal extension. For units $u, u^{-1} \in T(R)\backslash R$, at least one of $R \subsetneq R[u]$ and $R \subsetneq R[u^{-1}]$ is minimal and thus at least one of $u$ and $u^{-1}$ is in $R'$. Therefore, since $R'$ is a Marot ring, it is also a Prüfer valuation ring, necessarily with a unique (regular) maximal ideal that lies over $M$.

For the case that $R$ has exactly two regular maximal ideals $N$ and $M$ as given above, the fact that both $R_{(N)}$ and $R'_{(M)}$ are Prüfer valuation rings implies $R'$ is a Prüfer ring with a unique regular maximal ideal $N'$ that lies over $N$ and a unique regular maximal ideal $M'$ that lies over $M$. These are the only regular maximal ideals of $R'$ since each regular maximal ideal of $R'$ lies over a regular maximal ideal of $R$. □

**Theorem 3.4.** *Let $R$ be a Marot ring that is not integrally closed. If $R$ has a unique regular maximal ideal $M$, then the following are equivalent:*

1. *$R$ is strongly valuative.*
2. *$R$ is valuative.*
3. *$R$ is weakly valuative.*
4. *The integral closure of $R$ is a Prüfer valuation ring (with a unique regular maximal ideal) and it is a pointwise minimal extension of $R$.*

*Proof.* It is clear that (1) implies (2), and (2) implies (3). We next show that (4) implies (3).

Assume $R'$ is a Prüfer valuation ring and a pointwise minimal extension of $R$. Since $R'$ is a Prüfer valuation ring, it has a unique regular maximal ideal $M'$ [9, Theorem 6.5]. For each $s \in R'\backslash R$, $R \subsetneq R[s]$ is a minimal integral extension necessarily with $M = (R :_R s)$ and $MR[s] = M$. Thus $MR' = M$. So each element of $R'$ is weakly valuative over $R$.

For $t \in T(R)\backslash R'$, $(R' : t) \subseteq M'$. Thus if $z \in (R : t)$, then $z \in M'$ and so the extension $R \subseteq R[z]$ has no proper intermediate rings. It follows that $t$ is weakly valuative over $R$ and therefore $R$ is weakly valuative.

To complete the proof we show that (3) implies both (1) and (4). By Theorem 3.3, $R'$ is a Prüfer valuation ring with a unique regular maximal ideal $M'$ that lies over $M$.

First note that since $R$ is not integrally closed, there is an element $m \in \mathrm{Reg}(R')\backslash R$ such that $R \subsetneq R[m]$ is a minimal integral extension (Lemma 3.2). Since $M$ is the only regular maximal ideal, we have $M = (R :_R m)$ and $(M : M) \supseteq R[m]$.

Let $f \in M \cap \mathrm{Reg}(R)$ and let $q \in R'\backslash R$. The $R$-fractional ideal $qR + fR$ is regular and thus is generated by regular elements. For such a generating set $\{s_1, s_2, \ldots, s_n\}$, we have $s_i M \subseteq M$ for each $i$. Hence $qM \subseteq M$ and therefore $M$ is an ideal of $R'$.

By Theorem 2.21, $R$ is weakly additively regular. Therefore from [13, Theorem 3.13], $R$ is strongly valuative and $R'$ is a pointwise minimal extension of $R$. □

**Corollary 3.5.** *Let $R$ be a Marot ring with a unique regular maximal ideal $M$. If $R$ is (weakly, strongly) valuative and not integrally closed, then $R$ is weakly additively regular, $R'$ is a Prüfer valuation ring with a unique maximal ideal $M'$ and either $M' = M$ or there is a regular element $d \in R'$ such that $M' = dR'$ and $M = d^2R'$.*

*Proof.* That $R'$ is a Prüfer valuation ring with a unique regular maximal ideal $M'$ is from the previous theorem. Also, from the proof of that theorem, $M$ is an ideal of $R'$. Hence $R$ is weakly additively regular by Theorem 2.21. Thus by [13, Theorem 3.13] we have that either $M = M'$ is the unique regular maximal ideal of both $R$ and $R'$, or there is a regular element $d \in R'$ such that $M = d^2R' \subsetneq M = dR'$. □

Later we give an example of a Marot valuative ring with exactly two regular maximal ideals that are neither weakly additively regular nor integrally closed (Example 3.15).

**Lemma 3.6.** *Let $t \in T(R)\backslash R$. If $R \subsetneq R[t]$ is a closed minimal extension, then $t$ is strongly valuative over $R$ and $R[t] = R[(R : (R : t))]$.*

*Proof.* If $R \subsetneq R[t]$ is a closed minimal extension, then $(R :_R t)$ is an invertible $M$-primary ideal of $R$ where $M = \sqrt{(R :_R t)}$ is a regular maximal ideal of $R$ [2, Theorem 3.4]. Also, we have a pair of elements $a, b \in (R :_R t)$ such that $a + bt = 1$. We claim that $(R : (R : t)) \subseteq R[t]$. Let $u \in (R : (R : t))$. Then $ua, ub \in R$ and so $u = ua + (ub)t \in R[t]$. Therefore $R[(R : (R : t))] = R[t]$ and we have that $t$ is strongly valuative over $R$. □

For an ideal $I$ of $R$, $\Psi(I) = \bigcap\{R_{[P]} \mid I \nsubseteq P,\ P \in \mathrm{Spec}(R)\}$ (see, for example, [2, Page 1083]).

**Theorem 3.7.** *Let $R$ be a Marot ring that is not integrally closed. If $R$ has exactly two regular maximal ideals, then the following are equivalent:*

1. *R is strongly valuative.*
2. *R is valuative.*
3. *R is weakly valuative.*
4. *$R'$ is both a Prüfer ring and a pointwise minimal extension of R, R has a regular maximal ideal N such that $R_{(N)}$ is a Prüfer valuation ring, and for the other regular maximal ideal M, (i) M is a maximal ideal of $R'$, (ii) M contains each regular nonmaximal prime of R and $R'$, and (iii) $R_{(M)}$ is a (weakly) [strongly] valuative ring such that $MR_{(M)}$ is also the maximal ideal of $R'_{(M)}$.*

*Proof.* In general, a strongly valuative ring is valuative and a valuative ring is weakly valuative. Thus it suffices to show that (3) implies (4), and (4) implies (1).

We start by showing (3) implies (4). Assume $R$ is weakly valuative. Since $R$ has two regular maximal ideals, both are maximal $T(R)$-radical ideals (Theorem 3.1) and thus $R'$ is a pointwise minimal extension of $R$ by [3, Corollary 5.14]. Also, by Theorem 3.3, $R'$ is a Prüfer ring with exactly two regular maximal ideals. By [3, Theorem 5.10] (and the Marot assumption), there is a unique regular maximal ideal $M$ of $R$ such that $R_{(M)}$ is not a mock valuation ring and for the other regular maximal ideal $N$, $R_{[N]} = R_{(N)}$ is a Prüfer valuation ring with unique regular maximal ideal $NR_{(N)}$. We also have that $R_{(M)}$ is weakly valuative [3, Proposition 5.2]. As $R_{(M)}$ is also a Marot ring, it is strongly valuative and its integral closure, $R'_{(M)}$, is a Prüfer valuation ring that is a pointwise minimal extension of $R_{(M)}$ (Theorem 3.4). In addition, $M = (R :_R t)$ for each $t \in R'\backslash R$ (since $R'$ is a pointwise minimal extension of $R$). By Corollary 3.5, $MR_{(M)}$ is either the unique regular maximal ideal of $R'_{(M)}$ or $MR_{(M)} = d^2R'_{(M)} \subseteq dR'_{(M)} = M'R'_{(M)}$ where $M'$ is regular maximal ideal of $R'$ that lies over $M$. In the first case, $M'R'_{(M)} = MR_{(M)}$ and so $M' = M$, and in the second $M'R'_{(M)} \supsetneq MR_{(M)}$ and so $M' \supsetneq M$. We will show that the second case does not occur.

By Theorem 3.1, the set of regular nonmaximal primes is linearly ordered under set containment and $M$ contains each regular nonmaximal prime.

Since $R_{(P)}$ is a Prüfer valuation ring for each regular prime $P$ other than $M$, the contraction map from Spec$(R')$ to Spec$(R)$ is an order preserving bijective correspondence. It follows that $M'$ contains each regular nonmaximal prime of $R'$.

Since $R$ is a Marot ring and $M$ and $N$ are the only regular maximal ideals, there is a regular element $s \in N\backslash M$. As $M$ contains each regular nonmaximal prime, $N = \sqrt{sR}$. We also have $N' = \sqrt{sR'}$. Let $Q$ be a nonmaximal prime ideal contained in $N$ and let $m \in Q$. Then the ideal $I = sR + mR$ is such that $IR_{(N)} = sR_{(N)}$ and $IR_{(M)} = sR_{(M)} = R_{(M)}$. Hence $s$ divides $m$. In fact $s^n$ divides $m$ for each positive integer $n$. It follows that $\bigcap s^nR \supseteq Q$. Similarly $\bigcap s^nR' \supseteq Q'$ for each nonmaximal prime ideal $Q'$ of $R'$ that is contained in $N'$. Thus $\bigcap s^nR = P$ and $\bigcap s^nR' = P'$ for some nonmaximal primes $P$ of $R$ and $P'$ of $R'$.

Consider the extension $R \subsetneq R[1/s]$. We have $N = \sqrt{(R :_R 1/s)}$. For a finitely generated $N$-primary ideal $J$, $JR_{(M)} = R_{(M)}$ and $JR_{(N)}$ are both regular principal ideals. Hence $J$ is invertible. By [1, Corollary 3.7], $R \subsetneq R[1/s] = \Psi(N)$ is a closed minimal extension. Since $M$ contains each regular nonmaximal prime, $\Psi(N) = R_{(M)}$. The extension $R \subsetneq R[1/s]$ is the unique closed minimal extension of $R$ since

$N$ and $M$ are the only regular maximal ideals (and $M$ is the crucial maximal ideal of a minimal integral extension).

Finally we will show that $M$ is a common maximal ideal of $R$ and $R'$. By way of contradiction suppose there is a regular $d \in R'$ such that $M'R'_{(M)} = dR'_{(M)} \supsetneq d^2R'_{(M)} = MR'_{(M)}$. While $sdR'_{(M)} = M'R'_{(M)} = dR'_{(M)}$ implies it is possible to have $s$ divide $d$ in $R'$, we cannot have that each positive power of $s$ divides $d$ in $R'$ as this would put $d$ in $P'$, making $P'$ regular and thus properly contained in $M'$ and hence in $M$. Thus without loss of generality we may assume $d/s$ is not in $R'$. Since $d \in M'$ and $s \in R'\backslash M'$, $s/d$ is not in $R'$. Thus neither $R \subsetneq R[d/s]$ nor $R \subsetneq R[s/d]$ is integral. For the extension $R \subsetneq R[d/s]$, it is clear that this is not $R_{(M)} = \Psi(N)$ as $d \notin R_{(M)}$ (while $s$ is a unit of $R_{(M)}$). Hence $R \subsetneq R[d/s]$ is not a minimal extension.

For the extension $R \subsetneq R[s/d]$, the fact that $d \in M'$ while $s \in R'\backslash M'$ implies $s/d$ is not in $R'_{(M)}$ and so not in $R_{(M)}$. Thus $R[s/d] \neq \Psi(N)$. As $R \subsetneq \Psi(N)$ is the unique closed minimal extension $R$, $R \subsetneq R[s/d]$ is not a minimal extension, contradicting the assumption that $R$ is weakly valuative. Hence it must be that $M$ is a common maximal ideal of $R$ and $R'$. We also have that each regular nonmaximal prime of $R'$ is contained in $M$. Hence (3) implies (4).

To complete the proof we show that (4) implies (1). We assume all of the following: $R'$ is a pointwise minimal extension of $R$, $R$ has a regular maximal ideal $N$ such that $R_{(N)}$ is a Prüfer valuation ring, and for the other regular maximal ideal $M$, (i) $M$ is a maximal ideal of $R'$, (ii) $M$ contains each regular nonmaximal prime of $R$ and $R'$, and (iii) $R_{(M)}$ is a weakly valuative ring such that $MR_{(M)}$ is also the maximal ideal of $R'_{(M)}$ which is a Prüfer valuation ring. By Theorem 3.4, $R_{(M)}$ is strongly valuative. Since $R$ is Marot and $M$ contains each regular nonmaximal prime, there is a regular element $s \in N\backslash M$ necessarily with $N = \sqrt{sR}$. Also, for a finitely generated $N$-primary ideal $I$, $I$ contains a power of $s$ so $I$ is regular. Since $R_{(N)}$ is a Prüfer valuation ring, $IR_{(N)}$ is invertible. Also $IR_{(M)} = R_{(M)}$. It follows that $I$ is invertible. By [2, Corollary 3.7], $R \subsetneq R[1/s] = \Psi(N)$ is a closed minimal extension of $R$, and since $M$ contains each regular nonmaximal prime $\Psi(N) = R_{(M)}$. By Lemma 3.6, each element $t \in R_{(M)}\backslash R$ is strongly valuative over $R$.

We let v be a valuation map corresponding to the valuation pair $(R'_{(M)}, MR'_{(M)})$ and let w be a valuation map corresponding to the valuation pair $(R_{(N)}, NR_{(N)})$. Since $R$ is a Marot ring, both v and w map the units of $T(R)$ onto the elements of the corresponding value group [9, Theorem 7.9].

Let $x \in T(R)\backslash R_{(M)}$. We consider three main cases, the third will have three subcases.

**Case 1:** $x$ is in neither $R_{(N)}$ nor $R'_{(M)}$.
In this case, $(R_{(N)} : x) \subseteq NR_{(N)}$ and $(R'_{(M)} : x) \subseteq MR'_{(M)} = MR_{(M)}$. Thus if $x$ is in neither $R_{(N)}$ nor $R'_{(M)}$, then $(R : x) \subseteq NR_{(N)} \cap MR_{(M)} = N \cap M \subseteq R$. Hence in this case $x$ is strongly valuative over $R$.

**Case 2:** $x \in R_{(N)}\backslash R'_{(M)}$.
We have $(R'_{(M)} : x) \subseteq MR_{(M)}$ which implies $(R : x) \subseteq MR_{(M)}$. It follows that $R \subseteq R[(R : x)]$ has no proper intermediate rings as $R \subsetneq R_{(M)}$ is a closed minimal extension. Therefore $x$ is strongly valuative in this case.

**Case 3:** $x \in R'_{(M)} \backslash R_{(M)}$.
We have $(R :_R x) \subseteq M$ so there is a regular element $m \in M$ such that $mx \in R$. Since $R_{(M)}$ is a strongly valuative Marot with a single regular maximal ideal, it is weakly additively regular (Corollary 3.5). Thus there is a pair of elements $f, g \in R_{(M)}$ such that $z = fxm + gm^2$ is regular with $fR_{(M)} + m^2R_{(M)} = R_{(M)}$. The element $y' = fx + gm \in xR_{(M)} + mR_{(M)}$ is a unit of $R'_{(M)}$ since $f, x \in R'_{(M)} \backslash MR_{(M)}$. Also, there are elements $c, d \in R_{(M)}$ such that $cf + dm^2 = 1$. Thus $x = x(cf + dm^2) = c(y' - gm) + m(dxm) = cy' + m(dxm - g) \in y'R_{(M)} + mR_{(M)}$. We also have a regular element $q \in R \backslash M$ such that $y = qy' \in R'$. As $q$ is a unit of $R_{(M)}$ and $m/y \in MR_{(M)}$, $xR_{(M)} + mR_{(M)} = yR_{(M)} + mR_{(M)} = yR_{(M)}$. Hence $x/y \in R_{(M)}$. With regard to colons, $(R_{(M)} : x) = (R_{(M)} : y) = (1/y)R_{(M)}$ and $(R_{(M)} : (R_{(M)} : x)) = (R_{(M)} : R_{(M)} : y)) = yR_{(M)}$.

We have three subcases: (i) $\mathrm{w}(x) = \infty$, (ii) $\mathrm{w}(x) < 0$, and (iii) $0 \le \mathrm{w}(x) < \infty$.

If $\mathrm{w}(x) = \infty$, $(R_{(N)} : x) = T(R)$ and $(R_{(N)} : (R_{(N)} : x)) \subsetneq NR_{(N)}$. We also have $(1/y)R = (R : y) = (R_{(N)} : y) \cap (R_{(M)} : y) \subseteq T(R) \cap (R_{(M)} : x) = (R : x)$. It follows that $(R : (R : x)) \subseteq (R : (R : y)) = yR$. As $y \in R' \backslash R$, $R \subsetneq R[y]$ is a minimal extension and thus $R \subseteq R[(R : (R : x))]$ has no proper intermediate rings.

For the case $\mathrm{w}(x) < 0$, we have $(R_{(N)} : x) \subseteq NR_{(N)}$ and thus $R_{(N)}[(R : x)] = R_{(N)}$. Also $R_{(M)} \subseteq R_{(M)}[(R : x)] \subseteq R_{(M)}[1/y]$ with $R_{(M)} \subsetneq R_{(M)}[1/y]$ minimal. Hence $R \subseteq R[(R : x)]$ has no proper intermediate rings (Corollary 2.8).

Finally we consider the case $0 \le \mathrm{w}(x) < \infty$. We have a regular element $t \in R_{(N)}$ such that $\mathrm{w}(t) = \mathrm{w}(x)$. Hence $x/t \in R_{(N)}$. We also have $x/y \in R_{(M)}$. Thus there are regular elements $b \in R \backslash N$ and $c \in R \backslash M$ such that $bx/t, cx/y \in R$. It follows that $(b/t)R + (c/y)R \subseteq (R : x)$. Since $b$ is a unit of $R_{(N)}$ and $(R : x) \subseteq (R_{(N)} : x) = (1/t)R_{(N)}$, $(b/t)R_{(N)} + (c/y)_{(N)} \supseteq (R : x)_{(N)}$. Similarly $(R : x) \subseteq (R_{(M)} : x) = (1/y)R_{(M)}$, $(b/t)R_{(M)} + (c/y)_{(M)} \supseteq (R : x)_{(M)}$. Thus $(R : x) = (b/t)R + (c/y)R$. Since $(R : x)$ is a finitely generated fractional $R$-ideal, we have $(R : (R : x))_{(N)} = (R_{(N)} : (R_{(N)} : x)) \subseteq R_{(N)}$ and $(R : (R : x))_{(M)} = (R_{(M)} : (R_{(M)} : x)) = yR_{(M)}$. Another application of Corollary 2.8 yields that $R \subseteq R[(R : (R : x))]$ has no proper intermediate rings since $R_{(M)} \subsetneq R[(R : (R : x))]_{(M)} = R_{(M)}[y]$ is a minimal extension and $R[(R : (R : x))]_{(N)} = R_{(N)}$.

From all of the cases, we have that $x$ is strongly valuative over $R$ and therefore $R$ is strongly valuative. □

The next corollary provides alternate lists of conditions that are equivalent to those given in (4) of the previous theorem.

**Corollary 3.8.** *Let $R$ be a Marot ring that has exactly two regular maximal ideals and is not integrally closed. Then the following are equivalent:*

1. *$R$ is (weakly) [strongly] valuative.*
2. *$R$ has a regular maximal ideal $N$ such that $(R_{(N)}, NR_{(N)})$ is a valuation pair and for the other maximal ideal $M$: $M$ is a maximal ideal of $R'$ that contains each regular nonmaximal prime ideal of $R'$ and $R_{(M)}$ is valuative.*

3. *$R'$ is a Prüfer ring and $R$ has a regular maximal ideal $M$ such that (i) $M$ is a maximal ideal of $R'$, (ii) $M$ contains each regular nonmaximal prime of $R$ and $R'$, and (iii) $R_{(M)}$ is a (weakly) [strongly] valuative ring.*
4. *$R'$ is a pointwise minimal extension of $R$, $R$ has a regular maximal ideal $N$ such that $R_{(N)}$ is a Prüfer valuation ring, and for the other regular maximal ideal $M$, (i) $M$ is a maximal ideal of $R'$, (ii) $M$ contains each regular nonmaximal prime of $R$ and $R'$, and (iii) $R_{(M)}$ is a (weakly) [strongly] valuative ring such that $MR_{(M)}$ is also the maximal ideal of $R'_{(M)}$.*

*Proof.* It is clear that statement (4) of Theorem 3.7 implies statements (2), (3), and (4) here. Also statement (4) in this result clearly implies (2), and taken together (2), (3) and (4) in this result yields statement (4) of Theorem 3.7. For all three of (2), (3), and (4), we have the regular maximal ideal $M$ of $R$ that is also a maximal ideal of $R'$. Since $R$ has a second regular maximal ideal $N$, there is a regular maximal ideal $N'$ of $R'$ such that $N' \cap R = N$. Also $R'_{(M)}$ is the integral closure of $R_{(M)}$.

By basic properties of pullbacks, the prime ideals of $R$ that are not contained in $M$ are in one-to-one correspondence with the prime ideals of $R'$ that are not contained in $M$. Specifically for a prime $P'$ of $R'$ that is not contained in $M$, $P = P' \cap R$ is the corresponding prime ideal of $R$ and $P' = (M :_{R'} P)$. Since $M$ is a regular ideal of $R$, $MP'$ is a regular ideal of $R$ whenever $P'$ is a regular ideal of $R'$. Hence $R'$ has exactly two regular maximal ideals, $M$ and $N'$. Since $R$ is a Marot ring, there is a regular element $t \in M\backslash N$. So for each $q \in R'\backslash N'$ and $b \in R'$, $tq \in R\backslash N$, $tb \in R$, and $b/q = tb/tq \in R_{(N)}$. It follows that $R_{(N)} = R'_{(N)} = R'_{(N')}$.

To see that (2) implies (3), all we need to show is that $R'$ is a Prüfer ring. Since $R$ is Marot and $R_{(N)}$ is a valuation ring, $(R_{(N)}, NR_{(N)}) = (R'_{(N')}, N'R'_{(N')})$ is a valuation pair and $M$ and $N'$ are the only regular maximal ideals of $R'$. Next we consider $R'_{(M)}$. We have that $MR_{(M)} = MR'_{(M)}$ is the only regular maximal ideal of $R_{(M)}$, so we simply apply Theorem 3.4 to see that $R'_{(M)}$ is valuation ring (and $R'_{(M)}, MR'_{(M)}$ is a valuation pair). Thus $R'$ is a Prüfer ring and so (2) implies (3).

Finally assume the restrictions in (3). From the arguments above, $R_{(N)}$ is a valuation ring. So to show (3) implies (4), all that remains is to show that $R'$ is a pointwise minimal extension of $R$. Since $R'_{(M)}$ is the integral closure of $R_{(M)}$, it is also a pointwise minimal extension of $R_{(M)}$ by Theorem 3.4. That $R'$ is a pointwise minimal extension of $R$ now follows from Corollary 2.9 (and the fact that $R_{(N)} = R'_{(N)}$). □

**Theorem 3.9.** *Let $R$ be a ring whose integral closure, $R'$, is a valuation ring properly contained in $T(R)$. If $R \subsetneq R'$ is a minimal extension, then $R$ is strongly valuative.*

*Proof.* Since $R'$ is a valuation ring, there is a prime ideal $P$ of $R'$ such that for each $q \in T(R)\backslash R'$, there is an element $p \in P$ such that $pq \in R'\backslash P$. It is also the case that if $f \in R'\backslash P$, then $(R' : f) = R'$. Also note that for $h \in R$, $1 \in (R : h)$ implies $(R : (R : h)) \subseteq R$. Thus $h$ is strongly valuative over $R$.

Suppose $R \subsetneq R'$ is a minimal extension and let $t \in T(R)\backslash R$. We have two cases to consider, $t \in T(R)\backslash R'$ and $t \in R'\backslash R$. For the former, $(R : t) \subseteq (R' : t) \subseteq R'$. Since $R \subsetneq R'$ is a minimal extension and $(R : t) \subseteq R'$, $R \subseteq R[(R : t)]$ has no proper intermediate rings. Thus, in this case, $t$ is strongly valuative over $R$.

Next suppose $t \in R'\backslash R$. We split the argument into two subcases: $t \in R'\backslash P$ and $t \in P$. If $t \in R'\backslash P$, then $(R : t) \subseteq (R' : t) = R'$ in which case $R[(R : t)] \subseteq R'$, and thus $R \subseteq R[(R : t)]$ has no proper intermediate rings. Hence $t$ is strongly valuative over $R$ in this case.

Finally suppose $t \in P$. We again have $(R : t) \subseteq (R' : t)$ but now $(R' : t)$ is not contained in $R'$. If $(R : t) \subseteq R'$, then as above $R \subseteq R[(R : t)]$ has no proper intermediate rings. On the other hand, if $(R : t)$ is not contained in $R'$, then $(R : (R : t)) \subseteq R'$ and so $R \subseteq R[(R : (R : t))]$ $(\subseteq R')$ has no proper intermediate rings. Therefore each element of $T(R)$ is strongly valuative over $R$ and so $R$ is strongly valuative. □

Let $D$ be an integral domain and let $\mathscr{P} = \{P_\alpha\}_{\alpha \in \mathscr{A}}$ be a nonempty set of prime ideals of $D$. Next let $\mathscr{I} = \mathscr{A} \times \mathbb{N}$ and for each $i = (\alpha, n) \in \mathscr{I}$, let $K_i$ be the quotient field of $D/P_\alpha$. Form the $D$-algebra $B = \sum K_i$ and define a ring structure on $D \times B$ by setting $(r, b) + (s, c) = (r + s, b + c)$ and $(r, b)(s, c) = (rs, rc + sb + bc)$. The resulting ring is denoted $D + B$ and is referred to as the ring of the form $A + B$ corresponding to $D$ and $\mathscr{P}$. For $r \in D$, $b \in B$ and $i = (\alpha, n) \in \mathscr{I}$, $r_i$ denotes the image of $r$ in $K_i$ and $b_i$ denotes the $i$th component of $b$.

A few of the basic properties of these rings are given in the following theorem.

**Theorem 3.10.** [10, Theorems 8.3 and 8.4] *Let $\mathscr{P} = \{P_\alpha\}_{\alpha \in \mathscr{A}}$ be a nonempty set of prime ideals of a domain $D$ and let $R = D + B$ be the $A + B$ ring corresponding to $D$ and $\mathscr{P}$.*

1. *An element $(r, b)$ of $R$ is a zero divisor if and only if there is an $i = (\alpha, n) \in \mathscr{I} = \mathscr{A} \times \mathbb{N}$ such that $r_i + b_i = 0$. A necessary condition for $(s, c) \in R$ to be regular is that $s \in D\backslash \bigcup P_\alpha$.*
2. *For each $i \in \mathscr{I}$, the set $M_i = \{(r, b) \in R \mid r_i = -b_i\}$ is both a maximal ideal and a minimal prime ideal of $R$. All other prime ideals of $R$ are of the form $P + B$ for some prime ideal $P$ of $D$.*
3. *The total quotient ring of $R$ can be identified with the ring $D_{\mathscr{S}} + B$ where $\mathscr{S} = D\backslash \bigcup\{P_\alpha \mid P_\alpha \in \mathscr{P}\}$.*
4. *If $I$ is an ideal of $D$ such that $I \cap \mathscr{S} \neq \emptyset$, then $IR = I + B$ is a regular ideal of $R$. Conversely, if $J$ is a regular ideal of $R$, then $J = I + B = IR$ for some $I$ of $D$ such that $I \cap \mathscr{S} \neq \emptyset$.*
5. *If $I$ is an ideal of $D$, then $IR$ is an invertible of $R$ if and only if $I$ is an invertible ideal of $D$ and $I \cap \mathscr{S} \neq \emptyset$.*

The following definitions were introduced in [12]. A nonempty set of prime ideals $\mathscr{P} = \{P_\alpha\}_{\mathscr{A}}$ of a domain $D$ is said to be a *weakly additively regular family* if for each $g \in \bigcup P_\alpha$ and $f \in D\backslash \bigcup P_\alpha$, there is a pair of elements $s, t \in D$ such that $gs + ft \in D\backslash \bigcup P_\alpha$ and $sD + fD = D$. Also $\mathscr{P}$ is said to be a *Marot family* if for each ideal $I \nsubseteq \bigcup P_\alpha$, $I$ can be generated by the set $I\backslash \bigcup P_\alpha$.

The next theorem blends two results from [12] concerning special families of prime ideals and rings of the form $A + B$.

**Theorem 3.11.** (cf. [12, Theorems 3.6 and 3.9]) *Let $R = D + B$ be the ring of the form $A + B$ corresponding to a domain $D$ and a nonempty set of nonzero prime ideals $\mathscr{P} = \{P_\alpha\}_{\alpha \in \mathscr{A}}$ of $D$ corresponding to $D$ and $\mathscr{P}$.*

1. *$R$ is weakly additively regular if and only if $\mathscr{P}$ is a weakly additively regular family.*
2. *$R$ is Marot if and only if $\mathscr{P}$ is a Marot family.*

Another result from [12] gives us the following (stated in a slightly different way).

**Theorem 3.12.** (cf. [12, Corollary 3.11]) *Let $D$ be a Bezout domain and let $\mathscr{P} = \{P_\alpha\}_{\alpha \in \mathscr{A}}$ be a nonempty set of nonzero prime ideals of $D$ and let $R = D + B$ be the ring of form $A + B$ corresponding to $D$ and $\mathscr{P}$. Then each finitely generated regular ideal of $R$ is principal and thus $R$ is a regular Bezout ring (and a Prüfer ring).*

We will use these characterizations in the proof of the next example.

*Example 3.13.* Let $D' = \mathbb{Q}[X]$ and let $D$ be the pullback of $\mathbb{Q}$ over the maximal ideal $M = (X^2 + 1)D'$. For $\mathscr{P}' = \mathrm{Max}(D') \backslash \{M\}$, let $R = D + B$ be the ring of form $A + B$ corresponding to $D$ and $\mathscr{P}'$ and let $R' = D' + B$ be the ring of form $A + B$ corresponding to $D'$ and $\mathscr{P}'$.

1. For both $R$ and $R'$, $MR' = MR$ is the only regular prime ideal.
2. $R'$ is both a weakly additively regular valuation ring and a regular Bezout ring.
3. $R \subsetneq R' = R[X]$ is a minimal integral extension and thus $R$ is strongly valuative.
4. $R$ is not a Marot ring.

*Proof.* The set $\mathscr{P} = \mathrm{Max}(D) \backslash \{M\}$ yields the same module $B$ and thus the same $R$. For both $R'$ and $R$, $MR' = M + B = MR$ is the only regular prime ideal. Since $D'$ is a PID, $R'$ is a regular Bezout ring with a unique regular prime ideal. Thus $D'$ is valuation ring and so it is weakly additively regular (Theorem 2.19).

The extension $D \subsetneq D' = D[X]$ is a minimal integral extension (since the same is true for $D/M = \mathbb{Q} \subsetneq \mathbb{Q}[\sqrt{-1}] = D'/M$) and thus $R \subsetneq R' = R[X]$ is a minimal integral extension. Hence $R$ is strongly valuative by Theorem 3.9. We have $D' \backslash \bigcup P_\alpha = \{q(X^2 + 1)^n \mid n \geq 0,\ q \in \mathbb{Q} \backslash \{0\}\}$. Also $(p, 0)$ is a unit in $R$ for each nonzero $p \in \mathbb{Q}$. It follows that the (proper) regular principal ideals of $R$ have the form $(X^2 + 1)^m R$ for some $m \geq 1$. Since $X$ is not in $D$, $X(X^2 + 1)D$ and $(X^2 + 1)D$ are incomparable. We also have $X(X^2 + 1)D \subseteq \bigcup P_\alpha$ and $M = X(X^2 + 1)D + (X^2 + 1)D \supsetneq (X^2 + 1)D$ since $D' = XD + D$ (and $M = (X^2 + 1)D'$). It follows that $MR$ cannot be generated by regular elements of $R$. Thus $R$ is a not a Marot ring. □

The last example is the one promised above of a valuative Marot ring with exactly two regular maximal ideals that are neither weakly additively regular nor integrally closed. The next result provides a basis for exhibiting such a ring. Note that the restriction in (a) is used to show the ring $R$ is Marot.

**Theorem 3.14.** *Let $D'$ be a Dedekind domain with a pair of maximal ideals $P$ and $Q$ where neither is principal, but all three of $P^2$, $Q^2$, and $P \cap Q$ are principal. Assume $D'$ also satisfies these additional restrictions.*

(a) *For each nonunit $w \in D' \backslash P$, there is an element $d \in P$ such that $w + d$ is a unit of $D'$.*

*(b) The residue field $L = D'/P$ has a proper subfield $K$ such that $L = K + iK$ for some $i$.*

*(c) There are elements $a, b, c \in D$ such that $P \cap Q = aD'$, $P^2 = bD'$, and $Q^2 = cD'$ where $D$ is the pullback of $K$ over $P$.*

*Next we let $\mathscr{P} = \{P_\alpha\} = \mathrm{Max}(D') \backslash \{P, Q\}$ and $S' = \bigcup P_\alpha$. Also let $Q_o = D \cap Q$ and $S = D \cap S'$. Finally, let $R = D + B$ and $R' = D' + B$ be the rings of the form $A + B$ corresponding to $D$ and $D'$, respectively, and the set $\mathscr{P}$.*

1. *Each $P$-primary ideal of $D$ can be generated by elements in $P \backslash S'$ and each $Q_o$-primary ideal of $D$ can be generated by elements in $Q_o \backslash S'$.*
2. *$R'$ is the integral closure of $R$ and it is not weakly additively regular. Also $R'$ is a Prüfer ring with exactly two regular prime ideals.*
3. *$R$ is a valuative Marot ring with exactly two regular maximal ideals and it is not weakly additively regular.*

*Proof.* Since $L = K + iK$ is an algebraic extension of $K$, $D'$ is integral over $D$. The fact that $P$ is a common ideal of $D'$ and $D$ and $P^2R' = aR'$ is a regular ideal with $a \in D$ guarantee's that $R'$ is the integral closure of $R$. We also have that $D'_P = D'_{D \backslash P}$ is a discrete rank one valuation domains with maximal ideal $PD'_P$ also the maximal ideal of $D_P$. Hence $D_P$ is a pseudovaluation domain with integral closure $D'_P$. Since $L = K + iK$, there is an element $j \in D' \backslash P$ such that $j + P = i$. If $j$ is not a unit of $D'$, then there is an element $e \in P$ such that $k = j + e$ is a unit with $k + P = j + P = i$. We have $D' = D + kD$ and $D'_P = D_P + kD_P$.

Since the principal ideal $Q^2$ is $Q$-primary, no other prime contains $c$. Similarly no prime other than $P$ contains $b$. By checking locally in $D'$ we have that $Q = aD' + cD'$ and $P = aD' + bD'$. Also note that $a, b, c \in S' \cap D$. Thus checking locally in $D$ shows that $Q_0 = aD + cD$. In addition, since $Q_0 D_{(Q_0)} = QD'_Q$ and $D_{Q_0} = D'_Q$, $Q_0$ is locally principal as an ideal of $D$. Hence $Q_0$ is an invertible maximal ideal of $D$. It follows that each $Q_0$-primary ideal is a power of $Q_0$ and generated by $\{a, c\}^n$ (the $nth$ power of the set $\{a, c\}$) for some positive $n$.

With regard to $P$-primary ideals of $D$, we make use of [8, Theorem 3.5]. As noted above, $D' = D + kD$ and $D'_P = D_P + kD_P$ for some unit $k$ of $D'$. Thus $aD'_P = PD'_P = PD_P = aD_P + kaD_P$ with $a$ and $ka$ in $D \cap S'$. Suppose $x \in a^n D'_P \backslash a^{n+1} D'_P$ for some positive integer $n$. We will show that $xD_P$ contains $P^{n+1} D'_P$.

We have $x = fa^n$ for some unit $f \in D'_P$. We may write $f = g/h$ where $g, h \in D' \backslash P$. Let $q \in a^{n+1} D'_P = P^{n+1} D'_P$. Then $q = ra^{n+1}/s$ for some $r \in D'$ and $s \in D' \backslash P$. Since $f$ is a unit of $D'_P$, $q = ra^{n+1}/s = x(rf^{-1}a/s)$ with $rf^{-1}a/s \in PD_P$. Thus $xD_P$ contains $P^{n+1} D'_P$.

Let $J$ be a $P$-primary ideal of $D$. Then there is a positive integer $m$ such that $b^m \in J$. By [8, Theorem 3.5], we either have $JD_P = P^n D_P$ for some $n$, or $JD_P$ is a principal ideal of $D_P$. If $JD_P = P^n D_P$, then we $JD_P = a^n D_P + ka^n D_P$. By checking locally $J = a^n D + ka^n D + b^m D$ with $a^n, ka^n, b^m \in P \backslash S'$.

Next suppose $JD_P$ is a principal ideal of $D_P$. Then there is a positive integer $n$ and a unit $u \in D'_P$ such that $JD_P = ua^n D_P$. From above, $JD_P$ contains $P^{n+1} D_P$. Since

$u$ is a unit of $D'_P$, there are elements $y, z \in D'\backslash P$ with $z \in D$ such that $u = y/z$. Since $z$ is a unit of $D_P$, we may assume $y = u$. Next let $w \in P$ be such that $u + w$ is a unit of $D'$. Since $wa^n \in P^{n+1}$, $ua^n D_P = (u + w)a^n D_P$. Since $u + w$ is a unit of $D'$, $(u + w)a^n \in P\backslash S'$. Checking locally shows that $J = (u + w)a^n D + b^m D$ (with $(u + w)a^n, b^m \in P\backslash S'$). It follows that $R$ is a Marot ring. Also since $R'$ has exactly two regular maximal ideals with both invertible and neither principal, $R'$ is not weakly additively regular [12, Corollary 3.2]. Thus $R$ is not weakly additively regular.

Finally, since both regular prime ideals of $R'$ are maximal and $R'$ is a Prüfer ring, it is valuative [13, Theorem 2.10] (see Theorem 2.17 above). We also have that $D \subsetneq D'$ is a minimal integral extension and thus $R \subsetneq R'$ is a minimal integral extension. Hence $R$ is valuative by Theorem 3.7. $\square$

For a specific example satisfying the requirements in Theorem 3.14, we adapt the construction used in the proof of [4, Theorem 7].

*Example 3.15.* Let $E = \mathbb{Z}[\sqrt{10}]$ and $E' = E[z_1, z_2, z_3, \ldots]$. For each pair $f, g \in E'$ where no height one prime contains both, there is a smallest positive integer $n$ such that $f, g \in E[z_1, z_2, \ldots, z_n]$. The polynomials $fz_{n+1} + g$ and $f + gz_{n+1}$ are primes of $E'$ (see, for example, [15, Theorem 29, page 85]). Let $\mathscr{S}$ be the multiplicative set generated by these polynomials. Then $D' = E'_{\mathscr{S}}$ is a Dedekind domain, $P = 2D' + \sqrt{10}D'$ and $Q = 5D' + \sqrt{10}D'$ are invertible maximal ideals such that neither is principal, but $P^2 = 2D'$, $Q^2 = 5D'$, and $P \cap Q = \sqrt{10}D'$. We also have $D'/P = \mathbb{Z}_2(z_1, z_2, z_3, \ldots) = \mathbb{Z}_2(z_1^2, z_2, z_3, \ldots) + z_1\mathbb{Z}_2(z_1^2, z_2, z_3, \ldots)$ so the pullback of $\mathbb{Z}_2(z_1^2, z_2, z_3, \ldots)$ over $P$ is a domain $D$ whose integral closure is $D' = D + z_1 D$. Finally note that for $r \in D'\backslash P$, there is an element $s \in \mathscr{S}$ and an integer $m$ such that $r + 2z_m/s$ is a unit of $D'$. By Theorem 3.14, $R$ is a valuative Marot ring with exactly two regular maximal ideals that are neither integrally closed nor weakly additively regular.

## References


1. Cahen, P.-J., Dobbs, D.E., Lucas, T.G.: Valuative domains. J. Algebra Appl. **9**, 43–72 (2010)
2. Cahen, P.-J., Dobbs, D.E., Lucas, T.G.: Characterizing minimal ring extensions. Rocky Mt. J. Math. **41**, 1081–1125 (2011)
3. Cahen, P.-J., Dobbs, D.E., Lucas, T.G.: Valuative pairs of commutative rings. Houst. J. Math. **41**, 397–431 (2015)
4. Claborn, L.: Every Abelian group is a class group. Pac. J. Math. **18**, 219–222 (1966)
5. Dobbs, D.E., Shapiro, J.: A classification of the minimal overrings of certain commutative rings. J. Algebra **308**, 800–821 (2007)
6. Ferrand, D., Olivier, J.-P.: Homomorphismes minimaux d'anneaux. J. Algebra **16**, 461–471 (1970)
7. Griffin, M.: Prüfer rings with zero divisors. J. Reine Angew. Math. **239**(240), 55–67 (1969)
8. Hedstrom, J., Houston, E.: Pseudo-valuation domains. Pac. J. Math. **75**, 137–147 (1978)
9. Huckaba, J.: Commutative Rings with Zero Divisors. Dekker, New York (1988)

10. Lucas, T.G.: Krull rings, Prüfer v-multiplication rings and the ring of finite fractions. Rocky Mt. J. Math. **35**, 1251–1325 (2005)
11. Lucas, T.G.: Additively regular rings and Marot rings. Palest. J. Math. **5**, 90–99 (2016)
12. Lucas, T.G.: Weakly additively regular rings and special families of prime ideals. Palest. J. Math **7**, 14–31 (2017)
13. Lucas, T.G.: Valuative rings. J. Algebra Appl. **17**(7), 1850123, 29 pp (2018)
14. Portelli, D., Spangher, W.: Krull rings with zero divisors. Commun. Algebra **11**, 1817–1851 (1983)
15. Zariski, O., Samuel, P.: Communications in Algebra, II edn. Springer, Berlin (1960)

# Classifying Modules in Add of a Class of Modules with Semilocal Endomorphism Rings

**Pavel Příhoda**

**Abstract** We present a dimension theory for modules in A$dd(\mathcal{C})$, where $\mathcal{C}$ is a class of modules with semilocal endomorphism rings satisfying certain smallness conditions. For example, if $\mathcal{C}$ is the class of all finitely presented modules over a semilocal ring $R$, then we get cardinal invariants which describe pure projective $R$-modules up to isomorphism.

**Keywords** Factor categories · Semilocal endomorphism ring · Direct sum decompositions of modules

Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings satisfying certain smallness conditions which will be specified later. For example, $\mathcal{C}$ can be a class of countably generated Artinian modules over any ring or a class of finitely presented modules over a semilocal ring. In this note we suggest a dimension theory for modules in Add$(\mathcal{C})$, that is, a class of functions assigning cardinal invariants to modules of Add$(\mathcal{C})$ such that two modules of Add$(\mathcal{C})$ are isomorphic if and only if they have the same invariants. Note that if $R$ is a semilocal ring and $\mathcal{C} = \{R\}$, then Add$(\mathcal{C})$ is the class of projective $R$-modules. In [10] we gave the dimension theory for this case, so this paper can be considered as an extension of dimension theory for projective modules over a semilocal ring $R$ to the class of pure projective $R$-modules. Another example studied so far is the class $\mathcal{C}$ of uniserial $R$-modules. In [6] the dimension theory for the class of direct summands of serial modules was presented. This theory appeared to be a useful tool for understanding pure projective modules over serial rings. For example, it enabled to characterize chain domains possessing a pure projective module which is not a direct sum of finitely presented modules as those possessing a nontrivial idempotent one-generated ideal (see [11]).

A dimension theory for classes of modules with semilocal endomorphism ring appeared in [4]. In this note we reconsider these dimensions using factor categories. The application of factor categories in the study of direct-sum decompositions is due

P. Příhoda (✉)
Faculty of Mathematics and Physics, Department of Algebra, Charles University, Sokolovská 83, 186 00 Prague, Czech Republic
e-mail: prihoda@karlin.mff.cuni.cz



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*, Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_15

to Harada and Sai [8], who considered direct sums of modules with local endomorphism rings.

The paper is organized as follows. The first section is of expository character, we follow mostly [7], where a particular case of modules with finite type was considered. Let us point out that there is a more general treatment of the subject in [3]; however, we decided to present the topic in a way sufficient to understand the dimension theory for modules in $\mathrm{Add}(\mathcal{C})$ presented in the third section of the paper. The second section collects relevant properties of $I$-small modules introduced in [6].

## 1 Overview of the Finite Case

Let $R$ be a ring, let $0 \neq M \in \text{Mod-}R$ and let $I$ be an ideal of $\mathrm{End}_R(M)$. Any class of right $R$-modules $\mathcal{D}$ is always considered as a full subcategory of Mod-$R$. The ideal $\mathcal{I}$ of $\mathcal{D}$ *associated to* $I$ is the ideal consisting of all morphisms $f\colon X \to Y \in \mathcal{D}$ such that $\beta f \alpha \in I$ for any pair of homomorphisms $\alpha\colon M \to X$ and $\beta\colon Y \to M$. Observe that if $M$ is an object of $\mathcal{D}$, then $I = \mathcal{I} \cap \mathrm{End}_R(M)$. Notice that the ideal $\mathcal{I}$ depends on $I$ and $\mathcal{D}$, so the notation should be, for example, $\mathcal{I}_{I,\mathcal{D}}$ but $\mathcal{D}$ and $I$ will always be specified or obvious from the context.

Let us recall the definition of the Jacobson radical of the category according to Mitchell [9]. Let $\mathcal{D}$ be a full category of Mod-$R$ and set $\mathcal{J}(\mathcal{D}) := \{f \in \mathcal{D}(X,Y) \mid 1_X - gf$ is left invertible in $\mathrm{End}_{\mathcal{D}}(X)$ for every $g \in \mathcal{D}(Y,X)\}$. The original definition in [9] was for small preadditive categories and $\mathcal{J}$ was defined as the intersection of all maximal right ideals of $\mathcal{D}$. However, we just need to know that $\mathcal{J}(\mathcal{D})$ is an ideal of $\mathcal{D}$ and $\mathcal{J}(N,N)$ is $J(\mathrm{End}_R(N))$ for every $N \in \mathcal{D}$. The first statement is proved in [9, Lemma 4.1, Lemma 4.2] and the second one follows directly from the definition of $\mathcal{J}$. Observe that $f \in \mathcal{J}(\mathcal{D})$ if and only if, for every $N \in \mathcal{D}$, the ideal of $\mathcal{D}$ associated to $J(\mathrm{End}_R(N))$ contains $f$. Note that if $M$ is a module with semilocal endomorphism ring and $I$ is a maximal ideal of $\mathrm{End}_R(M)$, then the ideal of $\mathcal{D}$ associated to $\mathcal{I}$ contains $\mathcal{J}(\mathcal{D})$.

Most of the following results appeared in [3].

**Lemma 1.1.** *Let $M, N$ be nonzero modules with semilocal endomorphism rings, let $I$ be a maximal ideal of* $\mathrm{End}_R(M)$*, and let $\mathcal{I}$ be the ideal of $\mathcal{D}$ associated to $I$, where $\mathcal{D}$ is a class of modules containing $N$. Then either* $\mathcal{I} \cap \mathrm{End}_R(N) = \mathrm{End}_R(N)$ *or* $\mathcal{I} \cap \mathrm{End}_R(N)$ *is a maximal ideal of* $\mathrm{End}_R(N)$.

Proof. The arguments from the proof of [7, Lemma 4.4] can be used to check that $J(\mathrm{End}_R(N)) \subseteq J := \mathcal{I} \cap \mathrm{End}_R(N)$. The rest of the proof needs a slight modification: Suppose that $J \neq \mathrm{End}_R(N)$, so we have to prove that $\mathrm{End}_R(N)/J$ is a simple Artinian ring. Let $f, g \in \mathrm{End}_R(N)$ be such that $f + J, g + J$ are nontrivial orthogonal central idempotents of $\mathrm{End}_R(N)/J$. There exist $\alpha, \alpha'\colon M \to N$ and $\beta, \beta'\colon N \to M$ such that $\beta f \alpha \notin I$ and $\beta' g \alpha' \notin I$. Then $(\mathrm{End}_R(M)\beta f \alpha + I)/I$ is a nonzero left ideal and $(\beta' g \alpha' \mathrm{End}_R(M) + I)/I$ is a nonzero right ideal of a simple Artinian ring $\mathrm{End}_R(M)/I$, so $\beta' g \alpha' \mathrm{End}_R(M) \beta f \alpha + I \nsubseteq I$. On the other hand

$g\alpha'\mathrm{End}_R(M)\beta f \subseteq J$ (use $g+J$, $f+J$ are orthogonal and central), and $\beta' J\alpha \subseteq I$, since $J \subseteq \mathcal{I}$. This contradiction proves the lemma. ■

**Lemma 1.2.** *Let $M, N$ be nonzero modules with semilocal endomorphism rings contained in a class $\mathcal{D} \subseteq$ Mod-$R$, let $I$ be a maximal ideal of $\mathrm{End}_R(M)$ and let $\mathcal{I}$ be the ideal of $\mathcal{D}$ associated to $I$. Assume $J := \mathcal{I} \cap \mathrm{End}_R(N) \neq \mathrm{End}_R(N)$. Then $\mathcal{I}$ is the ideal of $\mathcal{D}$ associated to $J$.*

Proof. Let $f : X \to Y \in \mathcal{D}$ be such that $f$ is not in the ideal of $\mathcal{D}$ associated to $J$. Then there are $\alpha : N \to X$ and $\beta : Y \to N$ such that $\beta f \alpha \notin J = \mathcal{I} \cap \mathrm{End}_R(N)$. In particular, $f \notin \mathcal{I}$.

Conversely, assume that $f : X \to Y \in \mathcal{D}$ is not in $\mathcal{I}$, i.e., there are $\alpha : M \to X$ and $\beta : Y \to M$ such that $g := \beta f \alpha \notin I$. If $g$ is in the ideal of $\mathcal{D}$ associated to $J$, then $\mathrm{Hom}_R(M, N)(\mathrm{End}_R(M)g\mathrm{End}_R(M) + I)\mathrm{Hom}_R(N, M) \subseteq J$. It follows that the whole $\mathrm{End}_R(M)$ is in the ideal of $\mathcal{D}$ associated to $J$. Fix $\varphi : M \to N$, $\psi : N \to M$ such that $\psi\varphi \notin I$. Then $\psi\varphi\mathrm{End}_R(M)\psi\varphi \nsubseteq I$. But $\varphi\mathrm{End}_R(M)\psi \subseteq J \subseteq \mathcal{I}$, which is a contradiction. So $g$ is not in the ideal of $\mathcal{D}$ associated to $J$ and there are homomorphisms $\alpha' : N \to M$ and $\beta' : M \to N$ such that $\beta'\beta f \alpha\alpha' \notin J$. Thus $f$ is not in the ideal of $\mathcal{D}$ associated to $J$. ■

For a given class $\mathcal{C}$ of modules with semilocal endomorphism rings, let $\mathrm{Spec}(\mathcal{C})$ be the class of ideals in the category $\mathcal{C}$ such that $\mathcal{I} \in \mathrm{Spec}(\mathcal{C})$ if and only if $\mathcal{I}$ is associated to a maximal ideal of $\mathrm{End}_R(M)$ for some nonzero object $M$ of $\mathcal{C}$. For each $M \in \mathcal{C}$, set $V(M) := \{\mathcal{I} \in \mathrm{Spec}(\mathcal{C}) \mid 1_M \notin \mathcal{I}\}$, so that $V(M)$ is the finite set of ideals associated to the maximal ideals of $\mathrm{End}_R(M)$.

**Lemma 1.3.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings and let $M, N, M \oplus N \in \mathcal{C}$. Then $V(M) \cup V(N) = V(M \oplus N)$.*

Proof. If $\mathcal{I} \in V(M)$, then $1_{M\oplus N} \notin \mathcal{I}$, otherwise $1_M = \pi_M 1_{M\oplus N}\iota_M$ would imply $1_M \in \mathcal{I}$. Then $\mathcal{I} \in V(M \oplus N)$. Similarly, $\mathcal{I} \in V(N)$ implies $\mathcal{I} \in V(M \oplus N)$ and $V(M) \cup V(N) \subseteq V(M \oplus N)$ follows.

Conversely, if $\mathcal{I} \in V(M \oplus N)$, then $1_{M\oplus N} = \iota_M 1_M \pi_M + \iota_N 1_N \pi_N$ implies that either $1_M \notin \mathcal{I}$ or $1_N \notin \mathcal{I}$. Consequently, $\mathcal{I} \in V(M)$ or $\mathcal{I} \in V(N)$ and $V(M \oplus N) \subseteq V(M) \cup V(N)$. ■

For each $\mathcal{I} \in \mathrm{Spec}(\mathcal{C})$ we would like to define a 'dimension function' $\dim_{\mathcal{I}}$ assigning a cardinal number to every object of $\mathcal{C}$. These 'functions' should describe modules of $\mathcal{C}$ up to isomorphism, i.e., $X, Y \in \mathcal{C}$ should be isomorphic if and only if $\dim_{\mathcal{I}}(X) = \dim_{\mathcal{I}}(Y)$ for every $\mathcal{I} \in \mathrm{Spec}(\mathcal{C})$.

For any $M, N \in \mathcal{C}$ and $\mathcal{I} \in \mathrm{Spec}(\mathcal{C})$ consider the group $\mathrm{Hom}_R(M, N)/\mathcal{I}(M, N)$. It is zero if $1_M \in \mathcal{I}$. Otherwise $I := \mathcal{I}(M, M)$ is a maximal ideal of $\mathrm{End}_R(M)$ and $\mathrm{End}_R(M)/I$ is a simple Artinian ring. Therefore $\mathrm{Hom}_R(M, N)/\mathcal{I}(M, N)$ has a natural structure of a right module over $\mathrm{End}_R(M)/I$ so we would like to define the $\mathcal{I}$-dimension of $N$ to be the length of this module. Of course, it is necessary to check that the definition is independent of the choice of $M$. In fact, observe that $\mathrm{Hom}_R(M, N)/\mathcal{I}(M, N) = 0$ if $1_N \in \mathcal{I}$. Otherwise we can check that the composition length of $\mathrm{Hom}_R(M, N)/\mathcal{I}(M, N)$ is just the dual Goldie dimension of the ring $\mathrm{End}_R(N)/\mathcal{I}(N, N)$.

**Lemma 1.4.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings, $M, N \in \mathcal{C}$ and let $\mathcal{I} \in \operatorname{Spec}(\mathcal{C})$. Then $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N) = 0$ if $1_M \in \mathcal{I}$ or $1_N \in \mathcal{I}$. If $1_M \notin \mathcal{I}$ and $1_N \notin \mathcal{I}$, the length of $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N)$, considered as a right $\operatorname{End}_R(M)/\mathcal{I}(M, M)$-module, is the same as the dual Goldie dimension of $\operatorname{End}_R(N)/\mathcal{I}(N, N)$.*

Proof. The first part of the statement is obvious. Suppose that $1_M, 1_N \notin \mathcal{I}$. Then it follows from Lemma 1.2 that the ideals of $\mathcal{C}$ associated to $\mathcal{I}(M, M)$ and $\mathcal{I}(N, N)$ are both equal to $\mathcal{I}$. Put $I := \mathcal{I}(N, N)$. Let $e_1, \dots, e_k \in \operatorname{End}_R(N)$ be such that $e_1 + I, \dots, e_k + I$ is a complete set of primitive orthogonal idempotents of $\operatorname{End}_R(N)/I$. Then $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N) = \oplus_{i=1}^k (e_i \operatorname{Hom}_R(M, N) + \mathcal{I}(M, N))/\mathcal{I}(M, N)$. Note that for any $1 \le i \le k$ the module $e_i \operatorname{Hom}_R(M, N) + \mathcal{I}(M, N)/\mathcal{I}(M, N)$ is not zero: Since $e_i \notin \mathcal{I}$ and $\mathcal{I}$ is the ideal of $\mathcal{C}$ associated to $\mathcal{I}(M, M)$, $e_i \operatorname{Hom}_R(M, N) \subseteq \mathcal{I}$ cannot hold.

It remains to prove that for every $1 \le i \le k$ the $\operatorname{End}_R(M)/\mathcal{I}(M, M)$-module $e_i \operatorname{Hom}_R(M, N) + \mathcal{I}(M, N)/\mathcal{I}(M, N)$ is simple. Take $f \colon M \to N$ such that $e_i f \notin \mathcal{I}$. Then there exists $h \colon N \to M$ such that $e_i f h \notin \mathcal{I}$ since $\mathcal{I}$ is associated to $I$. Consequently, $e_i f h t - e_i \in I$ for some $t \in \operatorname{End}_R(N)$. Then $e_i f(htg) - e_i g \in \mathcal{I}(M, N)$ for every $g \colon M \to N$. ■

*Remark 1.5.* The previous proof gives a way of finding a decomposition of the $\operatorname{End}_R(M)/\mathcal{I}(M, M)$-module $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N)$ into a direct sum of simple modules: Fix some complete set of orthogonal primitive idempotents $e_1 + I, \dots, e_k + I$ of the ring $\operatorname{End}_R(N)/I$, where $I = \mathcal{I}(N, N)$. If $f + \mathcal{I}(M, N)$ belongs to $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N)$, then $(e_1 f + \mathcal{I}(M, N), \dots, e_k f + \mathcal{I}(M, N))$ is the decomposition of $f + \mathcal{I}(M, N)$ in the direct-sum decomposition $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N) = \oplus_{i=1}^k (e_i \operatorname{Hom}_R(M, N) + \mathcal{I}(M, N))/\mathcal{I}(M, N)$. So $f + \mathcal{I}(M, N) \mapsto e_i f + \mathcal{I}(M, N)$ can be considered as the canonical projection $\pi_i \colon \operatorname{Hom}_R(M, N)/\mathcal{I}(M, N) \to (e_i \operatorname{Hom}_R(M, N) + \mathcal{I}(M, N))/\mathcal{I}(M, N)$ with respect to this decomposition of $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N)$. We will use this fact in the proof of Proposition 1.7.

It is also possible to consider $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N)$ as a left module over $\operatorname{End}_R(N)/\mathcal{I}(N, N)$ and use its length to define the $\mathcal{I}$-dimension of $M$. Similarly one can show that the length of this left module is the dual Goldie dimension of $\operatorname{End}_R(M)/\mathcal{I}(M, M)$. So these two definitions coincide. Of course, it is not true that the bimodule $\operatorname{Hom}_R(M, N)/\mathcal{I}(M, N)$ has same lengths on both sides. Indeed, take a simple $R$-module $S$ and set $M := S$, $N := S \oplus S$, let $\mathcal{I}$ be the ideal of Mod-$R$ associated to the zero ideal of $\operatorname{End}_R(M)$, then $\mathcal{I}(M, M), \mathcal{I}(M, N), \mathcal{I}(N, N)$ are all zero, $\operatorname{Hom}_R(M, N)$ is of length two as a right $\operatorname{End}_R(M)$-module but of length one as a left $\operatorname{End}_R(N)$-module.

If $\mathcal{C}$ is a class of modules with semilocal endomorphism rings, $\mathcal{I} \in \operatorname{Spec}(\mathcal{C})$ and $N \in \mathcal{C}$, we define $\dim_{\mathcal{I}}(N)$ to be the dual Goldie dimension of $\operatorname{End}_R(N)/\mathcal{I}(N, N)$ (if $\mathcal{I} \notin V(N)$, then $\dim_{\mathcal{I}}(N) = 0$). As remarked above, there is another interpretation of $\dim_{\mathcal{I}}$. The factor category $\mathcal{C}/\mathcal{I}$ has a fully faithful embedding to a category of finitely generated modules over a division ring (see Proposition 1.7 below). Then $\dim_{\mathcal{I}}(N)$

is the length of the corresponding module. Let us make a remark on uniqueness of such an embedding.

*Remark 1.6.* Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings, let $M$ be a nonzero module of $\mathcal{C}$, $I$ a maximal ideal of $\mathrm{End}_R(M)$, and let $\mathcal{I}$ be the ideal of $\mathcal{C}$ associated to $I$. Suppose that $F\colon \mathcal{C}/\mathcal{I} \to \text{mod-}K$ and $G\colon \mathcal{C}/\mathcal{I} \to \text{mod-}K'$ are full and faithful functors into the categories of finitely generated modules over division rings $K, K'$. Then $K \simeq K'$, since $K \simeq e\mathrm{End}_K(F(M))e$ for every primitive idempotent $e \in \mathrm{End}_K(F(M))$ and $K' \simeq e'\mathrm{End}_{K'}(G(M))e'$ for every primitive idempotent $e' \in \mathrm{End}_{K'}(G(M))$. Moreover, for every $N \in \mathcal{C}$ dimensions (or lengths) $\dim_K(F(N))$ and $\dim_{K'}(G(N))$ both coincide with the dual Goldie dimension of $\mathrm{End}_R(N)/\mathcal{I}(N, N)$. (Observe that $\mathrm{End}_K(F(N)) \simeq \mathrm{End}_{\mathcal{C}/\mathcal{I}}(N)$. The dual Goldie dimension of $\mathrm{End}_K(F(N))$ is $\dim_K(F(N))$.)

**Proposition 1.7.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings and let $0 \neq M \in \mathcal{C}$. If $\mathcal{I}$ is the ideal of $\mathcal{C}$ associated to a maximal ideal $I$ of $\mathrm{End}_R(M)$, then there exists a division ring $K$ and a full and faithful functor $\mathcal{C}/\mathcal{I} \to \text{mod-}K$.*

Proof. Let $F\colon \mathcal{C} \to \mathcal{C}/\mathcal{I}$ be the canonical functor and let $S := \mathrm{End}_R(M)/I$. Consider the functor $G := \mathrm{Hom}_{\mathcal{C}/\mathcal{I}}(F(M), -)\colon \mathcal{C}/\mathcal{I} \to \text{Mod-}S$. In the proof of Lemma 1.4 we have seen that $G(F(N))$ is a finitely generated module, so we have to show that $G$ is full and faithful.

Let $f\colon X \to Y \in \mathcal{C}$ be such that $F(f) \neq 0$. Then $\beta f \alpha \notin I$ for some $\alpha\colon M \to X$ and $\beta\colon Y \to M$. In particular, $f\alpha \notin \mathcal{I}$ and $G(F(f))(F(\alpha)) \neq 0$. So $G$ is faithful.

In order to prove that $G$ is full, consider $N_1, N_2 \in \mathcal{C}$ such that $F(N_1) \neq 0$ and $F(N_2) \neq 0$. Let $I_i := \mathcal{I}(M, N_i)$, $i = 1, 2$. Let $e_1, \dots, e_k \in \mathrm{End}_R(N_1)$ and $f_1, \dots, f_l \in \mathrm{End}_R(N_2)$ be such that $F(e_1), \dots, F(e_k)$ is a complete set of orthogonal primitive idempotents of $\mathrm{End}_{\mathcal{C}/\mathcal{I}}(F(N_1))$ and $F(f_1), \dots, F(f_l)$ is a complete set of orthogonal primitive idempotents of $\mathrm{End}_{\mathcal{C}/\mathcal{I}}(F(N_2))$. By Remark 1.5, $GF(N_1) = \oplus_{j=1}^{k}(e_j\mathrm{Hom}_R(M, N_1) + I_1)/I_1$ and $GF(N_2) = \oplus_{j=1}^{l}(f_j\mathrm{Hom}_R(M, N_2) + I_2)/I_2$.

For every $i \in \{1, \dots, k\}$ there exists $\alpha_i\colon N_1 \to M$ such that $\alpha_i e_i \notin \mathcal{I}$ and for every $j \in \{1, \dots, l\}$ there exists $\beta_j\colon M \to N_2$ such that $f_j\beta_j \notin \mathcal{I}$. Since $S$ is simple Artinian and the $S$-modules $(e_i\mathrm{Hom}_R(M, N_1) + I_1)/I_1$, $(f_j\mathrm{Hom}_R(M, N_2) + I_2)/I_2$ are simple, $\mathrm{Hom}_S((e_i\mathrm{Hom}_R(M, N_1) + I_1)/I_1, (f_j\mathrm{Hom}_R(M, N_2) + I_2)/I_2) = \pi_j^2 \circ GF(\beta_j) \circ \mathrm{End}_S(S) \circ GF(\alpha_i) \circ \iota_i^1$, where $\iota_i^1\colon (e_i\mathrm{Hom}_R(M, N_1) + I_1)/I_1 \to GF(N_1)$ is the canonical embedding and $\pi_j^2\colon GF(N_2) \to (f_j\mathrm{Hom}_R(M, N_2) + I_2)/I_2$ is the canonical projection. Observe that $\mathrm{End}_S(S) = G(\mathrm{End}_{\mathcal{C}/\mathcal{I}}F(M))$. Further, let $\iota_i^2\colon (f_i\mathrm{Hom}_R(M, N_2) + I_2)/I_2 \to GF(N_2)$ be the canonical embedding and $\pi_j^1\colon GF(N_1) \to (e_j\mathrm{Hom}_R(M, N_1) + I_1)/I_1$ be the canonical projection. As remarked above, $GF(e_i) = \iota_i^1\pi_i^1$ and $GF(f_j) = \iota_j^2\pi_j^2$.

Let $\varphi \in \mathrm{Hom}_S(GF(N_1), GF(N_2))$. Then $\varphi = \sum_{i=1,j=1}^{k,l} G(F(f_j))\varphi G(F(e_i))$ and $G(F(f_j))\varphi G(F(e_i)) = \iota_j^2\pi_j^2\varphi\iota_i^1\pi_i^1$, $\pi_j^2\varphi\iota_i^1 = \pi_j^2 GF(\psi_{j,i})\iota_i^1$ for some $\psi_{j,i}\colon N_1 \to N_2$. Therefore $\varphi = GF(\sum_{i=1,j=1}^{k,l} f_j\psi_{j,i}e_i)$.

To conclude the proof, observe that mod-$S$ is equivalent to mod-$K$, where $K$ is the endomorphism ring of the unique simple $S$-module.

Now let us reformulate several results from [7] to our setting. The next lemma has the same proof as [7, Lemma 4.7, Lemma 4.8].

**Lemma 1.8.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings, $M_1, \dots, M_n \in \mathcal{C}$ and $S = \mathrm{End}_R(M_1 \oplus \dots \oplus M_n)$. The following conditions are equivalent for an endomorphism $f \in S$:*

*(i)* $f \in J(S)$.
*(ii)* $\pi_j f \iota_i \in \mathcal{I}(M_i, M_j)$ *for every* $i, j = 1, \dots, n$ *and every* $\mathcal{I} \in \cup_{k=1}^{n} V(M_k)$.
*(iii)* *For every* $i, j = 1, \dots, n$ *and for every* $\mathcal{P} \in V(M_i) \cap V(M_j)$ *in the category* $\mathcal{C}$, *one has* $\pi_j f \iota_i \in \mathcal{P}$.

*Moreover, if $A$ is a direct summand of $\oplus_{k=1}^{n} M_k$, then $g \in J(\mathrm{End}_R(A))$ if and only if $g$ is in every ideal of* Mod-$R$ *which is associated to a maximal ideal of* $\mathrm{End}_R(M_i)$ *for some* $i = 1, \dots, n$.

The proof of [7, Theorem 4.10] can be also transferred to our setting.

**Proposition 1.9.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings, let $M, N$ be direct summands of a finite direct sum of modules in $\mathcal{C}$. Then $M \simeq N$ if and only if* $\dim_{\mathcal{I}}(M) = \dim_{\mathcal{I}}(N)$ *for every* $\mathcal{I} \in \mathrm{Spec}(\mathrm{add}(\mathcal{C}))$.

PROOF. Note that $V(M) = V(N) = \{\mathcal{I}_1, \dots, \mathcal{I}_k\}$ is a finite set of ideals in $\mathrm{add}(\mathcal{C})$. If $k = 0$, then $M = N = 0$. Assume $k > 0$. For every $1 \le i \le k$ let $I_i = \mathcal{I}_i(M, M)$ and $J_i = \mathcal{I}_i(N, N)$. By Lemma 1.1, $I_1, \dots, I_k$ are the maximal ideals of $\mathrm{End}_R(M)$ and $J_1, \dots, J_k$ are the maximal ideals of $\mathrm{End}_R(N)$. Let $e_i \in \mathrm{End}_R(M)$, $f_i \in \mathrm{End}_R(N)$ be such that $e_i, f_i \in \mathcal{I}_j$ for every $j \ne i$ and $1_M - e_i, 1_N - f_i \in \mathcal{I}_i$. By Proposition 1.7, for every $1 \le i \le k$ there are homomorphisms $\alpha_i \colon M \to N$ and $\beta_i \colon N \to M$ inducing mutually inverse isomorphisms of $M$ and $N$ in Mod-$R/\mathcal{I}_i$. Consider $\alpha := \sum_{j=1}^{k} \alpha_i e_i \colon M \to N$ and $\beta := \sum_{i=1}^{k} \beta_i f_i$. Then $1_M - \beta\alpha \in I_1 \cap \dots \cap I_k = J(\mathrm{End}_R(M))$ and $1_N - \alpha\beta \in J_1 \cap \dots \cap J_k = J(\mathrm{End}_R(N))$. So $\beta\alpha$ and $\alpha\beta$ are isomorphisms, therefore $M \simeq N$. ∎

*Remark 1.10.* Note that, by Lemma 1.3, every ideal of $\mathrm{Spec}(\mathrm{add}(\mathcal{C}))$ is in $V(C)$ for some $C \in \mathcal{C}$. Therefore it is possible to extend dimension functions classifying objects in $\mathcal{C}$ to get a dimension theory for $\mathrm{add}(\mathcal{C})$.

## 2 *I*-small Modules

Recall that a family $f_\lambda, \lambda \in \Lambda$, of elements of $\mathrm{Hom}_R(X, Y)$ is called *summable* if, for any $x \in X$, $f_\lambda(x) = 0$, for all but finitely many $\lambda \in \Lambda$. If $f_\lambda, \lambda \in \Lambda$, is a summable family in $\mathrm{Hom}_R(X, Y)$, then we can define the homomorphism $f := \sum_{\lambda \in \Lambda} f_\lambda$ by $f(x) = \sum_{\lambda \in \Lambda, f_\lambda(x) \ne 0} f_\lambda(x)$.

Let us recall the notion of $I$-small module: Let $M$ be a module, $I$ an ideal of $\mathrm{End}_R(M)$. We say that $M$ is $I$-*small* provided for every summable family $f_\lambda, \lambda \in \Lambda$, of endomorphisms in $I$ the sum $\sum_{\lambda \in \Lambda} f_\lambda$ is in $I$. If $\mathcal{A}$ is a class of modules closed under arbitrary direct sums and $\mathcal{I}$ is an ideal of $\mathcal{A}$ closed under sums of summable families of morphisms, then the canonical functor $F\colon \mathcal{A} \to \mathcal{A}/\mathcal{I}$ preserves coproducts ([6, Lemma 2.5]). Thus, if we want to define the dimension function $\dim_{\mathcal{I}}$ on objects of $\mathcal{A}$ in such a way that $\dim_{\mathcal{I}}$ is compatible with arbitrary direct sums of objects in $\mathcal{A}$, the condition of $\mathcal{A}$ being $\mathcal{I}$-small introduced below seems to be essential. Let us recall [6, Corollary 2.7].

**Proposition 2.1.** *Let $\mathcal{A}$ be a full subcategory of* Mod-$R$ *closed under arbitrary direct sums. Suppose that $U$ is a nonzero module and $I$ is an ideal of* $\mathrm{End}_R(U)$ *such that $U$ is $I$-small. If $\mathcal{I}$ is the ideal of $\mathcal{A}$ associated to $I$, then the canonical functor $F\colon \mathcal{A} \to \mathcal{A}/\mathcal{I}$ preserves coproducts.*

Let $\mathcal{A}$ be a full subcategory of Mod-$R$ and let $\mathcal{I}$ be an ideal of $\mathcal{A}$. We say that $\mathcal{A}$ is $\mathcal{I}$-*small* if the sum of every summable family of morphisms of $\mathcal{I}$ is in $\mathcal{I}$.

**Lemma 2.2.** *Let $\mathcal{A}$ be a full subcategory of* Mod-$R$ *containing modules $M, N$. Let $\mathcal{I}$ be the ideal of $\mathcal{A}$ associated to an ideal $I$ of the ring* $\mathrm{End}_R(M)$. *Then the following are equivalent:*

*(i) $M$ is $I$-small.*
*(ii) $\mathcal{A}$ is $\mathcal{I}$-small.*

*In particular, if $M$ is $I$-small, then $N$ is $\mathcal{I}(N, N)$-small.*

Proof. (i) follows immediately from (ii), let us prove the converse. Take modules $X, Y \in \mathcal{A}$ and a summable family of homomorphisms $f_\lambda\colon X \to Y$, $\lambda \in \Lambda$. Suppose that the sum $f = \sum_{\lambda\in\Lambda} f_\lambda$ is not in $\mathcal{I}$, that is, there are $g\colon M \to X$ and $h\colon Y \to M$ such that $hfg \notin \mathcal{I}$. Observe that $hf_\lambda g$, $\lambda \in \Lambda$ is a summable family in $I$ and that $\sum_{\lambda\in\Lambda} hf_\lambda g = hfg$. So $M$ cannot be $I$-small in this case.

Recall that an $R$-module $M$ is *small* if for every family $N_\lambda$, $\lambda \in \Lambda$, of $R$-modules the canonical homomorphism $\alpha\colon \oplus_{\lambda\in\Lambda} \mathrm{Hom}_R(M, N_\lambda) \to \mathrm{Hom}_R(M, \oplus_{\lambda\in\Lambda} N_\lambda)$ is an isomorphism. Lemma 2.3 explains how to understand the relation between being small and being $I$-small in our particular case.

**Lemma 2.3.** *Let $\mathcal{A}$ be a full subcategory of* Mod-$R$, *let $M, N_\lambda$, $\lambda \in \Lambda$ be modules of $\mathcal{A}$ such that* $\mathrm{End}_R(M)$ *is semilocal and $\oplus_{\lambda\in\Lambda} N_\lambda$ is in $\mathcal{A}$. Let $\mathcal{I}$ be the ideal of $\mathcal{A}$ associated to a maximal ideal $I$ of* $\mathrm{End}_R(M)$. *If $M$ is $I$-small, then for any $f\colon M \to \oplus_{\lambda\in\Lambda} N_\lambda$ there is a finite set $\Lambda_0 \subseteq \Lambda$ such that $\pi_\lambda f \in \mathcal{I}$ for every $\lambda \in \Lambda \setminus \Lambda_0$.*

Proof. Let $e_1, \ldots, e_n \in \mathrm{End}_R(M)$ be such that $e_1 + I, \ldots, e_n + I$ is a complete set of primitive orthogonal idempotents of $\mathrm{End}_R(M)/I$. Suppose that the statement is not true for $f\colon M \to \oplus_{\lambda\in\Lambda} N_\lambda$. Then there exists $i \in \{1, \ldots, n\}$ and pairwise different elements $\lambda_1, \lambda_2, \cdots \in \Lambda$ such that $\pi_{\lambda_j} f e_i \notin \mathcal{I}$ for every $j \in \mathbb{N}$. For simplicity suppose that $i = 1$. Then there are $h_j\colon N_{\lambda_j} \to M$ such that $t'_j := e_1 h_j \pi_{\lambda_j} f e_1 \notin I$ for every $j \in \mathbb{N}$. Since $(e_1 + I)\mathrm{End}_R(M)/I(e_1 + I)$ is a division ring, we can suppose that $t_j := e_1 - e_1 h_j \pi_{\lambda_j} f e_1 \in I$ for every $j = 1, 2, \ldots$. Consider a countable family $t_1, t_2 - t_1, t_3 - t_2, \ldots$. This is a summable family of homomorphisms in $I$ but the sum of this family is $e_1 \notin I$, which is impossible if $M$ is $I$-small. ■

**Corollary 2.4.** *Let $\mathcal{A}$ be a full subcategory of* Mod-$R$ *closed under (arbitrary) direct sums. Let $M$ be a module of $\mathcal{A}$ such that* $\mathrm{End}_R(M)$ *is semilocal and let $I$ be a maximal ideal of* $\mathrm{End}_R(M)$. *If $M$ is $I$-small, then the functor*

$$\mathrm{Hom}_R(M,-)/\mathcal{I}(M,-)\colon \mathcal{A} \to \text{Mod-}\mathrm{End}_R(M)/I$$

*commutes with direct sums.*

**Lemma 2.5.** *Let $M$ be a nonzero module with semilocal endomorphism ring. Then $M$ is $J(\mathrm{End}_R(M))$-small if and only if $M$ is $I$-small for every maximal ideal $I$ of* $\mathrm{End}_R(M)$.

PROOF. Suppose that $M$ is $I$-small for every maximal ideal $I \subseteq \mathrm{End}_R(M)$. Take any summable family $f_\lambda$, $\lambda \in \Lambda$ in $J(\mathrm{End}_R(M))$. Then $f := \sum_{\lambda\in\Lambda} f_\lambda \in I$ for every maximal ideal $I \subseteq \mathrm{End}_R(M)$. Therefore also $f \in J(\mathrm{End}_R(M))$.

Conversely, suppose $M$ is $J(\mathrm{End}_R(M))$-small and there is a maximal ideal $I' \subseteq \mathrm{End}_R(M)$ such that $M$ is not $I'$-small. Then there exists a summable family $f_\lambda$, $\lambda \in \Lambda$ in $I'$ such that $f := \sum_{\lambda\in\Lambda} f_\lambda$ is not in $I'$. Let $g \in \mathrm{End}_R(M)$ be such that $g \in I$ for every maximal ideal $I' \neq I \subseteq \mathrm{End}_R(M)$ and $1_M - g \in I'$. Then $gf_\lambda$, $\lambda \in \Lambda$ is a summable family in $J(\mathrm{End}_R(M))$ with the sum $g\sum_{\lambda\in\Lambda} f_\lambda \notin I'$. This is a contradiction. ■

*Example 2.6.* (i) If $M$ is a finitely generated module, then $M$ is $I$-small for every ideal $I \subseteq \mathrm{End}_R(M)$. This is obvious since every summable family in $\mathrm{End}_R(M)$ has only finitely many nonzero members. In particular, a Noetherian module of finite dual Goldie dimension has semilocal endomorphism ring (cf. [5, Theorem 4.3(b)]) and is $I$-small for every maximal ideal $I \subseteq \mathrm{End}_R(M)$. Similarly, if $M$ is a finitely presented module over a semilocal ring $R$, then, by [2, Theorem 3.3], $\mathrm{End}_R(M)$ is semilocal and $M$ is $I$-small for every maximal ideal $I$ of $\mathrm{End}_R(M)$.
(ii) Let $M$ be an $R$-module such that $\mathrm{End}_R(M)$ is local. Then $M$ is $J(\mathrm{End}_R(M))$-small by [6, beginning of Section 6].
(iii) Let $M$ be an Artinian $R$-module with socle $S$. It is not true in general that $\mathrm{End}_R(M)$ is local if $M$ is indecomposable (see [5, Example 8.19]). However, by [1, Corollary 6], $\mathrm{End}_R(M)$ is semilocal. Note that $J_0 := \{f \in \mathrm{End}_R(M) \mid f(S) = 0\} \subseteq J(\mathrm{End}_R(M))$. Any summable family of $\mathrm{End}_R(M)$ has almost all its members in $J_0$. In particular, $M$ is $J(\mathrm{End}_R(M))$-small. By Lemma 2.5, $M$ is $I$-small for every maximal ideal $I \subseteq \mathrm{End}_R(M)$.

In the next section, we give a dimension theory for modules in $\mathrm{Add}(\mathcal{C})$, where $\mathcal{C}$ is either a class of Noetherian modules of finite dual Goldie dimension or a class of (unfortunately) countably generated Artinian modules or a class of finitely presented modules if the ring is semilocal.

## 3 The Infinite Case

We would like to extend Proposition 1.9 to infinite direct sums of modules with semilocal endomorphism rings. Of course, it is necessary to extend the definition of $\dim_{\mathcal{I}}$ to infinite direct sums. There is an obvious way: Let $M$ be a module with semilocal endomorphism ring, $I$ a maximal ideal of $\mathrm{End}_R(M)$, and let $\mathcal{I}$ be the ideal of the category Mod-$R$ associated to $I$. Then $\mathrm{Hom}_R(M, N)/\mathcal{I}(M, N)$ has a canonical structure of a module over a simple Artinian ring $\mathrm{End}_R(M)/I$. Let $S$ be the simple right $\mathrm{End}_R(M)/I$-module. For $N \in$ Mod-$R$ we would like to define $\dim_{\mathcal{I}}(N) = \kappa$, if $\mathrm{Hom}_R(M, N)/\mathcal{I}(M, N) \simeq S^{(\kappa)}$. Of course, it is necessary to check that such a definition is independent of the choice of $M$ and $I$.

**Proposition 3.1.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings, $M, N \in \mathcal{C}$ and $\mathcal{I}' \in V(M) \cap V(N)$. Let $\mathcal{I}$ be the ideal of* Mod-$R$ *associated to $\mathcal{I}'(M, M)$. Then for an arbitrary module $X$, the length of* $\mathrm{End}_R(M)/\mathcal{I}(M, M)$-*module* $\mathrm{Hom}_R(M, X)/\mathcal{I}(M, X)$ *is the same as the length of* $\mathrm{End}_R(N)/\mathcal{I}(N, N)$-*module* $\mathrm{Hom}_R(N, X)/\mathcal{I}(N, X)$ *(since there are no assumptions on $X$ these lengths can be infinite).*

Proof. Let $I := \mathcal{I}(M, M)$, $J := \mathcal{I}(N, N)$, $S := \mathrm{End}_R(M)/I$ and $T := \mathrm{End}_R(N)/J$. Assume that $M$ and $N$ are isomorphic in Mod-$R/\mathcal{I}$. Let $\varphi\colon M \to N$, $\psi\colon N \to M$ be homomorphisms such that $1_M - \psi\varphi, 1_N - \varphi\psi \in \mathcal{I}$ and let us denote $\overline{\varphi}, \overline{\psi}$ the corresponding morphisms in Mod-$R/\mathcal{I}$. In this case $S$ and $T$ are isomorphic via $\theta\colon S \to T$, $\theta(s) = \overline{\varphi} s \overline{\psi}$. Observe that the homomorphism $\mathrm{Hom}_R(\psi, X)$ induces a group isomorphism $\Phi\colon \mathrm{Hom}_R(M, X)/\mathcal{I}(M, X) \to \mathrm{Hom}_R(N, X)/\mathcal{I}(N, X)$ given by $\Phi(f + \mathcal{I}(M, X)) := f\psi + \mathcal{I}(N, X)$. Moreover, $\Phi((f + \mathcal{I}(M, X))s) = \Phi((f + \mathcal{I}(M, X))\theta(s)$ for every $s \in S$, hence a decomposition of $\mathrm{Hom}_R(M, X)/\mathcal{I}(M, X)$ into a direct sum of simple $S$-modules is mapped by $\Phi$ to a direct-sum decomposition of $\mathrm{Hom}_R(N, X)/\mathcal{I}(N, X)$ into simple $T$-modules. Therefore the lengths of these modules are the same.

In general $M^{\mathrm{codim}(T)} \simeq N^{\mathrm{codim}(S)}$ in Mod-$R/\mathcal{I}$ by Lemma 1.4 and Proposition 1.7, therefore we can restrict to the case $N = M^m$ for some $m \in \mathbb{N}$. Let $\iota_i\colon M \to N$, $\pi_i\colon N \to M$, $i = 1, \dots, m$ be the canonical embeddings and projections and let $\overline{\iota_i}, \overline{\pi_i}, i = 1, \dots, m$ be the corresponding morphisms in Mod-$R/\mathcal{I}$. Consider a homomorphism $\tau\colon S \to T$ given by $\tau(s) := \sum_{i=1}^m \overline{\iota_i} s \overline{\pi_i}$. Then any right $T$-module can be considered as an $S$-module via $\tau$. Let $S_0$ be a minimal right ideal of $S$, then it is possible to verify that $T_0 = \{\sum_{j=1}^m \overline{\iota_1} s_j \overline{\pi_j} \mid s_1, \dots, s_m \in S_0\}$ is a minimal right ideal of $T$ and $T_0 \simeq S_0^m$ as $S$-modules. Further, it is easy to verify that $\Psi(f + \mathcal{I}(N, X)) := (f\iota_1 + \mathcal{I}(M, X), \dots, f\iota_m + \mathcal{I}(M, X))$ gives an $S$-module isomorphism $\Psi\colon \mathrm{Hom}_R(N, X)/\mathcal{I}(N, X) \to \mathrm{Hom}_R(M, X)/\mathcal{I}(M, X)^m$. Therefore $m$ times the length of the $S$-module $\mathrm{Hom}_R(M, X)/\mathcal{I}(M, X)$ is the same as $m$ times the length of the $T$-module $\mathrm{Hom}_R(N, X)/\mathcal{I}(N, X)$. ■

The previous proposition allows us to define the $\mathcal{I}$-dimension for an arbitrary module. Let $\mathcal{D}$ be a class of modules, let $M \in \mathcal{D}$ be a nonzero module with semilocal endomorphism ring and let $\mathcal{I}$ be the ideal of $\mathcal{D}$ associated to a maximal ideal of $I \subseteq$

$\mathrm{End}_R(M)$. For every $X \in \mathcal{D}$, we define $\dim_{\mathcal{I}}(X)$ to be the length of the $\mathrm{End}_R(M)/I$-module $\mathrm{Hom}_R(M, X)/\mathcal{I}(M, X)$.

Let us recall [6, Remark 2.9], which provides a useful criterion to establish whether a morphism between two direct sums belongs to an ideal.

*Remark 3.2.* Let $\mathcal{I}$ be an ideal of a category $\mathcal{C} \subseteq$ Mod-$R$ such that $\mathcal{C}$ is $\mathcal{I}$-small and let $M_i, i \in I, N_j, j \in J$ be two families of modules from $\mathcal{C}$ such that $\oplus_{i\in I} M_i, \oplus_{j\in J} N_j \in \mathcal{C}$. Then $f \in \mathrm{Hom}_R(\oplus_{i\in I} M_i, \oplus_{j\in J} N_j)$ belongs to $\mathcal{I}$ if and only if $\pi_j f \iota_i \in \mathcal{I}$ for every $i \in I$, $j \in J$, where $\iota_i : M_i \to \oplus_{k\in I} M_k$ is the canonical embedding and $\pi_j : \oplus_{k\in J} N_k \to N_j$ is the canonical projection.

**Proposition 3.3.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings, and $M \in \mathcal{C}$ be nonzero. Let $I$ be a maximal ideal of* $\mathrm{End}_R(M)$ *and $\mathcal{I}$ be the ideal of* $\mathrm{Add}(\mathcal{C})$ *associated to $I$. If $M$ is $I$-small, then the functor* $\mathrm{Hom}_R(M, -)$ *induces a full and faithful functor* $G : \mathrm{Add}(\mathcal{C})/\mathcal{I} \to \text{Mod-}\mathrm{End}_R(M)/I$.

Proof. Let $F : \mathrm{Add}(\mathcal{C}) \to \mathrm{Add}(\mathcal{C})/\mathcal{I}$ be the canonical functor and let $G := \mathrm{Hom}_{\mathrm{Add}(\mathcal{C})/\mathcal{I}}(M, -)$. As remarked above $F$ and $GF$ preserve direct sums. Let $\mathcal{D}$ be the full subcategory of $\mathrm{Add}(\mathcal{C})$ whose objects are arbitrary direct sums of modules of $\mathcal{C}$. First let us check that the restriction $GF$ to $\mathcal{D}$ is a full functor on $\mathcal{D}$. Recall that by Proposition 1.7, the functor $GF$ gives an onto map $\varphi_{C_1,C_2} : \mathcal{D}(C_1, C_2) \to \mathrm{Hom}_{\mathrm{End}_R(M)/I}(GF(C_1), GF(C_2))$ for every $C_1, C_2 \in \mathcal{C}$. Consider $D_1 := \oplus_{j\in J_1} C_j$, $D_2 := \oplus_{j\in J_2} C'_j \in \mathcal{D}$ and let $\iota_{j_1} : C_{j_1} \to D_1$, $j_1 \in J_1$, $\pi_{j_2} : D_2 \to C'_{j_2}$, $j_2 \in J_2$ be the corresponding embeddings and projections. Let $f \in \mathrm{Hom}_{\mathrm{End}_R(M)/I}(GF(D_1), GF(D_2))$. For $j_1 \in J_1$, $j_2 \in J_2$ let $f_{j_2,j_1}$ be such that $f_{j_2,j_1} \in \varphi^{-1}_{C_{j_1},C'_{j_2}}(GF(\pi_{j_2}) \circ f \circ GF(\iota_{j_1}))$. Moreover, put $f_{j_2,j_1} = 0$ if $GF(\pi_{j_2}) \circ f \circ GF(\iota_{j_1}) = 0$. By Lemma 1.4, $GF(C_{j_1})$ is finitely generated, therefore for any $j_1 \in J_1$ there are only finitely many $j_2 \in J_2$ such that $f_{j_2,j_1} \neq 0$. Therefore there exists $f' : D_1 \to D_2$ such that $\pi_{j_2} f' \iota_{j_1} = f_{j_2,j_1}$. Then it is easily seen that $GF(f') = f$.

Now we can prove that $GF$ is full on $\mathrm{Add}(\mathcal{C})$. Let $A_1, A_2 \in \mathrm{Add}(\mathcal{C})$. Then there are $D_1, D_2 \in \mathcal{D}$ such that $A_i$ is a direct summand of $D_i$, $i = 1, 2$. Let $\pi_i : D_i \to A_i$, $\iota_i : A_i \to D_i$, $i = 1, 2$ be the corresponding projections and embeddings. Let $f : GF(A_1) \to GF(A_2)$. From the previous part of the proof there exists $f' : D_1 \to D_2$ such that $GF(f') = GF(\iota_2) f GF(\pi_1)$. Then $f'' := \pi_2 f' \iota_1$ satisfies $GF(f'') = f$.

We have proved that $G$ is full. It remains to prove that $G$ is faithful. Let $A_1, A_2 \in \mathrm{Add}(\mathcal{C})$ and $f : A_1 \to A_2$ be such that $GF(f) = 0$. We have to prove that $f \in \mathcal{I}$. Suppose the contrary. Then there are $\alpha : M \to A_1$ and $\beta : A_2 \to M$ such that $\beta f \alpha \notin I$, hence $\mathrm{Hom}_{\mathrm{Add}(\mathcal{C})/\mathcal{I}}(M, f)(\alpha) \neq 0$ which is not possible as $\mathrm{Hom}_{\mathrm{Add}(\mathcal{C})/\mathcal{I}}(M, f) = 0$. ■

Any module over a simple Artinian ring is determined up to isomorphism by its length. Therefore

**Corollary 3.4.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings, let $M \in \mathcal{C}$ be nonzero, and let $I$ be a maximal ideal of* $\mathrm{End}_R(M)$ *such that $M$ is $I$-small. If $\mathcal{I}$ is an ideal of* $\mathrm{Add}(\mathcal{C})$ *associated to $I$ and $X, Y \in \mathrm{Add}(\mathcal{C})$, then* $\dim_{\mathcal{I}}(X) = \dim_{\mathcal{I}}(Y)$ *if and only if $X$ and $Y$ are isomorphic in* $\mathrm{Add}(\mathcal{C})/\mathcal{I}$.

**Lemma 3.5.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings. Consider a nonzero module $M \in \mathcal{C}$, a maximal ideal $I \subseteq \mathrm{End}_R(M)$ such that $M$ is $I$-small and an ideal $\mathcal{I}$ of* $\mathrm{Add}(\mathcal{C})$ *associated to $I$. Moreover let $M_i, i \in \mathbb{N}$, be a countable family of modules in $\mathcal{C}$. If $A$, $B$ are direct summands of $\oplus_{i\in\mathbb{N}} M_i$ such that* $\dim_{\mathcal{I}}(A) = \dim_{\mathcal{I}}(B)$*, then there are $f, g \in \mathrm{End}_R(\oplus_{i\in\mathbb{N}} M_i)$ satisfying the following conditions:*

*(i) For any $i, j \in \mathcal{C}$ $\pi_j f \iota_i \neq 0$ or $\pi_j g \iota_i \neq 0$ implies $\mathcal{I} \cap \mathcal{C} \in V(M_i) \cap V(M_j)$.*
*(ii)* $1_A - \pi_A g \iota_B \pi_B f \iota_A, 1_B - \pi_B f \iota_A \pi_A g \iota_B \in \mathcal{I}$.
*(iii) If $\mathcal{I} \cap \mathcal{C} \neq \mathcal{L} \in$* $\mathrm{Spec}(\mathcal{C})$ *such that $\mathcal{C}$ is $\mathcal{L}$-small, then $\pi_j f \iota_i, \pi_j g \iota_i \in \mathcal{L}$ for every $i, j \in \mathbb{N}$.*

Proof. Let $F\colon \mathrm{Add}(\mathcal{C}) \to \mathrm{Add}(\mathcal{C})/\mathcal{I}$ be the canonical functor. By Corollary 3.4, $F(A) \simeq F(B)$. We can proceed as in [6, Lemma 3.3]: Suppose that $M = \oplus_{i\in\mathbb{N}} M_i = A \oplus A' = B \oplus B'$ and let $\iota_A\colon A \to M$, $\iota_B\colon B \to M$, $\pi_A\colon M \to A$, $\pi_B\colon M \to B$ be the canonical embeddings and projections. Let $f_0\colon F(A) \to F(B)$ and $g_0\colon F(B) \to F(A)$ be mutually inverse isomorphisms and let $f_0', g_0' \in \mathrm{End}_{\mathrm{Add}(\mathcal{C})/\mathcal{I}}(F(M))$ be such that $F(\pi_B) f_0' F(\iota_A) = f_0$, $F(\pi_A) g_0' F(\iota_B) = g_0$. Let $f', g' \in \mathrm{End}_R(M)$ be such that $F(f') = f_0'$, $F(g') = g_0'$. Because of Remark 3.2, we may choose $f', g'$ satisfying $\pi_j f' \iota_i = 0$, $\pi_j g' \iota_i = 0$ for every $i, j \in \mathbb{N}$ such that $\mathcal{I}' := \mathcal{I} \cap \mathcal{C} \notin V(M_i) \cap V(M_j)$.

Observe that for every $i \in \mathbb{N}$ there exists $h_i \in \mathrm{End}_R(M_i)$ such that $1_{M_i} - h_i \in \mathcal{I}'$ and $h_i \in \mathcal{L}$ for every $\mathcal{I}' \neq \mathcal{L} \in \mathrm{Spec}(\mathcal{C})$. Indeed, fix $i \in \mathbb{N}$. If $\mathcal{I}' \notin V(M_i)$, put $h_i = 0$. If $V(M_i) = \{\mathcal{I}', \mathcal{L}_1, \dots, \mathcal{L}_n\}$, then $\mathcal{I}(M_i, M_i), \mathcal{L}_1(M_i, M_i), \dots, \mathcal{L}_n(M_i, M_i)$ are the maximal ideals of $\mathrm{End}_R(M_i)$. Hence, the Chinese Reminder Theorem gives $h_i \in \mathrm{End}_R(M_i)$ such that $1_{M_i} - h_i \in \mathcal{I}'$ and $h_i \in \cap_{i=1}^n \mathcal{L}_i$. Of course, $h_i \in \mathcal{L}$ for every $\mathcal{L} \notin V(M_i)$.

Let $h := \oplus_{i\in\mathbb{N}} h_i \in \mathrm{End}_R(M)$, $f := hf'$, $g := hg'$. Notice $F(f) = F(f')$, $F(g) = F(g')$, therefore (ii) holds. The choice of $f', g'$ guarantees that (i) is satisfied too. Finally, if $\mathcal{L} \neq \mathcal{I}'$ is an ideal of $\mathrm{Spec}(\mathcal{C})$, then every $h_i$ is in $\mathcal{L}$ which implies (iii). ■

Let $\mathcal{C}$ be a full subcategory of Mod-$R$ and let $\mathcal{I}$ be an ideal of $\mathcal{C}$. We say that the ideal $\mathcal{J}$ of $\mathrm{Add}(\mathcal{C})$ is *associated* to $\mathcal{I}$ if $\mathcal{J}$ is the largest ideal of $\mathrm{Add}(\mathcal{C})$ such that $\mathcal{C} \cap \mathcal{J} = \mathcal{I}$. Observe that if $M \in \mathcal{C}$, $I$ is an ideal of $\mathrm{End}_R(M)$, $\mathcal{I}$ is the ideal of $\mathcal{C}$ associated to $I$, and $\mathcal{J}$ is the ideal of $\mathrm{Add}(\mathcal{C})$ associated to $\mathcal{I}$, then $\mathcal{J}$ is the ideal of $\mathrm{Add}(\mathcal{C})$ associated to $I$.

We have already recalled that a module $M$ is *small* if for every family of modules $N_\lambda$, $\lambda \in \Lambda$, and every homomorphism $f\colon M \to \oplus_{\lambda\in\Lambda} N_\lambda$ there exists a finite set $\Lambda_0 \subseteq \Lambda$ such that $f(M) \subseteq \oplus_{\lambda\in\Lambda_0} N_\lambda$. A module is said to be *$\sigma$-small* if it is a countable union of small modules (observe that every countably generated module is $\sigma$-small).

**Proposition 3.6.** *Let $\mathcal{C}$ be a class of modules with semilocal endomorphism rings, let $M_i$, $i \in \mathbb{N}$ be a countable family of objects in $\mathcal{C}$ such that for every $i \in \mathbb{N}$ the module $M_i$ is $\sigma$-small and $J(\mathrm{End}_R(M_i))$-small. If $A, B$ are direct summands of $\oplus_{i\in\mathbb{N}} M_i$ such that $\dim_{\mathcal{I}}(A) = \dim_{\mathcal{I}}(B)$ for every ideal $\mathcal{I}$ of $\mathrm{Add}(\mathcal{C})$ associated to an ideal of $\mathrm{Spec}(\mathcal{C})$, then $A \simeq B$.*

PROOF. Let $A \oplus A_1 = M = B \oplus B_1$. Using the standard Eilenberg's trick (cf. the proof of [6, Lemma 7.2]) we can suppose $A_1 \simeq B_1$. Let us denote $\iota_A : A \to M$, $\iota_B : B \to M$, $\pi_A : M \to A$, and $\pi_B : M \to B$ the canonical embeddings and projections. Let $\mathcal{S}$ be the set of ideals in $\mathrm{Add}(\mathcal{C})$ such that $\mathcal{I} \in \mathcal{S}$ if and only if $\mathcal{I}$ is associated to an ideal from $\cup_{i\in\mathbb{N}} V(M_i)$.

Step 1: There are $f, g \in \mathrm{End}_R(M)$ such that $1_A - \pi_A g \iota_B \pi_B f \iota_A$, $1_B - \pi_B f \iota_A \pi_A g \iota_B \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$: For every $\mathcal{I} \in \mathcal{S}$ take $f_{\mathcal{I}}, g_{\mathcal{I}}$ satisfying the conditions (i)–(iii) of Lemma 3.5. Observe that $f_{\mathcal{I}}, \mathcal{I} \in \mathcal{S}$ and $g_{\mathcal{I}}, \mathcal{I} \in \mathcal{S}$ are summable families of homomorphisms (in fact, condition (i) of Lemma 3.5 says that $f_{\mathcal{I}}(M_i) \neq 0$ only if $\mathcal{I}$ is associated to an ideal from $V(M_i)$ and similarly for $g_{\mathcal{I}}$). Put $f := \sum_{\mathcal{I}\in\mathcal{S}} f_{\mathcal{I}}$, $g := \sum_{\mathcal{I}\in\mathcal{S}} g_{\mathcal{I}}$. It is easy to verify $f - f_{\mathcal{I}} \in \mathcal{I}$, $g - g_{\mathcal{I}} \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$: Note that $f - f_{\mathcal{I}} = \sum_{\mathcal{I}\neq\mathcal{L}\in\mathcal{S}} f_{\mathcal{L}}$, every $f_{\mathcal{L}}$ on the right hand side is in $\mathcal{I}$. By Lemma 2.2, $\mathrm{Add}(\mathcal{C})$ is $\mathcal{I}$-small, hence also $f - f_{\mathcal{I}} \in \mathcal{I}$. Lemma 3.5(ii) gives $1_A - \pi_A g \iota_B \pi_B f \iota_A \in \mathcal{I}$ and $1_B - \pi_B f \iota_A \pi_A g \iota_B \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$.

Step 2: Assume $f : A \to B$ and $g : B \to A$ satisfy $1_A - gf$, $1_B - fg \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$. For a small module $A'$ contained in $A$ there exists $g' : B \to A$ such that $1_A - g'f$, $1_B - fg' \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$ and $g'f(a) = a$ for any $a \in A'$. Similarly, for a small module $B'$ contained in $B$ there exists $f' : A \to B$ such that $1_A - gf'$, $1_B - f'g \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$ and $f'g(b) = b$ for any $b \in B'$.

We prove the first statement only. Let $f_1 : A_1 \to B_1$, $g_1 : B_1 \to A_1$ be mutually inverse isomorphisms and let $f_0 := f \oplus f_1$, $g_0 := g \oplus g_1$. Observe that $1_M - g_0 f_0 \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$. Take $n \in \mathbb{N}$ such that $A'$ and $g_0 f_0(A')$ are both submodules of $\oplus_{i=1}^n M_i$ (such an $n$ exists since $A'$ is small). Let $\iota : \oplus_{i=1}^n M_i \to M$ be the canonical embedding and let $\pi : M \to \oplus_{i=1}^n M_i$ be the canonical projection. By Proposition 1.9, $\pi(1_M - g_0 f_0)\iota \in J(\mathrm{End}_R(\oplus_{i=1}^n M_i))$, therefore $\pi g_0 f_0 \iota$ is invertible. Let $h \in \mathrm{End}_R(\oplus_{i=1}^n M_i)$ be its inverse and define $h_0 := h \oplus 1_{\oplus_{i\geq n+1} M_i} \in \mathrm{End}_R(M)$. Observe that $1_M - h_0 \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$. Put $g' := \pi_A h_0 \iota_A g$. Since $1_M - h_0 \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$, $g - g' \in \mathcal{I}$ and hence $1_A - g'f$, $1_B - fg' \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$. Let $a \in A'$. Then $g'f(a) = \pi_A h_0 \iota_A g f(a) = \pi_A(h_0\iota)\pi g_0 f_0 \iota\pi(a) = \pi_A(\iota h)(\pi g_0 f_0 \iota)\pi(a) = \pi_A \iota\pi(a) = a$.

Step 3: Since $M_i$'s are $\sigma$-small modules there are small modules $A'_i$, $i \in \mathbb{N}$ contained in $A$ and small modules $B'_i$, $i \in \mathbb{N}$ contained in $B$ such that $A = \sum_{i\in\mathbb{N}} A'_i$ and $B = \sum_{i\in\mathbb{N}} B'_i$. Now we define inductively small modules $A_i$, $i \in \mathbb{N}$ contained in $A$, small modules $B_i$, $i \in \mathbb{N}$ contained in $B$, homomorphisms $f_i : A \to B$, $i \in \mathbb{N}$, $g_i : B \to A$ such that

(i) $g_i f_i(a) = a$ for every $a \in A_i$,
(ii) $f_{i+1} g_i(b) = b$ for every $b \in B_i$,
(iii) $f_i(A_i) \subseteq B_i$, $g_i(B_i) \subseteq A_{i+1}$,

(iv) $1_A - g_i f_i, 1_B - f_i g_i, 1_A - g_i f_{i+1}, 1_B - f_{i+1} g_i \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$ and every $i \in \mathbb{N}$, and
(v) $\sum_{i\in\mathbb{N}} A_i = A$, $\sum_{i\in\mathbb{N}} B_i = B$.

Put $A_1 := A'_1$, and let $f_1 \colon A \to B$, $g_1 \colon B \to A$ be such that $g_1 f_1(a) = a$, for every $a \in A_1$ and $1_A - g_1 f_1, 1_B - f_1 g_1 \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$. The previous steps of the proof imply the existence of these homomorphisms.

Suppose that $f_1, \ldots, f_n, g_1, \ldots, g_n, A_1, \ldots, A_n, B_1, \ldots, B_{n-1}$ have been found. Define $B_n := B'_n + f_n(A_n)$, then define $f_{n+1} \colon A \to B$ such that $1_A - g_n f_{n+1}, 1_B - f_{n+1} g_n \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$ and $f_{n+1} g_n(b) = b$ for every $b \in B_n$. Put $A_{n+1} := A'_{n+1} + g_n(B_n)$ and another application of Step 2 gives $g_{n+1} \colon B \to A$ such that $g_{n+1} f_{n+1}(a) = a$ for every $a \in A_{n+1}$ and $1_A - g_{n+1} f_{n+1}, 1_B - f_{n+1} g_{n+1} \in \mathcal{I}$ for every $\mathcal{I} \in \mathcal{S}$.

It is easily seen that $f_n|_{A_n} = f_{n+1}|_{A_n}$, $g_n|_{B_n} = g_{n+1}|_{B_n}$. Therefore we can define $f \colon A \to B$ and $g \colon B \to A$ by $f(a) = f_n(a)$ if $a \in A_n$ and $g(b) = g_n(b)$ if $b \in B_n$. Then $f$ and $g$ are mutually inverse isomorphisms. ■

**Theorem 3.7.** *Let $\mathcal{C}$ be a class of $\sigma$-small modules with semilocal endomorphism rings such that every module $M \in \mathcal{C}$ is $J(\mathrm{End}_R(M))$-small. Two modules $A, B \in$* $\mathrm{Add}(\mathcal{C})$ *are isomorphic if and only if* $\dim_{\mathcal{I}}(A) = \dim_{\mathcal{I}}(B)$ *for every ideal of* $\mathrm{Add}(\mathcal{C})$ *associated an element of $\mathcal{I} \in$* $\mathrm{Spec}(\mathcal{C})$.

Proof. We proceed as in [6, Theorem 7.4]. Apply [5, Theorem 2.47] to the class of $\sigma$-small modules to deduce that $A$ has a decomposition $A = \oplus_{x\in X} A_x$, such that, for every $x \in X$, the module $A_x$ is isomorphic to a direct summand of a countable direct sum of modules from $\mathcal{C}$. Similarly let $B = \oplus_{y\in Y} B_y$ be a decomposition of $B$ into direct summands of countable direct sums of modules from $\mathcal{C}$. The additivity of $\dim_{\mathcal{I}}$ gives $\sum_{x\in X} \dim_{\mathcal{I}}(A_x) = \sum_{y\in Y} \dim_{\mathcal{I}}(B_y)$ for every $\mathcal{I} \subseteq \mathrm{Add}(\mathcal{C})$ associated to an ideal of $\mathrm{Spec}(\mathcal{C})$, where the sums indicate the cardinalities of disjoint unions of $\dim_{\mathcal{I}}(A_x)$, $x \in X$, and $\dim_{\mathcal{I}}(B_y)$, $y \in Y$. Observe that there is a set $\mathcal{C}' \subseteq \mathcal{C}$ such that $A, B \in \mathrm{Add}(\mathcal{C}')$, let $\mathcal{S}$ be the set of ideals associated to ideals from $\cup_{M\in\mathcal{C}'} V(M)$ and notice that $\dim_{\mathcal{I}}(A) = \dim_{\mathcal{I}}(B) = 0$ if $\mathcal{I} \notin \mathcal{S}$. For any $\mathcal{I} \in \mathcal{S}$ let $E_{\mathcal{I}}$ be a fixed set of cardinality $\dim_{\mathcal{I}}(A)$ (hence $E_{\mathcal{I}}$ is empty if $\dim_{\mathcal{I}}(A) = 0$) and let $p_{\mathcal{I}} \colon E_{\mathcal{I}} \to X$, $q_{\mathcal{I}} \colon E_{\mathcal{I}} \to Y$ be such that $|p_{\mathcal{I}}^{-1}(x)| = \dim_{\mathcal{I}}(A_x)$ for every $x \in X$ and $|q_{\mathcal{I}}^{-1}(y)| = \dim_{\mathcal{I}}(B_y)$ for every $y \in Y$. Let us consider the unoriented bipartite graph $G$ on the set $X \dot\cup Y$ with multiple edges whose set of edges is $\{\{p_{\mathcal{I}}(e), q_{\mathcal{I}}(e)\} \mid e \in E_{\mathcal{I}}, \mathcal{I} \in \mathcal{S}\}$.

We claim that degree of any vertex in the graph $G$ is at most countable: Fix $x \in X$. The module $A_x$ is isomorphic to a direct summand of $\oplus_{i\in\mathbb{N}} M_i$ for some $M_i \in \mathcal{C}$. Therefore $\dim_{\mathcal{I}}(A_x) = 0$ whenever $\mathcal{I} \notin \mathcal{S}'$, where $\mathcal{S}'$ is the set of ideals of $\mathrm{Add}(\mathcal{C})$ associated to the ideals from $\cup_{i\in\mathbb{N}} V(M_i)$. Since $V(M_i)$ are finite subsets of $\mathrm{Spec}(\mathcal{C})$, $\mathcal{S}'$ is countable. Moreover $\dim_{\mathcal{I}}(A_x) \le \dim_{\mathcal{I}}(\oplus_{i\in\mathbb{N}} M_i) \le \aleph_0$. Therefore the set of edges incident to $x$ is $T = \{\{x, q(e)\} \mid e \in p_{\mathcal{I}}^{-1}(x), \mathcal{I} \in \mathcal{S}'\}$. Obviously $|T| \le \aleph_0$ which proves the claim (the number of edges incident to $y \in Y$ can be expressed similarly).

Let $\kappa$ be an ordinal of cardinality at least $|X|$. As in the proof of [6, Theorem 7.4] we construct families of sets $X_\lambda \subseteq X$, $\lambda \in \kappa$, $Y_\lambda \subseteq Y$, $\lambda \in \kappa$ such that $\{X_{\lambda+1} \setminus X_\lambda \mid \lambda <$

$\kappa\}$ is a partition of $X$, $\{Y_{\lambda+1} \setminus Y_\lambda \mid \lambda < \kappa\}$ is a partition of $Y$. Moreover, for every $\lambda < \kappa$ the sets $X_{\lambda+1} \setminus X_\lambda$ and $Y_{\lambda+1} \setminus Y_\lambda$ are at most countable and $\dim_{\mathcal{I}}(\bigoplus_{x \in X_{\lambda+1} \setminus X_\lambda} A_x) = \dim_{\mathcal{I}}(\bigoplus_{y \in Y_{\lambda+1} \setminus Y_\lambda} B_y)$ for every $\mathcal{I} \in \mathcal{S}$. The construction is literally the same, so we do not repeat it here. Then we conclude by Proposition 3.6. ■

**Acknowledgements** The author was partially supported by grant GA ČR P201/12/G028. The author is indebted to the referee for valuable comments.

## References

1. Camps, R., Dicks, W.: On semilocal rings. Israel J. Math. **81**(1–2), 203–211 (1993)
2. Facchini, A., Herbera, D.: Local morphisms and modules with a semilocal endomorphism ring. Algebr. Represent. Theor **9**(4), 403–422 (2006)
3. Facchini, A., Perone, M.: Maximal ideals in preadditive categories and semilocal categories. J. Algebra Appl. **10**(1), 1–27 (2011)
4. Facchini, A., Wiegand, R.: Direct sum decompositions of modules, semilocal endomorphism rings, and Krull monoids. J. Algebra **256**, 280–307 (2002)
5. Facchini, A.: Module Theory. Endomorphism Rings and Direct Sum Decompositions in Some Classes of Modules, Progress in Math, vol. 167. Birkhäuser Verlag, Basel (1998)
6. Facchini, A., Příhoda, P.: Factor categories and infinite direct sums. Int. Electron. J. Algebra **5**, 135–168 (2009)
7. Facchini, A., Příhoda, P.: Endomorphism rings with finitely many maximal right ideals. Comm. Algebra **39**(9), 3317–3338 (2011)
8. Harada, M., Sai, Y.: On categories of indecomposable modules I. Osaka J. Math. **7**, 323–344 (1970)
9. Mitchell, B.: Rings with several objects. Adv. Math. **8**, 1–161 (1972)
10. Příhoda, P.: Projective modules are determined by their radical factors. J. Pure Appl. Algebra **210**(3), 827–835 (2007)
11. Příhoda, P., Puninski, G.: Pure projective modules over chain domains with Krull dimension. J. Algebra **459**, 189–212 (2016)

# The Multiplicative Ideal Theory of Leavitt Path Algebras of Directed Graphs—A Survey

**Kulumani M. Rangaswamy**

**Abstract** Let $L$ be the Leavitt path algebra of an arbitrary directed graph $E$ over a field $K$. This survey article describes how this highly non-commutative ring $L$ shares a number of the characterizing properties of a Dedekind domain or a Prüfer domain expressed in terms of their ideal lattices. Special types of ideals such as the prime, the primary, the irreducible, and the radical ideals of $L$ are described in terms of the graphical properties of $E$. The existence and the uniqueness of the factorization of a non-zero ideal of $L$ as an irredundant product of prime or primary or irreducible ideals are established. Such factorization always exists for every ideal in $L$ if the graph $E$ is finite or if $L$ is two-sided Artinian or two-sided Noetherian. In all these factorizations, the graded ideals of $L$ seem to play an important role. Necessary and sufficient conditions are given under which $L$ is a generalized ZPI ring, that is, when every ideal of $L$ is a product of prime ideals. Intersections of various special types of ideals are investigated and an analogue of Krull's theorem on the intersection of powers of an ideal in $L$ is established.

**Keywords** Leavitt path algebras · Multiplicative ideal theory · Factorization of ideals

## 1 Introduction

Leavitt path algebras of directed graphs are algebraic analogues of graph C*-algebras and, ever since they were introduced in 2004, have become an active area of research [1]. Every Leavitt path algebra $L := L_K(E)$ of a directed graph $E$ over a field $K$ is equipped with three mutually compatible structures: $L$ is an associative $K$-algebra, $L$ is a $\mathbb{Z}$-graded algebra, and $L$ is an algebra with an involution $^*$. Further, $L$ possesses a large supply of idempotents, but it is highly non-commutative. Indeed, in most of the cases, the center of this $K$-algebra is trivial, being just the field $K$. In spite

K. M. Rangaswamy (✉)
Department of Mathematics, University of Colorado, Colorado Springs 80918, USA
e-mail: kmranga@gmail.com



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_16

of this, it is somewhat intriguing and certainly interesting that the ideals of such a non-commutative algebra $L$ exhibit the behavior of the ideals of a Prüfer domain and sometimes that of a Dedekind domain, thus making the multiplicative ideal theory of these algebras $L$ worth investigating. The purpose of this survey is to give a detailed account of some of these properties of $L$ and the resulting factorizations of its ideals. To start with, the ideal multiplication in $L$ is commutative: $AB = BA$ for any two ideals $A, B$ of $L$. As we shall see, the Prüfer-domain-like properties of $L$ lead to satisfactory factorizations of ideals of $L$ as products of prime, primary, or irreducible ideals. The graded ideals of $L$ seem to possess interesting properties such as coinciding with their own radical, being realizable as Leavitt path algebras of suitable graphs, possessing local units and many others. They play an important role in the factorization of non-graded ideals of $L$. As noted in ([1], Theorem 2.8.10 and in [19]), the two-sided ideal structure of $L$ can be described completely in terms of the hereditary saturated subsets and breaking vertices and cycles without exits in the graph $E$ and irreducible polynomials in $K[x, x^{-1}]$, and the association preserves the lattice structures. This fact facilitates the description of various factorization properties of the two-sided ideals in $L$.

This paper is organized as follows. After the preliminaries, Section 3 describes the various properties of the graded ideals of $L$ which are foundational to the study of non-graded ideals and in the factorization of ideals in $L$. In Section 4, $L$ is shown to be an arithmetical ring, that is, its ideal lattice is distributive and, as a consequence, the Chinese Remainder Theorem holds in $L$. In addition, $L$ is shown to be a multiplication ring. The ideal version of the number-theoretic theorem $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn$ for positive integers $m, n$ holds in $L$, namely, for any two ideals $M, N$ in $L$, $(M \cap N)(M + N) = MN$, again a characterizing property of Prüfer domains. In the next section, the prime, the primary, the irreducible, and the radical ideals of $L$ are described in terms of the graph properties of $E$. It is interesting to note that for a graded ideal $I$ of $L$ the first three of these properties coincide and that $I$ is always a radical ideal. In Section 6, we consider the existence and the uniqueness of factorizations of a non-zero ideal $I$ as a product of prime, primary, or irreducible ideals of $L$. It is shown that if $E$ is a finite graph or more generally, if $L$ is two-sided Noetherian or Artinian, then every ideal of $L$ is a product of prime ideals. This leads to a complete characterization of $L$ as a generalized ZPI ring, that is, a ring in which every ideal of $L$ is a product of prime ideals. Finally, an analogue of the Krull's theorem on powers of an ideal is proved for Leavitt path algebras. The results of this paper indicate the potential for successful utilization of the ideas and results from the ideal theory of commutative rings in the deeper study of the ideal theory of Leavitt path algebras (of course using different techniques, as $L$ is non-commutative, and using the graphical properties of $E$ and the nature of the graded ideals of $L$).

## 2 Preliminaries

For the general notation, terminology and results in Leavitt path algebras, we refer to [1, 18, 22] and for those in graded rings, we refer to [14, 17]. We refer to [8–13, 16] for results in commutative rings. Below we give an outline of some of the needed basic concepts and results.

A (directed) graph $E = (E^0, E^1, r, s)$ consists of two sets $E^0$ and $E^1$ together with maps $r, s : E^1 \to E^0$. The elements of $E^0$ are called *vertices* and the elements of $E^1$ *edges*. For each $e \in E^1$, say,

$$\bullet_{s(e)} \stackrel{e}{\longrightarrow} \bullet_{r(e)}$$

$s(e)$ is called the **source** of $e$ and $r(e)$ the **range** of $e$. If $\stackrel{u}{\bullet} \stackrel{e}{\longrightarrow} \stackrel{v}{\bullet}$ is an edge, then $\stackrel{u}{\bullet} \stackrel{e^*}{\longleftarrow} \stackrel{v}{\bullet}$ denotes the **ghost edge** $e^*$ with $s(e^*) = v$ and $r(e^*) = u$.

A vertex $v$ is called a **sink** if it emits no edges and a vertex $v$ is called a **regular vertex** if it emits a non-empty finite set of edges. An **infinite emitter** is a vertex which emits infinitely many edges.

A **path** $\mu$ of length $n$ is a sequences of edges $\mu = e_1 \dots e_n$ where $r(e_i) = s(e_{i+1})$ for all $i = 1, \cdots, n-1$. $|\mu|$ denotes the length of $\mu$. The path $\mu = e_1 \dots e_n$ in $E$ is **closed** if $r(e_n) = s(e_1)$, in which case $\mu$ is said to be *based at the vertex* $s(e_1)$. A closed path $\mu$ as above is called **simple** provided it does not pass through its base more than once, i.e., $s(e_i) \neq s(e_1)$ for all $i = 2, \dots, n$. The closed path $\mu$ is called a **cycle** if it does not pass through any of its vertices twice, that is, if $s(e_i) \neq s(e_j)$ for every $i \neq j$.

An *exit* for a path $\mu = e_1 \dots e_n$ is an edge $e$ such that $s(e) = s(e_i)$ for some $i$ and $e \neq e_i$.

If there is a path from vertex $u$ to a vertex $v$, we write $u \geq v$. A subset $D$ of vertices is said to be **downward directed** if for any $u, v \in D$, there exists a $w \in D$ such that $u \geq w$ and $v \geq w$. A subset $H$ of $E^0$ is called **hereditary** if, whenever $v \in H$ and $w \in E^0$ satisfy $v \geq w$, then $w \in H$. A hereditary set is **saturated** if, for any regular vertex $v$, $r(s^{-1}(v)) \subseteq H$ implies $v \in H$.

**Definition 1.** *Given an arbitrary graph $E$ and a field $K$, the Leavitt path algebra $L_K(E)$ is defined to be the $K$-algebra generated by a set $\{v : v \in E^0\}$ of pair-wise orthogonal idempotents, together with a set of variables $\{e, e^* : e \in E^1\}$ which satisfy the following conditions:*

*(1) $s(e)e = e = er(e)$ for all $e \in E^1$.*

*(2) $r(e)e^* = e^* = e^*s(e)$ for all $e \in E^1$.*

*(3) (The "CK-1 relations") For all $e, f \in E^1$, $e^*e = r(e)$ and $e^*f = 0$ if $e \neq f$.*

*(4) (The "CK-2 relations") For every regular vertex $v \in E^0$,*

$$v = \sum_{e \in E^1, s(e) = v} ee^*.$$

Note that $L$ need not have an identity. Indeed, $L$ will have the identity 1 exactly when the vertex set $E^0$ is finite and in that case $1 = \sum_{v \in E^0} v$. However, $L$ possesses **local units**, namely, given any finite set of elements $a_1, \ldots, a_n \in L$, there is an idempotent $u$ such that $ua_i = a_i = a_i u$ for all $i = 1, \ldots, n$. Every element $a \in L := L_K(E)$ can be written as $a = \sum_{i=1}^{n} k_i \alpha_i \beta_i^*$ where $\alpha_i, \beta_i$ are paths and $k_i \in K$. Here $r(\alpha_i) = s(\beta_i^*) = r(\beta_i)$. From this, it is easy to see that $L = \bigoplus_{u \in E^0} Lu$.

Many well-known examples of rings occur as Leavitt path algebras.

*Example 1.* The Leavitt path algebra of the straight line graph $E$ :

$$\bullet_{v_1} \xrightarrow{e_1} \bullet_{v_2} \xrightarrow{e_2} \cdots \xrightarrow{e_{n-1}} \bullet_{v_n}$$

is isomorphic to the matrix ring $M_n(K)$.

(Indeed, if $p_1 = e_1 \cdots e_{n-1}$, $p_2 = e_2 \ldots e_{n-1}$, ..., $p_{n-1} = e_{n-1}$, $p_n = v_n$, then $\{\epsilon_{ij} = p_i p_j^* : 1 \leq i, j \leq n\}$ is a set of matrix units, that is, $\epsilon_{ii}^2 = \epsilon_{ii}$ and $\epsilon_{ij}\epsilon_{jk} = \epsilon_{ik}$. Then $\epsilon_{ij} \longmapsto E_{ij}$ induces the isomorphism, where $E_{ij}$ is the $n \times n$ matrix with 1 at $(i, j)$ position and 0 everywhere else.)

*Example 2.* If $E$ is the graph with a single vertex and a single loop


then $L_K(E) \cong K[x, x^{-1}]$, the Laurent polynomial ring, induced by the map $v \mapsto 1$, $x \mapsto x$, $x^* \mapsto x^{-1}$.

The defining relations of a Leavitt path algebra $L_K(E)$ show that it is a non-commutative ring. Indeed if $e$ is an edge in $E$, say, $\overset{u}{\bullet} \xrightarrow{e} \overset{v}{\bullet}$ where $u \neq v$, then by defining relation (1), $ue = e$, but $eu = evu = e(vu) = 0$. The following proposition describes when $L_K(E)$ becomes a commutative ring.

**Proposition 1.** *Let $E$ be a connected graph. Then the Leavitt path algebra $L_K(E)$ is commutative if and only if either $E$ consists of just a single vertex $\{\bullet\}$ or $E$ is the graph with a single vertex and a single loop as in Example 2. In this case $L_K(E)$ $\cong K$ or $K[x, x^{-1}]$.*

Every Leavitt path algebra $L_K(E)$ is a $\mathbb{Z}$ **-graded algebra**, namely, $L_K(E) = \bigoplus_{n \in \mathbb{Z}} L_n$ induced by defining, for all $v \in E^0$ and $e \in E^1$, deg$(v) = 0$, deg$(e) = 1$, deg$(e^*) = -1$. Here the $L_n$, called **homogeneous components**, are abelian subgroups satisfying $L_m L_n \subseteq L_{m+n}$ for all $m, n \in \mathbb{Z}$. Further, for each $n \in \mathbb{Z}$, the subgroup $L_n$ is given by

$$L_n = \{\sum k_i \alpha_i \beta_i^* \in L : |\alpha_i| - |\beta_i| = n\}.$$

An ideal $I$ of $L_K(E)$ is said to be a **graded ideal** if $I = \bigoplus_{n \in \mathbb{Z}} (I \cap L_n)$. If $I$ is a non-graded ideal, then $\bigoplus_{n \in \mathbb{Z}} (I \cap L_n)$ is the largest graded ideal contained in $I$ and is called the **graded part** of $I$, denoted by $gr(A)$.

We will also be using the fact that the Jacobson radical (and in particular, the prime/Baer radical) of $L_K(E)$ is always zero (see [1]).

Let $\Lambda$ be an arbitrary non-empty (possibly, infinite) index set. For any ring $R$, we denote by $M_\Lambda(R)$ the ring of matrices over $R$ whose entries are indexed by $\Lambda \times \Lambda$ and whose entries, except for possibly a finite number, are all zero. It follows from the works in [4] that $M_\Lambda(R)$ is Morita equivalent to $R$.

**Throughout this paper $L$ will denote the Leavitt path algebra $L_K(E)$ of an arbitrary directed graph $E$ over a field $K$.**

## 3 Graded Ideals of a Leavitt Path Algebra

In this section, we shall describe some of the salient properties of the graded ideals of a Leavitt path algebra $L$. As we shall see in a later section, these properties impact the factorization of ideals of $L$. Every ideal of $L$, whether graded or not, is shown to possess an orthogonal set of generators. As a consequence, we get the interesting property that every finitely generated ideal of $L$ is a principal ideal. It is interesting to note that if $I$ is a graded ideal of $L$, then both $I$ and $L/I$ can be realized as Leavitt path algebras of suitable graphs.

Suppose $H$ is a hereditary saturated subset of vertices. A **breaking vertex** of $H$ is an infinite emitter $w \in E^0 \backslash H$ with the property that $0 < |s^{-1}(w) \cap r^{-1}(E^0 \backslash H)| < \infty$. The set of all breaking vertices of $H$ is denoted by $B_H$. For any $v \in B_H$, $v^H$ denotes the element $v - \sum_{s(e)=v, r(e) \notin H} ee^*$. The following theorem of Tomforde describes graded ideals of $L$ by means of their generators.

**Theorem 1.** *([22]) Suppose $H$ is a hereditary saturated set of vertices and $S$ is a subset of $B_H$. Then the ideal $I(H, S)$ generated by the set of idempotents $H \cup \{v^H : v \in S\}$ is a graded ideal of $L$, and conversely every graded ideal $I$ of $L$ is of the form $I(H, S)$ where $H = I \cap E^0$ and $S = \{u \in B_H : u^H \in I\}$.*

Given a pair $(H, S)$ where $H$ is a hereditary saturated set of vertices in the graph $E$ and $S$ is a subset of $B_H$, one could construct the **Quotient graph** $E\backslash(H, S)$ given by $(E\backslash(H, S))^0 = E^0 \backslash H \cup \{u' : u \in B_H \backslash S\}$, $(E\backslash(H, S))^1 = \{e \in E^1 : r(e) \notin H\} \cup \{e' : e \in E^1$ with $r(e) \in B_H \backslash S\}$ and $r, s$ are extended to $(E\backslash(H, S))^0$ by setting $s(e') = s(e)$ and $r(e') = r(e)'$.

The next theorem describes a generating set $Y$ for a not necessarily graded non-zero ideal of $L$. This set $Y$ is actually an orthogonal set of generators.

**Theorem 2.** *([19]) Let $E$ be an arbitrary graph and let $I$ be an arbitrary non-zero ideal of $L = L_K(E)$ with $H = I \cap E^0$ and $S = \{u \in B_H : u^H \in I\}$. Then $I$ is generated by the set*

$$Y = H \cup \{v^H : v \in S\} \cup \{f_t(c_t) : t \in T\},$$

*where $T$ is some index set (which may be empty), for each $t \in T$, $c_t$ is a cycle without exits in $E \backslash (H, S)$, no $v$ in $S$ is on any cycle $c_t$, and $f_t(x) \in K[x]$ is a polynomial with a non-zero constant term and is of the smallest degree such that $f_t(c_t) \in I$. Any two elements $x \neq y$ in $Y$ are orthogonal, that is, $xy = 0 = yx$.*

If $I$ is a finitely generated ideal, then the orthogonal set $Y$ of generators mentioned in the above theorem can be shown to be finite and, in that case, the single element $a = \sum_{y \in Y} y$ will be a generator for the ideal $I$. Consequently, we obtain the following interesting result.

**Theorem 3.** *([19]) Every finitely generated ideal in a Leavitt path algebra is a principal ideal, i.e., of the form $LaL$ for some $a \in L$.*

*Remark 1.* In [3], the above theorem has been extended by showing that every finitely generated one-sided ideal of $L$ is a principal ideal, that is, $L$ is a Bêzout ring.

An important property of graded ideals is the following.

**Theorem 4.** *([21]) Every graded ideal $I(H, S)$ of $L$ can be realized as a Leavitt path algebra $L_K(F)$ of some graph $F$ and further the corresponding quotient ring $L/I(H, S)$ is also a Leavitt path algebra, being isomorphic to the Leavitt path algebra $L_K(E \backslash (H, S))$ of the quotient graph $E \backslash (H, S)$.*

Since Leavitt path algebras possess local units, we conclude that the graded ideals $I$ of $L$ possess local units. Using this, we obtain some interesting properties of graded ideals.

**Proposition 2.** *([20]) (i) Let $A$ be a graded ideal of $L$. Then*
*(a) for any ideal $B$ of $L$, $AB = A \cap B$, $BA = B \cap A$ and, in particular, $A^2 = A$;*
*(b) $AB = BA$ for all ideals $B$;*
*(c) If $A = A_1 \cdots A_m$ is a product of ideals, then $A = \bigcap_{i=1}^{m} gr(A_i) = \prod_{i=1}^{m} gr(A_i)$.*

*Similarly, if $A = A_1 \cap \cdots \cap A_m$ is an intersection of ideals $A_i$, then $A = \bigcap_{i=1}^{m} gr(A_i) = \prod_{i=1}^{m} gr(A_i)$.*

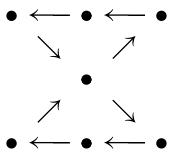
*(ii) If $A_1, \ldots, A_m$ are graded ideals of $L$, then $\prod_{i=1}^{m} A_i = \bigcap_{i=1}^{m} A_i$.*

*Proof.* We shall point out the easy proof of (i)(a). We need only to prove $A \cap B \subseteq AB$. Let $x \in A \cap B$. Since the graded ideal $A$ has local units, there is an idempotent $u \in A$ such that $ua = a = au$. Clearly then $a = ua \in AB$. So $A \cap B = AB$. Similarly, $B \cap A = BA$. Hence $AB = BA$. In particular, $A^2 = A \cap A = A$.

A natural question is when every ideal of $L$ will be a graded ideal. This can happen when $E$ satisfies the following graph property.

**Definition 2.** *A graph $E$ satisfies* ***Condition (K)*** *if whenever a vertex $v$ lies on a simple closed path $\alpha$, $v$ also lies on another simple closed path $\beta$ distinct from $\alpha$.*

Here is a simple graph satisfying Condition (K), where every vertex satisfies the required property.



**Theorem 5.** *([18, 22]) The following conditions are equivalent for $L := L_K(E)$:*
*(a) Every ideal of $L$ is graded;*
*(b) Every prime ideal of $L$ is graded;*
*(c) The graph $E$ satisfies Condition (K).*

## 4 The Lattice of Ideals of a Leavitt Path Algebra

This section describes how the ideals of a Leavitt path algebra $L$ share lattice-theoretic properties and module-theoretic properties of the ideals of a Dedekind domain or a Prüfer domain. We start with noting that, in this non-commutative ring $L$, the multiplication of ideals is commutative. Moreover, $L$ is left/right hereditary, that is, every left/right or two-sided ideal of $L$ is projective as a left or a right ideal. The ideal lattice of $L$ is distributive and multiplicative. It is also shown how many of the characterizing properties of a Prüfer domain stated in terms of its ideals hold in $L$.

Using a deep theorem of George Bergman, Ara and Goodearl proved the following result that every Leavitt path algebra is a left/right hereditary ring, a property shared by Dedekind domains.

**Theorem 6.** *(Theorem 3.7, [5]) Every ideal (including any one-sided ideal) of a Leavitt path algebra $L$ is projective as a left/right $L$-module.*

In Section 3, we noted that if $A$ is a graded ideal of $L$, then $AB = BA$ for any ideal $B$ of $L$. What happens if $A$ is not a graded ideal? With an analysis of the "non-graded parts" of $A$ and $B$, it was shown in [1, 20] that even though $L$ is, in general, non-commutative, the multiplication of its ideals is commutative as noted next.

**Theorem 7.** *([1, 20]) For any two arbitrary ideals $A, B$ of a Leavitt path algebra $L$, $AB = BA$.*

The next result shows that every Leavitt path algebra $L$ is an arithmetical ring, that is, the ideal lattice of $L$ is distributive, a property that characterizes Prüfer domains.

**Theorem 8.** *([20]) For any three ideals $A, B, C$ of the Leavitt path algebra $L$, we have*

$$A \cap (B + C) = (A \cap B) + (A \cap C).$$

*Remark 2.* A well-known result in commutative rings (see, e.g., Theorem 18, Chapter V, [23]) states that if the ideal lattice of a commutative ring $R$ is distributive (such as when $R$ is a Dedekind domain), then the Chinese Remainder Theorem holds in $R$: This means that the simultaneous congruences $x \equiv x_i \pmod{A_i}$ $(i = 1, \cdots, n)$ where the $A_i$ are ideals and the elements $x_i \in R$, admits a solution for $x$ in $R$ provided the compatibility condition $x_i + x_j \equiv 0 \pmod{A_i + A_j}$ holds for all $i \neq j$. The proof of this theorem does not require $R$ to be commutative and nor does it require the existence of a multiplicative identity in $R$. So, as a consequence of Theorem 8, one can show that the Chinese Remainder Theorem holds in Leavitt path algebras. (Thus Leavitt path algebras satisfy another property of Dedekind domains.)

We next use Theorem 8 to show that every Leavitt path algebra is a multiplication ring, a useful property in the multiplicative ideal theory of Leavitt path algebras.

**Theorem 9.** *([20]) The Leavitt path algebra $L = L_K(E)$ of an arbitrary graph $E$ is a multiplication ring, that is, for any two ideals $A, B$ of $L$ with $A \subseteq B$, there is an ideal $C$ of $L$, such that $A = BC = CB$. Moreover, if $A$ is a prime ideal, then $AB = A = BA$.*

A well-known property of a Dedekind domain $R$ is that if there are only finitely many prime ideals in $R$, then $R$ is a principal ideal domain (see Theorem 16, Chapter V in [23]). Interestingly, as the next theorem shows, a Leavitt path algebra possesses this property.

**Theorem 10.** *([6]) Let $L := L_K(E)$ be the Leavitt path algebra of an arbitrary graph $E$. If $L$ has only a finite number of prime ideals, then every ideal of $L$ is a principal ideal, i.e., of the form $LaL$ for some $a \in L$.*

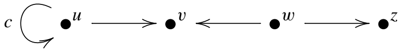
Recently, it was shown (see [7]) that the ideals of a Leavitt path algebra satisfy two more characterizing properties of Prüfer domains.

**Theorem 11.** *([7]) Let $A, B, C$ be any three ideals of a Leavitt path algebra $L$. Then*
*(i) $A(B \cap C) = AB \cap AC$;*
*(ii) $(A \cap B)(A + B) = AB$.*

Note that the statement (ii) in the preceding theorem is the ideal version of a well-known theorem in elementary number theory that, for any two positive integers $a, b$, $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$.

However not all characterizing properties of a Prüfer domain hold in a Leavitt path algebra. For instance, a domain $R$ is a Prüfer domain if and only if finitely generated ideals of $R$ are cancellative, that is, if $A$ is a non-zero finitely generated ideal, then for any two ideals $B, C$ of $R$, $AB = AC$ implies $B = C$. This property may not hold in a Leavitt path algebra as the next example shows.

*Example 3.* Consider the graph $E$




Here $H = \{v\}$ is a hereditary saturated subset. Let $A = \langle H \rangle$, the ideal generated by $H$. Clearly the cycle $c$ has no exits in $E \backslash H$. Let $B$ be the non-graded ideal $A + \langle p(c) \rangle$, where $p(x) = 1 + x \in K[x]$. Clearly $gr(B) = A$. Since $A$ is a graded ideal, we apply Proposition 2 (a), to conclude that $AB = A \cap B = A = A^2 = AA$. But $A \neq B$.

## 5 Prime, Radical, Primary, and Irreducible Ideals of a Leavitt Path Algebra

In this section, we describe special types of ideals in $L$ such as the prime, the irreducible, the primary, and the radical (= semiprime) ideals using graphical properties. While these concepts are independent for ideals in a commutative ring, we show that the first three properties of ideals coincide for graded ideals in the Leavitt path algebra $L$. We also show that a non-graded ideal $I$ of $L$ is irreducible if and only if $I$ is a primary ideal if and only if $I = P^n$, a power of a prime ideal $P$. This is useful in the factorization of ideals in the next section. We also characterize the radical ideals of $L$. It may be some interest to note that every graded ideal of $L$ is a radical ideal.

The following description of prime ideals of $L$ was given in [18].

**Theorem 12.** *(Theorem 3.2, [18]) An ideal $P$ of $L := L_K(E)$ with $P \cap E^0 = H$ is a prime ideal if and only if $P$ satisfies one of the following properties:*

*(i) $P = I(H, B_H)$ and $E^0 \backslash H$ is downward directed;*

*(ii) $P = I(H, B_H \backslash \{u\})$, $v \geq u$ for all $v \in E^0 \backslash H$ and the vertex $u'$ that corresponds to $u$ in $E \backslash (H, B_H \backslash \{u\})$ is a sink;*

*(iii) $P$ is a non-graded ideal of the form $P = I(H, B_H) + \langle p(c) \rangle$, where $c$ is a cycle without exits based at a vertex $u$ in $E \backslash (H, B_H)$, $v \geq u$ for all $v \in E^0 \backslash H$ and $p(x)$ is an irreducible polynomial in $K[x, x^{-1}]$ such that $p(c) \in P$.*

Recall, an ideal $I$ of a ring $R$ is called an **irreducible ideal** if, for ideals $A, B$ of $R$, $I = A \cap B$ implies that either $I = A$ or $I = B$. Given an ideal $I$, the **radical of the ideal** $I$, denoted by $Rad(I)$ or $\sqrt{I}$, is the intersection of all prime ideals containing $I$. A useful property is that if $a \in Rad(I)$, then $a^n \in I$ for some integer $n \geq 0$. (The proof of this property is given in Theorem 10.7 of [15] for non-commutative rings with identity, but the proof also works for rings without identity but with local units.)

If $Rad(I) = I$ for an ideal $I$, then $I$ is called a **radical ideal** or a **semiprime ideal**. An ideal $I$ of $R$ is said to be a **primary ideal** if, for any two ideals $A, B$, if $AB \subseteq I$ and $A \nsubseteq I$, then $B \subseteq Rad(I)$.

*Remark 3.* We note in passing that for any graded ideal $I$ of $L$, say $I = I(H, S)$, $Rad(I) = I$. Because, $Rad(I)/I$ is a nil ideal in $L/I$ and $L/I$, being isomorphic to the Leavitt path algebra $L_K(E\backslash(H, S))$, has no non-zero nil ideals.

We now point out an interesting property of graded ideals of $L$.

**Theorem 13.** *([20]) Suppose $I$ is a graded ideal of $L$. Then the following are equivalent:*
*(i) $I$ is a primary ideal;*
*(ii) $I$ is a prime ideal;*
*(iii) $I$ is an irreducible ideal.*

The next theorem extends the above result to arbitrary ideals of $L$.

**Theorem 14.** *([20]) Suppose $I$ is a non-graded ideal of $L$. Then the following are equivalent:*
*(i) $I$ is a primary ideal;*
*(ii) $I = P^n$, a power of a prime ideal $P$ for some $n \geq 1$;*
*(iii) $I$ is an irreducible ideal.*

The final result of this section describes the radical (also known as semiprime) ideals of $L$.

**Theorem 15.** *([2]) Let $A$ be an arbitrary ideal of $L$ with $A \cap E^0 = H$ and $S = \{v \in B_H : v^H \in A\}$. Then the following properties are equivalent:*
*(i) $A$ is a radical ideal of $L$;*
*(ii) $A = I(H, S) + \sum_{i \in Y} \langle f_i(c_i) \rangle$, where $Y$ is an index set which may be empty, for each $i \in Y$, $c_i$ is a cycle without exits based at a vertex $v_i$ in $E\backslash(H, S)$ and $f_i(x)$ is a polynomial with its constant term non-zero which is a product of distinct irreducible polynomials in $K[x, x^{-1}]$.*

## 6 Factorization of Ideals in *L*

As noted in the introduction, ideals in an arithmetical ring admit interesting representations as products of special types of ideals ([10–12]). In this section, we explore the existence and the uniqueness of factorizations of an arbitrary ideal in a Leavitt path algebra $L$ as a product of prime ideals and as a product of irreducible/primary ideals. The prime factorization of graded ideals of $L$ seems to influence that of the non-graded ideals in $L$. Indeed, an ideal $I$ is a product of prime ideals in $L$ if and only its graded part $gr(I)$ has the same property and, moreover, $I/gr(I)$ is finitely generated with a generating set of cardinality no more than the number of distinct prime ideals in an irredundant factorization of $gr(I)$. It is interesting to note that if $I$ is a graded ideal and if $I = P_1 \cdots P_n$ is an irredundant product of prime ideals, then necessarily each of the ideals $P_j$ must be graded. We also show that $I$ is an intersection of irreducible ideals if and only if $I$ is an intersection of prime ideals. If $L$ is the Leavitt path algebra of a finite graph or, more generally, if $L$ is two-sided Noetherian or two-sided Artinian, then every ideal of $L$ is shown to be a product of prime ideals. We also give necessary and sufficient conditions under which every non-zero ideal of $L$ is a product of prime ideals, that is, when $L$ is a generalized ZPI ring. We end this section by proving for $L$ an analogue of the Krull's theorem on the intersection of powers of an ideal.

We begin with the following useful proposition.

**Proposition 3.** *([20]) Suppose $I$ is a non-graded ideal of $L$. If $gr(I)$ is a prime ideal, then $I$ is a product of prime ideals.*

Using this, we obtain the following main factorization theorem.

**Theorem 16.** *([20]) Let $E$ be an arbitrary graph. For a non-graded ideal $I$ of $L := L_K(E)$, the following are equivalent:*

*(i) $I$ is a product of prime ideals;*

*(ii) $I$ is a product of primary ideals;*

*(iii) $I$ is a product of irreducible ideals;*

*(iv) $gr(I)$ is a product of (graded) prime ideals;*

*(v) $gr(I) = P_1 \cap \cdots \cap P_m$ is an irredundant intersection of $m$ graded prime ideals $P_j$ and $I/gr(I)$ is generated by at most $m$ elements and is of the form $I/gr(I) = \bigoplus_{r=1}^{k} \langle f_r(c_r) \rangle$ where $k \leq m$ and, for each $r = 1 \cdots k$, $c_r$ is a cycle without exits in $E^0 \backslash I$ and $f_r(x) \in K[x]$ is a polynomial with non-zero constant term of smallest degree such that $f_r(c_r) \in I$.*

As a consequence of Theorem 16, we obtain a number of corollaries.

**Corollary 1.** *([20]) Let $E$ be a finite graph, or more generally, let $E^0$ be finite. Then every non-zero ideal of $L = L_K(E)$ is a product of prime ideals.*

Using a minimal or maximal argument, the above corollary can be extended to the case when the ideals of $L$ satisfy the DCC or ACC as noted below.

**Corollary 2.** *([20]) Suppose $L$ is two-sided Artinian or two-sided Noetherian. Then every non-zero ideal of $L$ is a product of prime ideals.*

We now give the necessary and sufficient conditions under which $L$ is a generalized ZPI ring, that is, when every ideal of $L$ is a product of prime ideals.

**Theorem 17.** *([20]) Let $E$ be an arbitrary graph and let $L := L_K(E)$. Then every proper ideal of $L$ is a product of prime ideals if and only if every homomorphic image of $L$ is either a prime ring or contains only finitely many minimal prime ideals.*

The next theorem states that an irredundant factorization of an ideal $A$ as a product of prime ideals in $L$ is unique up to a permutation of the factors. It also points out the interesting fact that if $A$ is a graded ideal, then every factor in this irredundant factorization must also be a graded ideal.

Recall that $A = P_1 \cdots P_n$ is an **irredundant product** of the ideals $P_i$, if $A$ is not the product of a proper subset of the set $\{P_1, \ldots, P_n\}$.

**Theorem 18.** *([6]) (a) Suppose $A$ is an arbitrary ideal of $L$ and $A = P_1 \cdots P_m = Q_1 \cdots Q_n$ are two representations of $A$ as irredundant products of prime ideals $P_i$ and $Q_j$. Then $m = n$ and $\{P_1, \ldots, P_m\} = \{Q_1, \ldots, Q_n\}$;*

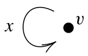
*(b) If $A$ is a graded ideal of $L$ and if $A = P_1 \cdots P_m$ is an irredundant product of prime ideals $P_j$, then the ideals are all graded and $A = P_1 \cap \cdots \cap P_m$.*

From Proposition 2(c) and the equivalence of conditions (i) and (iv) of Theorem 16, we derive following proposition.

**Proposition 4.** *If an ideal $I$ of $L$ is an intersection of finitely many prime ideals, then $I$ is a product of (finitely many) prime ideals.*

But a product of prime ideals in $L$ need not be an intersection of prime ideals as the next example shows.

*Example 4.* If $E$ is the graph with a single vertex and a single loop




then $L_K(E) \cong K[x, x^{-1}]$, the Laurent polynomial ring, induced by the map $v \mapsto 1$, $x \mapsto x$, $x^* \mapsto x^{-1}$. So it is enough to find a ideal $A$ in $K[x, x^{-1}]$ with the desired property. Consider the prime ideal $A = \langle p(x) \rangle$ in $K[x, x^{-1}]$, where $p(x)$ is an irreducible polynomial. We claim that $B = A^2$ is not an intersection of prime ideals in $K[x, x^{-1}]$. Suppose, on the contrary, $B = \bigcap_{\lambda \in \Lambda} M_\lambda$ where $\Lambda$ is some (finite or infinite) index set and each $M_\lambda$ is a (non-zero) prime ideal of $K[x, x^{-1}]$ and hence a maximal ideal of the principal ideal domain $K[x, x^{-1}]$. Now there is a homomorphism $\phi : R \longrightarrow \prod_{\lambda \in \Lambda} R/M_\lambda$ given by $r \mapsto (\ldots, r + M_\lambda, \ldots)$ with $\ker(\phi) = B$. Then $\bar{A} = \phi(A) \cong A/B \neq 0$ satisfies $(\bar{A})^2 = 0$ and this is impossible since $\prod_{\lambda \in \Lambda} R/M_\lambda$, being a direct product of fields, does not contain any non-zero nilpotent ideals.

The next proposition is new and gives necessary and sufficient conditions under which a product of prime ideals in a Leavitt path algebra is also an intersection of prime ideals. This happens exactly when every ideal of $L$ is a radical ideal.

**Proposition 5.** *Let $E$ be an arbitrary graph and let $L := L_K(E)$. Then the following properties are equivalent:*

*(i) Every product of prime ideals in $L$ is an intersection of prime ideals;*
*(ii) The graph $E$ satisfies Condition (K);*
*(iii) Every ideal of $L$ is a radical ideal;*
*(iv) Every ideal of $L$ is a graded ideal.*

*Proof.* Assume (i). Assume, by way of contradiction, that the graph $E$ does not satisfy Condition (K). Then, for some admissible pair $(H, S)$, the quotient graph $E\backslash(H, S)$ does not satisfy Condition (L) (see [1]) and thus there is a cycle $c$ without exits in $E\backslash(H, S)$. By [1, Lemma 2.7.1], the ideal $M$ of $L_K(E\backslash(H, S))$ generated by $\{c^0\}$ is isomorphic to the matrix ring $M_\Lambda(K[x, x^{-1}])$ where $\Lambda$ is some index set. Then [7, Proposition 1] and Example 4 imply that, for any prime ideal $P$ of $M$, $P^2$ is not an intersection of prime ideals of $M$. Since the graded ideal $M$ is a ring with local units ([1, Corollary 2.5.23]), every ideal (prime ideal) of $M$ is an ideal (prime ideal) of $L_K(E\backslash(H, S))$ and, for any prime ideal $Q$ of $L_K(E\backslash(H, S))$, $M \cap Q$ is a prime ideal of $M$. Consequently, $P^2$ cannot be an intersection of prime ideals of $L_K(E\backslash(H, S))$. This is a contradiction, since $L_K(E\backslash(H, S))$, being isomorphic to the quotient ring $L/I(H, S)$, satisfies (i). Consequently, the graph $E$ must satisfy Condition (K), thus proving (ii).

Assume (ii). By [1, Proposition 2.9.9], every ideal of $L$ is graded. On the other hand if $I = I(H, S)$ is a graded ideal, then $L/I$ is isomorphic to the Leavitt path algebra $L_K(E\backslash(H, S)$ and since the prime radical (the intersection of all prime ideals of $L_K(E\backslash(H, S))$ is zero, $I$ is the intersection of all the prime ideals containing $I$ and hence is a radical ideal. This proves (iii).

Assume (iii). We claim that every ideal of $L$ must be a graded ideal. Suppose, by way of contradiction, there is a non-graded ideal $I$ in $L$, say, $I = I(H, S) + \sum_{i \in Y} \langle f_i(c_i)\rangle$, where $Y$ is an index set and, for each $i \in Y$, $f_i(x) \in K[x]$ and $c_i$ is a cycle without exits in $E\backslash(H, S)$. Now for a fixed $i \in Y$ and an irreducible polynomial $p(x) \in K[x, x^{-1}]$, $P = I(H, S) + \langle p(c_i)\rangle$ is a prime ideal and $\bar{P} = P/I(H, S) = \langle p(c_i)\rangle \subsetneqq M = \langle\{c_i^0\}\rangle$. As noted in the proof of (i) $\Longrightarrow$ (ii), $\bar{P}^2$ is not a radical ideal of $L/I(H, S)$ and hence $P^2$ is not a radical ideal in $L$, a contradiction. Hence every ideal of $L$ is a graded ideal. This proves (iv).

Now (iv) $\Longrightarrow$ (i), by Proposition 2(c).

We end this section by considering the powers of an ideal in $L$. From Proposition 2, it is clear that if $A$ is a graded ideal of $L$, then $A = A^2$ and so $A = A^n$ for all $n \geq 1$. What happens if $A$ is a non-graded ideal? The next proposition implies that, for such an $A$, $A \neq A^n$ for any $n > 1$.

**Proposition 6.** *([6]) If $A$ is a non-graded ideal in $L$, then $\bigcap_{n=1}^{\infty} A^n$ is a graded ideal, being equal to $gr(A)$.*

As a corollary, we obtain

**Corollary 3.** *An ideal $A$ of $L$ is a graded ideal if and only if $A = A^n$ for all $n \geq 1$.*

W. Krull showed that if $A$ is an ideal of a commutative Noetherian ring with identity 1, then $\bigcap_{n=1}^{\infty} A^n = 0$ if and only if $1 - x$ is not a zero divisor for all $x \in A$ (see Theorem 12, Section 7 in [23]). As a consequence of Proposition 6, we obtain an analogue of Krull's theorem for Leavitt path algebras.

**Corollary 4.** *([6]) Let $A$ be an arbitrary ideal of $L$. Then $\bigcap_{n=1}^{\infty} A^n = 0$ if and only if $A$ contains no vertices of the graph $E$.*

**Acknowledgements** My thanks to Gene Abrams for carefully reading this article, making corrections, and offering suggestions.

## References


1. Abrams, G., Ara, P., Siles Molina, M.: Leavitt path algebras. Lecture Notes in Mathematics, vol. 2191. Springer (2017). ISBN 978-1-4471-7344-1
2. Abrams, G., Greenfeld, B., Mesyan, Z., Rangaswamy, K.M.: Chains of semiprime and prime ideals in Leavitt path algebras. Contemp. Math. **715**, 1–16 (2018). https://doi.org/10.1090/conm/715/14400
3. Abrams, G., Mantese F., Tonolo, A.: Leavitt path algebras are Bézout. Israel J. Math. (To appear)
4. Ánh, P.N., Márki, L.: Morita equivalence of rings without identity. Tsukuba J. Math. **11**, 1–16 (1987). https://doi.org/10.21099/tkbjm/1496160500
5. Ara, P., Goodearl, K.: Leavitt path algebras of separated graphs. J. Reine Angew. Math. **669**, 165–224 (2012). https://doi.org/10.1515/CRELLE.2011.146
6. Esin, S., Kanuni, M., Rangaswamy, K.M.: On intersections of two-sided ideals of Leavitt path algebras. J. Pure Appl. Algebra **221**, 632–644 (2017). https://doi.org/10.1016/j.jpaa.2016.07.009
7. Esin, S., Kanuni, M., Koç, A., Radler, K., Rangaswamy, K.M.: On Prüfer-like Properties of Leavitt Path Algebras (To appear)
8. Fontana, M., Houston, E., Lucas, T.: Factoring Ideals in Integral Domains. Springer (2013)
9. Fuchs, L., Mosteig, F.: Ideal theory in Prüfer domains—an unconventional approach. J. Algebra **252**, 411–430 (2002). https://doi.org/10.1016/S0021-8693(02)00040-6
10. Fuchs, L., Heinzer, W., Olberding, B.: Maximal prime divisors in arithmetical rings, Rings, modules, algebras and abelian groups. Lecture Notes in Pure and Applied Mathematics, vol. 236. Dekker, New York (2004)
11. Fuchs, L., Heinzer, W., Olberding, B.: Commutative ideal theory without finiteness conditions—primal ideals. Trans. Am. Math. Soc. **357**, 2771–2798 (2005). https://doi.org/10.1090/S0002-9947-04-03583-4
12. Fuchs, L., Heinzer, W., Olberding, B.: Commutative ideal theory without finiteness conditions—completely irreducible ideals. Trans. Am. Math. Soc. **358**, 3113–3131 (2006). https://doi.org/10.1090/S0002-9947-06-03815-3
13. Halter-Koch, F.: Ideal Systems, an Introduction to Multiplicative Ideal Theory. Marcel Dekker (1998)
14. Hazrat, R.: Graded rings and Graded Grothendieck Groups. LMS Lecture Notes Series, vol. 435. Cambridge University Press, Cambridge (2016)

15. Lam, T.Y.: Lectures on Modules and Rings, Grad. Texts in Mathematics, vol. 189. Springer (1999)
16. Larsen, M.D., McCarthy, P.J.: Multiplicative Theory of Ideals. Academic Press, New York, London (1971)
17. Nastasescu, C., van Oystaeyen, F.: Graded Ring Theory. North-Holland, Amsterdam (1982)
18. Rangaswamy, K.M.: Theory of prime ideals of Leavitt path algebras over arbitrary graphs. J. Algebra **375**, 73–90 (2013). https://doi.org/10.1016/j.jalgebra.2012.11.004
19. Rangaswamy, K.M.: On generators of two-sided ideals of Leavitt path algebras over arbitrary graphs. Communications in Algebra **42**, 2859–2868 (2014). https://doi.org/10.1080/00927872.2013.765008
20. Rangaswamy, K.M.: The multiplicative ideal theory of Leavitt path algebras. J. Algebra **487**, 173–199 (2017). https://doi.org/10.1016/j.jalgebra.2017.05.031
21. Ruiz, E., Tomforde, M.: Ideals in graph algebras. Algebras Repres. Theory **17**, 849–861 (2014). https://doi.org/10.1007/s10468-013-9421-3
22. Tomforde, M.: Uniqueness theorem and ideal structure of Leavitt path algebras. J. Algebra **318**, 270–299 (2007). https://doi.org/10.1016/j.jalgebra.2007.01.031
23. Zariski, O., Samuel, P.: Commutative Algebra, vol. 1. Van Nostrand Company (1969)

# When Two Principal Star Operations Are the Same

**Dario Spirito**

**Abstract** We study when two fractional ideals of the same integral domain generate the same star operation.

**Keywords** Star operations · Principal star operations · $m$-canonical ideals

**2010 Mathematics Subject Classification** 13G05 · 13A15

## 1 Introduction

Throughout the paper, $R$ will denote an integral domain with quotient field $K$ and $\mathcal{F}(R)$ will be the set of *fractional ideals* of $R$, that is, the set of $R$-submodules $I$ of $K$ such that $xI \subseteq R$ for some $x \in K \setminus \{0\}$.

A *star operation* on $R$ is a map $\star : \mathcal{F}(R) \longrightarrow \mathcal{F}(R)$ such that, for every $I, J \in \mathcal{F}(R)$ and every $x \in K$:

- $I \subseteq I^\star$;
- if $I \subseteq J$, then $I^\star \subseteq J^\star$;
- $(I^\star)^\star = I^\star$;
- $(xI)^\star = x \cdot I^\star$;
- $R^\star = R$.

The usual examples of star operations are the identity (usually denoted by $d$), the $v$-*operation* (or *divisorial closure*) $J \mapsto J^v := (R : (R : J))$, the $t$- and the $w$-operation (which are defined from $v$) and the star operations $I \mapsto \bigcap_{T \in \Delta} IT$, where $\Delta$ is a set of overrings of $R$ intersecting to $R$. While these examples are the easiest to work with, they usually cover only a rather small part of the set of star operations.

D. Spirito (✉)
Dipartimento di Matematica e Fisica, Università degli Studi "Roma Tre", Roma, Italy
e-mail: spirito@mat.uniroma3.it



A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_17

A much more general construction is given in [9, Proposition 3.2]: if $(I : I) = R$, then the map $J \mapsto (I : (I : J))$ is a star operation. This construction is much more flexible than the more "classical" ones, and allows to construct a much higher number of star operations (see, e.g., [10, Proposition 2.1(1)] or [11, Theorem 2.1] for its use to construct an infinite family of star operations, or [14, 15] for constructions in the case of numerical semigroups). In this paper, we slightly generalize this construction (removing the condition $(I : I) = R$), associating to each ideal $I$ a star operation $v(I)$ (which we call the star operation *generated* by $I$); we study under which conditions two ideals $I$ and $J$ generate the same star operation and, in particular, we are interested in understanding when this happens only for isomorphic ideals.

The structure of the paper is as follows: in Section 3 we give some general properties of principal star operations; in Section 4, we generalize some results of [9] from $m$-canonical ideals to general ideals; in Section 5 we study the effect of localizations on principal star operations; in Section 6 we study operations generated by ideals whose $v$-closure is $R$ (and, in particular, what happens when $R$ is a unique factorization domain); in Section 7 we study the Noetherian case, reaching a necessary and sufficient condition for $v(I) = v(J)$ under the assumption $(I : I) = (J : J) = R$.

## 2 Background

By an *ideal* of $R$ we shall always mean a fractional ideal of $R$, reserving the term *integral ideal* for those contained in $R$.

Let $\star$ be a star operation on $R$. An ideal $I$ of $R$ is $\star$-*closed* if $I = I^\star$; the set of $\star$-closed ideals is denoted by $\mathcal{F}^\star(R)$. When $\star = v$ is the divisorial closure, the elements of $\mathcal{F}^v(R)$ are called *divisorial ideals*.

Let $\mathrm{Star}(R)$ be the set of star operations on $R$. Then, $\mathrm{Star}(R)$ has a natural order structure, where $\star_1 \leq \star_2$ if and only if $I^{\star_1} \subseteq I^{\star_2}$ for every $I \in \mathcal{F}(R)$, or equivalently if $\mathcal{F}^{\star_1}(R) \supseteq \mathcal{F}^{\star_2}(R)$. Under this order, $\mathrm{Star}(R)$ is a complete lattice whose minimum is the identity and whose maximum is the $v$-operation.

A star operation is said to be *of finite type* if it is determined by its action on finitely generated ideals, or equivalently if

$$I^\star = \bigcup \{J^\star \mid J \subseteq I \text{ is finitely generated}\}$$

for every $I \in \mathcal{F}(R)$. A star operation is *spectral* if there is a subset $\Delta \subseteq \mathrm{Spec}(D)$ such that

$$I^\star = \bigcap \{IR_P \mid P \in \Delta\}$$

for every $I \in \mathcal{F}(R)$.

If $\star$ is a star operation of $R$, a prime ideal $P$ is a $\star$-*prime* if it is $\star$-closed; the set of the $\star$-primes, denoted by $\mathrm{Spec}^\star(R)$, is called the $\star$-*spectrum*. A $\star$-*maximal ideal* of $R$ is an ideal maximal among the set of proper ideals of $R$ that are $\star$-closed;

their set is denoted by $\mathrm{Max}^\star(R)$. Any $\star$-maximal ideal is prime; however, $\star$-maximal ideals need not exist. If $\star$ is a star operation of finite type, then every $\star$-closed proper integral ideal is contained in some $\star$-maximal ideal; furthermore, for every $\star$-closed ideal $I$ we have $I = \bigcap\{IR_P \mid P \in \mathrm{Spec}^\star(R)\}$.

## 3 Principal Star Operations

**Definition 3.1.** Let $R$ be an integral domain. For every $I \in \mathcal{F}(R)$, the *star operation generated by* $I$, denoted by $v(I)$, is the supremum of all the star operations $\star$ on $R$ such that $I$ is $\star$-closed. If $\star = v(I)$ for some ideal $I$, we say that $\star$ is a *principal* star operation. We denote by $\mathrm{Princ}(R)$ the set of principal star operations of $R$.

We can give a more explicit representation of $v(I)$.

**Proposition 3.2.** *For every fractional ideal $J$, we have*

$$J^{v(I)} = J^v \cap (I : (I : J)) = J^v \cap \bigcap_{\alpha \in (I:J)\setminus\{0\}} \alpha^{-1} I. \tag{1}$$

*Furthermore, if $(I : I) = R$ then $J^{v(I)} = (I : (I : J))$.*

*Proof.* The fact that the two maps $J \mapsto J^v \cap (I : (I : J))$ and $J \mapsto J^v \cap \bigcap_{\alpha \in (I:J)\setminus\{0\}} \alpha^{-1} I$ give star operations and coincide follows in the same way as [9, Lemma 3.1 and Proposition 3.2]. The second representation clearly implies that they close $I$; furthermore, if $I$ is closed then $J^v$ and each $\alpha^{-1}I$ are closed, and thus the two representations of (1) give exactly $v(I)$.

The "furthermore" statement follows again from [9, Lemma 3.1 and Proposition 3.2]. □

In the paper [9] that introduced the map $J \mapsto (I : (I : J))$ when $(I : I) = R$, an ideal $I$ was said to be *m-canonical* if $J = (I : (I : J))$ for every ideal $J$. This is equivalent to saying that $(I : I) = R$ and that $v(I)$ is the identity.

The definition of $v(I)$ can be extended to semistar operations, as in [13, Example 1.8(2)]; such construction was called the *divisorial closure with respect to* $I$ in [4]. The terminology "generated" is justified by the following Proposition 3.3.

**Proposition 3.3.** *Let $\star$ be a star operation on $R$. Then,* $\star = \inf\{v(I) \mid I \in \mathcal{F}^\star(R)\}$.

*Proof.* Let $\sharp := \inf\{v(I) \mid I \in \mathcal{F}^\star(R)\}$. By definition, $\star \leq v(I)$ for every $I \in \mathcal{F}^\star(R)$, and thus $\star \leq \sharp$. Conversely, let $J$ be a $\star$-ideal; then, $\sharp \leq v(J)$ and thus $J$ is $\sharp$-closed. It follows that $\star \geq \sharp$, and thus $\star = \sharp$. □

Our main interest in this paper is to understand when two ideals generate the same star operation. The first cases are quite easy.

**Lemma 3.4.** *Let $I$ be a fractional ideal of $R$. Then, the following hold.*

*(a)* $v(I) = v$ *if and only if* $I$ *is divisorial.*
*(b)* *If* $(I : I) = R$*, then* $v(I) = d$ *if and only if* $I$ *is* $m$*-canonical.*
*(c)* *For every* $a \in K$*,* $a \neq 0$*, we have* $v(I) = v(aI)$*.*
*(d)* *If* $L$ *is an invertible ideal of* $R$*, then* $v(I) = v(IL)$*.*

*Proof.* The only non-trivial part is the last point. If $L$ is invertible, then

$$I^{v(IL)}L \subseteq (I^{v(IL)}L)^{v(IL)} = (IL)^{v(IL)} = IL$$

and thus $I^{v(IL)} \subseteq IL(R : L) = I$, i.e., $I$ is $v(IL)$-closed; it follows that $v(I) \geq v(IL)$. Symmetrically, we have $v(IL) \geq v(IL(R : L)) = v(I)$, and thus $v(I) = v(IL)$. □

We note that if $J = IL$ for some invertible ideal $L$, then $I$ and $J$ are locally isomorphic. However, the latter condition is neither necessary nor sufficient for $I$ and $J$ to generate the same star operation, even excluding divisorial ideals. For example, if $R$ is an almost Dedekind domain that is not Dedekind, then all ideals are locally isomorphic but not all are divisorial, and two nondivisorial maximal ideals generate different star operations (if $M \neq N$ are two such ideals, then $(M : N) = M$ and so $N^{v(M)} = N^v \cap (M : (M : N)) = R$). For an example of non-locally isomorphic ideals generating the same star operation see Example 7.10.

The following necessary condition has been proved in [14, Lemma 3.7] when $I$ and $J$ are fractional ideals of a numerical semigroup; the proof of the integral domain case (which was also stated later in the same paper) can be obtained in exactly the same way.

**Proposition 3.5.** *Let* $R$ *be an integral domain and* $I, J$ *be nondivisorial ideals of* $R$*. If* $v(I) = v(J)$ *then*

$$I = I^v \cap \bigcap_{\gamma \in (I:J)(J:I) \setminus \{0\}} (\gamma^{-1} I).$$

## 4 Local Rings

As the construction of the principal star operation $v(I)$ generalizes the definition of $m$-canonical ideal, we expect that $I$ is in some way "$m$-canonical for $v(I)$". Pursuing this strategy, we obtain the following generalization of [9, Lemma 2.2(e)].

**Lemma 4.1.** *Let* $I$ *be an ideal of a domain* $R$ *such that* $(I : I) = R$*. Let* $\{J_\alpha \mid \alpha \in A\}$ *be* $v(I)$*-ideals such that* $\bigcap_{\alpha \in A} J_\alpha \neq (0)$*. Then,*

$$\left(I : \bigcap_{\alpha \in A} J_\alpha\right) = \left(\sum_{\alpha \in A} (I : J_\alpha)\right)^{v(I)}.$$

*Proof.* Let $J := \sum_{\alpha\in A}(I : J_\alpha)$. Since $(I : I) = R$, we have $L^{v(I)} = (I : (I : L))$ for every ideal $L$; therefore,

$$(I : J) = \left(I : \sum_{\alpha\in A}(I : J_\alpha)\right) = \bigcap_{\alpha\in A}(I : (I : J_\alpha)) = \bigcap_{\alpha\in A} J_\alpha^{v(I)} = \bigcap_{\alpha\in A} J_\alpha$$

and thus

$$J^{v(I)} = (I : (I : J)) = \left(I : \bigcap_{\alpha\in A} J_\alpha\right),$$

as claimed. □

The following definition abstracts a property proved, for $m$-canonical ideals of local domains, in [9, Lemma 4.1].

**Definition 4.2.** Let $\star$ be a star operation on $R$. We say that an ideal $I$ of $R$ is *strongly $\star$-irreducible* if $I = I^\star \neq \bigcap\{J \in \mathcal{F}^\star(R) \mid I \subsetneq J\}$.

**Lemma 4.3.** *Let $R$ be a domain and $I$ be a nondivisorial ideal of $R$. If $I$ is strongly $v(I)$-irreducible and $v(I) = v(J)$, then $I = uJ$ for some $u \in K$.*

*Proof.* Suppose $v(I) = v(J)$. Then

$$I = I^{v(J)} = I^v \cap \bigcap_{\alpha\in(J:I)\setminus\{0\}} \alpha^{-1}J.$$

Both $I^v$ and each $\alpha^{-1}J$ are $v(I)$-ideals; hence, either $I = I^v$ (which is impossible since $I$ is not divisorial) or $I = \alpha^{-1}J$ for some $\alpha \in K$. □

**Lemma 4.4.** *Suppose $(R, M)$ is a local ring and $R = (I : I)$. If $M$ is $v(I)$-closed, then $I$ is strongly $v(I)$-irreducible.*

*Proof.* Let $\{J_\alpha\}$ be a family of $v(I)$-ideals such that $I = \bigcap J_\alpha$. Then,

$$R = (I : I) = \left(I : \bigcap_\alpha J_\alpha\right) = \left(\sum_\alpha (I : J_\alpha)\right)^{v(I)}$$

by Lemma 4.1.

Hence $(I : J_\alpha) \subseteq R$ for every $\alpha$; suppose $I \subsetneq J_\alpha$ for all $\alpha$. Then, $1 \notin (I : J_\alpha)$ and thus $(I : J_\alpha) \subseteq M$; therefore, $\sum(I : J_\alpha) \subseteq M$ and, since $M$ is $v(I)$-closed, also $\left(\sum_\alpha(I : J_\alpha)\right)^{v(I)} \subseteq M$, a contradiction. Therefore, we must have $J_\alpha = I$ for some $\alpha$, and $I$ is strongly $v(I)$-irreducible. □

As a consequence of the previous two lemmas, we have a very general result for local rings.

**Proposition 4.5.** *Let $(R, M)$ be a local domain and $I$ a nondivisorial ideal of $R$ such that $(I : I) = R$. If $M = M^{v(I)}$ (in particular, if $M$ is divisorial), then $v(I) = v(J)$ for some ideal $J$ if and only if $I = uJ$ for some $u \in K$.*

*Proof.* By Lemma 4.4, $I$ is strongly $v(I)$-irreducible; by Lemma 4.3 it follows that $I = uJ$. □

**Corollary 4.6.** *Let $(R, M)$ be a local domain, and $I$ and $J$ two nondivisorial ideals of $R$. If $R$ is completely integrally closed and $M$ is divisorial, then $v(I) = v(J)$ if and only if $I = uJ$ for some $u \in K$.*

*Proof.* Since $R$ is completely integrally closed, $(L : L) = R$ for all ideals $L$; furthermore, since $M$ is divisorial $M^{v(L)} = M$ for every $L$. The claim follows from Proposition 4.5. □

One problem of the previous results is the hypothesis $(I : I) = R$. In the following proposition we eliminate it at the price of forcing more properties on $R$.

**Proposition 4.7.** *Let $(R, M)$ be a local ring, and let $T := (M : M)$. Let $I, J$ be ideals of $R$, properly contained between $R$ and $T$, such that $v(I) = v(J)$.*

*(a) If $(I : I), (J : J) \subseteq T$, then $(I : I) = (J : J)$.*
*(b) Suppose also that $(I : I) =: A$ is local with divisorial maximal ideal, and that $I$ and $J$ are not divisorial over $A$. Then, there is a $u \in K$ such that $I = uJ$.*

*Proof.* If $M$ is principal, $T = R$ and the statement is vacuous. Suppose thus $M$ is not principal: then, we also have $T = (R : M)$. We first claim that $L^v = T$ for every ideal $L$ properly contained between $R$ and $T$. Indeed, the containment $R \subsetneq L$ implies that $(R : L) \subsetneq R$ and thus, since $R$ is local, $(R : L) \subseteq M$ and $L^v \supseteq T \supsetneq L$; hence, $L^v = T$.

(a) Let $T_1 := (I : I)$ and $T_2 := (J : J)$, and define $\star_i$ as the star operation $L^{\star_i} := L^v \cap LT_i$. Since $T$ contains $T_1$ and $T_2$, it is both a $T_1$- and a $T_2$-ideal. We claim that $L \neq R$ is $\star_i$-closed if and only if it is a $T_i$-ideal: the "if" part is obvious, while if $L = L^v \cap LT_i$ then $L^v = T$ is a $T_i$-ideal and thus $L$ is intersection of two $T_i$-ideals.

If $v(I) = v(J)$, then $I$ is $\star$-closed if and only if $J$ is $\star$-closed; therefore, since $I$ is $\star_1$-closed and $J$ is $\star_2$-closed, both $I$ and $J$ are $T_1$- and $T_2$-ideals. But $(I : I)$ (respectively, $(J : J)$) is the maximal overring of $R$ in which $I$ (respectively, $J$) is an ideal; thus $(I : I) = (J : J)$.

(b) Consider the star operation generated by $I$ on $A$, i.e., $v_A(I) : L \mapsto (A : (A : L)) \cap (I : (I : L))$ for every $L \in \mathcal{F}(A)$. By the first paragraph of the proof, applied on the $A$-ideals, we have $(A : (A : L)) = T$ for all ideals $L$ of $A$ properly contained between $A$ and $T$; in particular, this happens for $J$ (since $R \subset J$ implies $A = AR \subseteq AJ = J$, and $A \neq J$ since $J$ is not divisorial), and thus $J^{v_A(I)} = J^{v(I)} = J$. Symmetrically, $I^{v_A(J)} = I$; hence, $v_A(I) = v_A(J)$. By Proposition 4.5, applied to $A$, we have $I = uJ$ for some $u \in K$, as claimed. □

Recall that a *pseudo-valuation domain* (PVD) is a local domain $(R, M)$ such that $M$ is the maximal ideal of a valuation overring of $R$ (called the valuation domain *associated* to $R$) [8].

**Corollary 4.8.** *Let $(R, M)$ be a pseudo-valuation domain with associated valuation ring $V$, and suppose that the field extension $R/M \subseteq V/M$ is algebraic. Let $I, J$ be nondivisorial ideals of $R$. Then, $v(I) = v(J)$ if and only if $I = uJ$ for some $u \in K$.*

*Proof.* By [12, Proposition 2.2(5)], there are $a, b \in K$ such that $a^{-1}I$ and $b^{-1}J$ are properly contained between $R$ and $V = (M : M)$. Furthermore, since $R/M \subseteq V/M$ is algebraic, every ring between $R$ and $V$ is the pullback of some intermediate field, and in particular it is itself a PVD with maximal ideal $M$. The claim follows from Proposition 4.7. □

## 5 Localizations

Let $\star$ be a star operation on $R$ and $T$ a flat overring of $R$. Then, $\star$ is said to be *extendable* to $T$ if the map

$$\begin{aligned} \star_T : \mathcal{F}(T) &\longrightarrow \mathcal{F}(T) \\ IT &\longmapsto I^\star T \end{aligned}$$

is well-defined; when this happens, $\star_T$ is called the *extension* of $\star$ to $T$ and is a star operation on $T$ [16, Definition 3.1]. In general, not all star operations are extendable, although finite-type operations are (see [10, Proposition 2.4] and [16, Proposition 3.3(d)]).

We would like to have an equality $v(I)_T = v(IT)$, where the latter is considered as a star operation on $T$. In general, this is false, both because $v(I)$ may not be extendable and because the extension $v(I)_T$ may not be equal to $v(IT)$.

For example, let $V$ be a valuation domain and suppose that its maximal ideal $M$ is principal. Let $P$ be a prime ideal of $V$. Then, the only star operation on $V$ is the identity, and thus $v(I) = d$ for all ideals $I$; in particular, $v(I)$ is extendable to $V_P$ and the extension $v(I)_{V_P}$ is the identity on $V_P$. Suppose now that $P = PV_P$ is not principal as an ideal of $V_P$. Then, $V_P$ has two star operations (the identity and the $v$-operation) and if $a \in K \setminus \{0\}$ then $aV_P$ generates the $v$-operation. Hence, the extension of $v(aV) \in \mathrm{Star}(V)$ to $V_P$ is different from $v(aV_P) \in \mathrm{Star}(V_P)$.

In the Noetherian case, however, everything works.

**Proposition 5.1.** *If $R$ is Noetherian, then $v(I)_T = v(IT)$ for every flat overring $T$ of $R$.*

*Proof.* By definition, $J^{v(I)} = (R : (R : J)) \cap (I : (I : J))$; multiplication by a flat overring commutes with finite intersections, and since every ideal is finitely generated, the colon localizes, and thus

$$\begin{aligned}J^{v(I)}T &= (R:(R:J))T \cap (I:(I:J))T = \\ &= (T:(T:JT)) \cap (IT:(IT:JT)) = \\ &= (JT)^{v_T} \cap (IT:(IT:JT)) = (JT)^{v(IT)},\end{aligned}$$

i.e., $v(I)_T = v(IT)$. □

Another case where localization works well is for Jaffard families. If $R$ is an integral domain with quotient field $K$, a *Jaffard family* of $R$ is a set $\Theta$ of flat overrings of $R$ such that [6, Section 6.3.1]:

- $\Theta$ is locally finite;
- $I = \prod\{IT \cap R \mid T \in \Theta, IT \neq T\}$ for every integral ideal $I$;
- $(IT_1 \cap R) + (IT_2 \cap R) = R$ for every integral ideal $I$ and every $T_1 \neq T_2$ in $\Theta$.

Jaffard families can be used to factorize the set of star operations of a domain $R$ into a direct product of sets of star operations.

**Theorem 5.2.** *Let $R$ be an integral domain and let $\Theta$ be a Jaffard family on $R$. Then, every star operation on $R$ is extendable to every $T \in \Theta$, and the map*

$$\begin{aligned}\lambda_\Theta \colon \mathrm{Star}(R) &\longrightarrow \prod_{T\in\Theta} \mathrm{Star}(T) \\ \star &\longmapsto (\star_T)_{T\in\Theta}\end{aligned}$$

*is an order-preserving order-isomorphism.*

*Proof.* It is a part of [16, Theorem 5.4]. □

For principal star operations, the previous result must be modified using, instead of the direct product, a "direct sum"-like construction. Given a family $\Theta$ of overrings, we set

$$\bigoplus_{T\in\Theta} \mathrm{Princ}(T) := \left\{(\star^{(T)}) \in \prod_{T\in\Theta} \mathrm{Princ}(T) \mid \star^{(T)} \neq v^{(T)} \text{ for only finitely many } T\right\}.$$

Using this terminology, we have the following.

**Proposition 5.3.** *Let $R$ be an integral domain and $\Theta$ be a Jaffard family on $R$. For every ideal $I$ of $R$ and every $T \in \Theta$, we have $v(I)_T = v(IT)$; furthermore, the map*

$$\begin{aligned}\Upsilon \colon \mathrm{Princ}(R) &\longrightarrow \bigoplus_{T\in\Theta} \mathrm{Princ}(T) \\ v(I) &\longmapsto (v(IT))_{T\in\Theta}\end{aligned}$$

*is a well-defined order-isomorphism.*

*Proof.* By Theorem 5.2 $v(I)$ is extendable to any $T \in \Theta$; furthermore, by [16, Lemma 5.3], we have $(J : L)T = (JT : LT)$ for every pair of fractional ideals $J, L$ of $R$. Using the same calculation of Proposition 5.1 we get $v(I)_T = v(IT)$.

In particular, it follows that the map $\Upsilon$ is just the restriction of the localization map $\lambda_\Theta$ to $\mathrm{Princ}(R)$; since $\lambda_\Theta$ is an isomorphism (by Theorem 5.2), we have only to show that the image of $\Upsilon$ is the direct sum $\bigoplus_{T\in\Theta} \mathrm{Princ}(T)$.

Since $IT = T$ for all but a finite number of $T$ (by definition of a Jaffard family), we have $v(IT) = v(T) = v^{(T)}$ for all but a finite number of $T$. In particular, the image of $\Upsilon$ lies inside the direct sum.

Suppose, conversely, that $(v(J_T))_{T\in\Theta} \in \bigoplus_{T\in\Theta} \mathrm{Princ}(T)$. We can suppose that $J_T \subseteq T$ for every $T$, and that $J_T = T$ if $v(J_T) = v^{(T)}$. Define thus $I := \bigcap_{T\in\Theta} J_T$: then, $I$ is nonzero (since $J_T \neq T$ for only a finite number of $T$) and $IT = J_T$ for every $T$ [16, Lemma 5.2]. Therefore, $v(I)_T = v(IT) = v(J_T)$, and the image of $\Upsilon$ is exactly $\bigoplus_{T\in\Theta} \mathrm{Princ}(T)$. □

Proposition 5.3 can be interpreted as a way to factorize principal star operations.

**Corollary 5.4.** *Let $R$ be an integral domain and $\Theta$ be a Jaffard family on $R$. Let $I$ be an integral ideal of $R$. Then, there are $T_1, \dots, T_n \in \Theta$ such that $v(I) = v(IT_1 \cap R) \wedge \cdots \wedge v(IT_n \cap R)$.*

*Proof.* Since $I \subseteq R$, we have $IT = T$ for all but finitely many $T \in \Theta$; let $T_1, \dots, T_n$ be the exceptions. The claim follows from Proposition 5.3. □

Recall that an integral domain is said to be *h-local* if every ideal is contained in a finite number of maximal ideals and every prime ideal is contained in only one maximal ideal.

**Corollary 5.5.** *Let $R$ be an $h$-local Prüfer domain, and let $\mathcal{M}$ be the set of non-divisorial maximal ideals of $R$. Then, there is a bijective correspondence between* $\mathrm{Princ}(R)$ *and the set $\mathcal{P}_{\mathrm{fin}}(\mathcal{M})$ of finite subsets of $\mathcal{M}$. Furthermore, $\mathcal{M}$ is finite if and only if every star operation is principal.*

*Proof.* Since $R$ is $h$-local, $\{R_M \mid M \in \mathrm{Max}(R)\}$ is a Jaffard family of $R$, and thus by Proposition 5.3 there is a bijective correspondence $\Upsilon$ between $\mathrm{Princ}(R)$ and $\bigoplus_{M\in\mathrm{Max}(R)} \mathrm{Princ}(R_M)$. If $M \notin \mathcal{M}$, then $MR_M$ is principal and thus $\mathrm{Star}(R_M) = \mathrm{Princ}(R_M) = \{d = v\}$; hence, $\Upsilon$ restricts to a bijection $\Upsilon'$ between $\mathrm{Princ}(R)$ and $\bigoplus_{M\in\mathcal{M}} \mathrm{Princ}(R_M)$. Since $R_M$ is a valuation domain, each $\mathrm{Princ}(R_M)$ is composed by two elements (the identity and the $v$-operation). Thus, we can construct a bijection $\Upsilon_1$ from the direct sum to $\mathcal{P}_{\mathrm{fin}}(\mathcal{M})$ by associating to $\star := (\star^{(M)})$ the finite set $\Upsilon_1(\star) := \{M \in \mathcal{M} \mid \star^{(M)} \neq v\}$. The composition $\Upsilon_1 \circ \Upsilon'$ is a bijection from $\mathrm{Princ}(R)$ to $\mathcal{P}_{\mathrm{fin}}(\mathcal{M})$.

The last claim follows immediately. □

A factorization property similar to Corollary 5.4 can be proved for ideals having a primary decomposition with no embedded primes.

**Proposition 5.6.** *Let $Q_1, \dots, Q_n$ be primary ideals, let $P_i := \mathrm{rad}(Q_i)$ for all $i$ and let $I := Q_1 \cap \cdots \cap Q_n$. If the $P_i$ are pairwise incomparable, then $v(I) = v(Q_1) \wedge \cdots \wedge v(Q_n)$.*

*Proof.* For every $i$, the ideal $Q_i$ is $v(Q_i)$-closed, and thus $I$ is $(v(Q_1) \wedge \cdots \wedge v(Q_n))$-closed; hence, $v(I) \geq v(Q_1) \wedge \cdots \wedge v(Q_n)$. To prove the converse, we need to show that each $Q_i$ is $v(I)$-closed.

Without loss of generality, let $i = 1$, and define $\widehat{Q} := Q_2 \cap \cdots \cap Q_n$; we claim that $Q_1 = (I :_R \widehat{Q})$. Since $Q_1\widehat{Q} \subseteq Q_1 \cap \widehat{Q} = I$, clearly $Q_1 \subseteq (I :_R \widehat{Q})$. Conversely, let $x \in (I :_R \widehat{Q})$. Since the radicals of the $Q_i$ are pairwise incomparable, $Q_i \nsubseteq P_1$ for every $i > 1$, and so $\widehat{Q} \nsubseteq P_1$; therefore, there is a $q \in \widehat{Q} \setminus P_1$. Then, $xq \in I$, and in particular $xq \in Q_1$. If $x \notin Q_1$, then since $Q_1$ is primary we would have $q^t \in Q_1$ for some $t \in \mathbb{N}$; however, this would imply $q \in \mathrm{rad}(Q_1) = P_1$, against the choice of $q$. Thus, $Q_1 \subseteq (I :_R \widehat{Q})$ and so $Q_1 = (I :_R \widehat{Q})$.

By definition, $I$ is $v(I)$-closed; hence, also $(I :_R \widehat{Q})$ is $v(I)$-closed. It follows that $Q_1$ is $v(I)$-closed, and thus that each $Q_i$ is $v(I)$-closed, i.e., $v(I) \leq v(Q_1) \wedge \cdots \wedge v(Q_n)$. The claim is proved. □

# 6 *v*-Trivial Ideals

In this section, we analyze principal operations generated by $v$-trivial ideals.

**Definition 6.1.** An ideal $I$ of a domain $R$ is *$v$-trivial* if $I^v = R$.

**Lemma 6.2.** *If $I$ is $v$-trivial, then $(I : I) = R$.*

*Proof.* If $I^v = R$, then $(R : I) = R$, and thus $(I : I) \subseteq (R : I) = R$. □

**Definition 6.3.** A star operation $\star$ is *semifinite* (or *quasi-spectral*) if every $\star$-closed ideal $I \subsetneq R$ is contained in a $\star$-prime ideal.

All finite type and all spectral operations are semifinite; on the other hand, if $V$ is a valuation domain with maximal ideal that is branched but not finitely generated, the $v$-operation on $V$ is not semifinite. The class of semifinite operations is closed by taking infima, but not by taking suprema (see [5, Example 4.5]).

**Lemma 6.4.** *Let $R$ be an integral domain, and let $I$, $J$ be $v$-trivial ideals of $R$.*

*(a)* *If $J \subsetneq I$, then $J^{v(I)} = I$, and in particular $v(I) \neq v(J)$.*

*Suppose $v$ is semifinite on $R$.*

*(b)* *$I \cap J$ is $v$-trivial.*
*(c)* *$I \subseteq J^{v(I)}$.*
*(d)* *If $I \neq J$, then $v(I) \neq v(J)$.*

*Proof.* (a) Since $I$ is $v$-trivial, by Lemma 6.2 and Proposition 3.2 we have $J^{v(I)} = (I : (I : J))$.
However, $R \subseteq (I : J) \subseteq (R : J) = R$ (using the $v$-triviality of $J$) and thus $J^{v(I)} = (I : R) = I$, as claimed. In particular, $J = J^{v(J)} \neq J^{v(I)}$ and so $v(I) \neq v(J)$.

(b) If $(I \cap J)^v \neq R$, then by semifiniteness there is a prime ideal $P$ such that $I \cap J \subseteq P = P^v$. However, this would imply $I \subseteq P$ or $J \subseteq P$, against the hypothesis that $I$ and $J$ are $v$-trivial.

(c) Since $J \subseteq J^{v(I)}$, it follows that $J^{v(I)}$ is $v$-trivial, and by the previous point so is $J^{v(I)} \cap I$. If $I \nsubseteq J^{v(I)}$, it would follow that $J^{v(I)} \cap I \subsetneq I$, but $J^{v(I)} \cap I$ is $v(I)$-closed, against (a). Hence $I \subseteq J^{v(I)}$.

(d) If both $I$ and $J$ are $v(I)$-closed, then so is $I \cap J$; by (b), $(I \cap J)^v = R$. The claim follows applying (a) to $I \cap J$ and $I$ (or $J$). □

**Corollary 6.5.** *Let $R$ be a domain such that $v$ is semifinite. Let $I, J$ be ideals of $R$ such that $I^v$ and $J^v$ are invertible; then, $v(I) = v(J)$ if and only if $I = LJ$ for some invertible ideal $L$.*

*Proof.* By invertibility, we have

$$R = I^v(R : I^v) = (I^v(R : I^v))^v = (I(R : I^v))^v;$$

since $I \subseteq I(R : I^v) \subseteq R$, the ideal $I(R : I^v)$ is $v$-trivial. Analogously, $R = (J(R : J^v))^v$ and $J(R : J^v)$ is $v$-trivial. Hence, by Lemma 6.4(d) $I(R : I^v) = J(R : J^v)$; thus, $I = I^v(R : J^v)J$, and $L := I^v(R : J^v)$ is invertible. □

We denote by $h(I)$ the height of the integral ideal $I$.

**Corollary 6.6.** *Let $R$ be a unique factorization domain. Then,*

*(a) for every principal star operation $\star \neq v$ there is a proper ideal $I$ such that $h(I) > 1$ and $\star = v(I)$;*
*(b) if $I, J$ are fractional ideals of $R$, $v(I) = v(J)$ if and only if $I = uJ$ for some $u \in K$.*

*Proof.* Let $\star = v(I)$ for some ideal $I$. By [7, Corollary 44.5], every $v$-closed ideal of $R$ is principal; hence, let $I^v = pR$. Then, $(p^{-1}I)^v = R$, i.e., $p^{-1}I$ is $v$-trivial. In particular, $\star = v(I) = v(p^{-1}I)$, and $p^{-1}I$ is a proper ideal of $R$ with $h(p^{-1}I) > 1$ (since all prime ideals of height 1 are $v$-closed).

Suppose that we also have $\star = v(J)$. With the same reasoning of the previous paragraph, $q^{-1}J$ is $v$-trivial for some $q$; thus $v(p^{-1}I) = v(I) = v(J) = v(q^{-1}J)$. Applying Lemma 6.4 (d) to $p^{-1}I$ and $q^{-1}J$ we get $p^{-1}I = q^{-1}J$, i.e., $I = (pq^{-1})J$. □

For star operations generated by $v$-trivial prime ideals, we can also determine the set of closed ideals.

**Proposition 6.7.** *Let $R$ be a domain such that $v$ is semifinite and such that $I^v$ is invertible for every ideal $I$, and let $P \in \mathrm{Spec}(R)$. Then $\mathcal{F}^{v(P)}(R) = \mathcal{F}^v(R) \cup \{LP \mid L$ is an invertible ideal$\}$. In particular, $v(P)$ is a maximal element of $\mathrm{Princ}(R) \setminus \{v\}$.*

*Proof.* Let $I$ be a nondivisorial ideal; multiplying by an invertible ideal $L$, we can suppose $I^v = R$. If $I \subseteq P$, by Lemma 6.4 (a) $I^{v(P)} = P$, and thus $I \neq I^{v(P)}$ unless $I = P$; suppose $I \nsubseteq P$. Then $(P : I) = P$: we have $(P : I) \subseteq (R : I) = R$, and thus if $xI \subseteq P$ then $x \in P$. Therefore, $I^{v(P)} = I^v \cap (P : (P : I)) = R \cap (P : P) = R \neq I$.

For the "in particular" claim, note that if $v(I) \geq v(P)$ then $I$ should be $\star$-closed; by the previous part of the proof, this means that either $I$ is divisorial (and so $v(I) = v$) or $I = LP$ for some invertible $L$ (and thus $v(I) = v(P)$ by Lemma 3.4(d)). □

**Corollary 6.8.** *Let $R$ be a unique factorization domain, and let $P \in \mathrm{Spec}(R)$. Then, $\mathcal{F}^{v(P)}(R) = \mathcal{F}^v(R) \cup \{aP \mid a \in K\}$.*

We have seen in Proposition 3.3 that all star operations can be "generated" by principal star operations; we can use $v$-trivial ideals to show that in many cases we need infinitely many of them.

**Proposition 6.9.** *Let $R$ be a domain such that $v$ is semifinite, and let $I_1, \dots, I_n$ be $v$-trivial ideals; let $\star := v(I_1) \wedge \cdots \wedge v(I_n)$. Then, the ideal $I_1 \cap \cdots \cap I_n$ is the minimal $v$-trivial ideal that is $\star$-closed.*

*Proof.* Let $J := I_1 \cap \cdots \cap I_n$. By Lemma 6.4 (b), $J$ is $v$-trivial. Clearly $J$ is $\star$-closed. Suppose $L$ is $v$-trivial; then, applying Lemma 6.4(c),

$$L^\star = L^{v(I_1) \wedge \cdots \wedge v(I_n)} \supseteq I_1 \cap \cdots \cap I_n = J.$$

Therefore, $J$ is the minimum among $v$-trivial $\star$-closed ideals. □

**Corollary 6.10.** *Let $R$ be a unique factorization domain, and let $\star \in \mathrm{Star}(R)$ be such that $\star \neq v$. If $\bigcap\{J \in \mathcal{F}^\star(R) \mid J^v = R\} = (0)$, then $\star$ is not the infimum of a finite family of principal star operations.*

*Proof.* Since $R$ is a UFD, the $v$-operation is semifinite, and every principal star operation can be generated by a $v$-trivial ideal. If $\star$ were to be finitely generated, say $\star = v(I_1) \wedge \cdots \wedge v(I_n)$, then $J := I_1 \cap \cdots \cap I_n$ would be the minimal $v$-trivial $\star$-closed ideal; however, by hypothesis, there must be a $v$-trivial $\star$-closed ideal $J'$ not containing $J$, and thus $\star$ cannot be finitely generated. □

**Proposition 6.11.** *Let $R$ be a domain, and let $\Delta$ be a set of overrings whose intersection is $R$. Let $\star$ be the star operation $I \mapsto \bigcap\{IT \mid T \in \Delta\}$. Suppose that*

*(1) $v$ is semifinite;*
*(2) every $v$-trivial ideal contains a finitely generated $v$-trivial ideal;*
*(3) there is a $v$-trivial $\star$-closed ideal.*

*Then, $\star$ is not the infimum of a finite family of principal star operations.*

*Proof.* By substituting an overring $T \in \Delta$ with $\{T_M \mid M \in \mathrm{Max}(T)\}$, we can suppose without loss of generality that each member of $\Delta$ is local.

If $\star$ were finitely generated, by Proposition 6.9 there would be a minimal $v$-trivial $\star$-closed ideal, say $J$. By hypothesis, there is finitely generated $v$-trivial ideal $I \subseteq J$; since $I^\star = J$, by [1, Theorem 2], we have $IT = JT$ for every $T \in \Delta$.

Since $I^\star \neq R$, there must be an $S \in \Delta$ such that $IS \neq S$; by Nakayama's lemma, $I^2S = (IS)^2 \subsetneq IS$, and so $(I^2)^\star \subseteq I^2S \cap R \subsetneq I$. In particular, $(I^2)^\star$ is a $v$-trivial $\star$-closed ideal, against the definition of $I$. Thus, $\star$ is not finitely generated. □

The first two hypothesis hold, for example, for unique factorization domains of dimension $d > 1$; the third one holds, for example, in the following cases:

- $\star$ is a spectral star operation of finite type different from the $w$-operation (see [2, 17]);
- if $R$ is integrally closed and (at least) one maximal ideal is not divisorial, and $\star$ is the $b$-operation/integral closure;
- if $R$ is a UFD, all star operations coming from overrings, except the $v$-operation.

## 7 Noetherian Domains

In this section, we study in more detail the case of Noetherian domains; in particular, we shall give in Theorem 7.8 a necessary and sufficient condition on when $v(I) = v(J)$, under the assumption that $(I : I) = R = (J : J)$. We first state a case that is already settled, even without this hypothesis.

**Proposition 7.1.** *[14, Proposition 5.4] Let $(R, M)$ be a local Noetherian integral domain of dimension 1 such that its integral closure $V$ is a discrete valuation domain that is finite over $R$; suppose also that the induced map of residue fields $R/M \subseteq V/M_V$ is an isomorphism. Then, $v(I) = v(J)$ if and only if $I = uJ$ for some $u \in K$, $u \neq 0$.*

We denote by $\mathrm{Ass}(I)$ the set of associated primes of $I$.

**Proposition 7.2.** *Let $R$ be a domain and $I$ an ideal of $R$. Then,* $\mathrm{Spec}^{v(I)}(R) \supseteq \mathrm{Spec}^{v}(R) \cup \mathrm{Ass}(I)$*, and if $R$ is Noetherian the two sets are equal.*

*Proof.* If $P \in \mathrm{Ass}(I)$, then $P = (I :_R x) = x^{-1}I \cap R$ for some $x \in R$, and thus it is $v(I)$-closed; if $P \in \mathrm{Spec}^v(R)$ then $P = P^v$ and thus $P = P^{v(I)}$.

Conversely, suppose $R$ is Noetherian and $P = P^{v(I)}$. Then $P = P^v \cap (I : (I : P)) = P^v \cap (I : J)$, where $J = (I : P)$; let $J = j_1R + \cdots + j_nR$. We have

$$\begin{aligned} P &= P^v \cap (I : J) = P^v \cap R \cap (I : J) = P^v \cap (I :_R J) = \\ &= P^v \cap (I :_R j_1R + \cdots + j_nR) = P^v \cap \textstyle\bigcap_{i=1}^n (I :_R j_iR), \end{aligned}$$

and, since $P$ is prime, this implies that $P^v = P$ or $(I :_R j_iR) = P$ for some $i$. In the latter case, since $j_i \in K$, $j_i = a/b$ for some $a, b \in R$; hence $(I :_R j_iR) = (I : ab^{-1}R) \cap R = (bI :_R aR)$, and thus $P$ is associated to $bI$. There is an exact sequence

$$0 \longrightarrow \frac{bR}{bI} \longrightarrow \frac{R}{bI} \longrightarrow \frac{R}{bR} \longrightarrow 0$$

and, since $R$ is a domain, $bR/bI \simeq R/I$ and thus $\mathrm{Ass}(bI) \subseteq \mathrm{Ass}(I) \cup \mathrm{Ass}(bR)$ [3, Chapter IV, Proposition 3]; therefore, $P$ is associated to $I$ or it is divisorial (since an associated prime of a divisorial ideal—in this case, $bR$—is divisorial). □

**Remark 7.3.** Note that, if $P^v = R$, then $(I : P) \subseteq (R : P) = R$, and thus $j_i \in R$; in this case, $b = 1$ and the last part of the proof can be greatly simplified.

The following is a slight improvement of Proposition 6.7. We denote by $X^1(R)$ the set of height-1 prime ideals of $R$.

**Corollary 7.4.** *Let $R$ be an integrally closed Noetherian domain. Then, the maximal elements of* $\mathrm{Princ}(R) \setminus \{v\}$ *are the $v(P)$, as $P$ ranges in* $\mathrm{Spec}(R) \setminus X^1(R)$.

*Proof.* Since $R$ is integrally closed, the divisorial prime ideals of $R$ are the height 1 primes. In particular, if $P$ is a prime ideal of height $> 1$, then $v(P)$ is maximal by Proposition 6.7.

Conversely, suppose $v(I)$ is maximal in $\mathrm{Princ}(R) \setminus \{v\}$. If all associated primes of $I$ have height 1, then $I = \bigcap_{P \in X^1(R)} IR_P$, and so $I$ is divisorial, against $v(I) \neq v$. Hence, there is a $P \in \mathrm{Ass}(I) \setminus X^1(R)$; by Proposition 7.2, $P \in \mathrm{Spec}^{v(I)}(R)$, and thus $v(I) \leq v(P)$. As $v(I)$ is maximal, it follows that $v(I) = v(P)$. The claim is proved. □

**Corollary 7.5.** *Let $R$ be a Noetherian unique factorization domain. Then, $v(I)$ is a maximal element of* $\mathrm{Princ}(R) \setminus \{v\}$ *if and only if $I = uP$ for some prime ideal* $P \in \mathrm{Spec}(R) \setminus X^1(R)$ *and some $u \in K$.*

*Proof.* It is enough to join Corollary 7.4 (the maximal elements are the $v(P)$) with Corollary 6.6 ($v(I) = v(P)$ if and only if $I = uP$). □

Proposition 7.2 allows to determine, in the Noetherian case, all the spectra of the principal star operations. We need a lemma.

**Lemma 7.6.** *Let $\star_1, \ldots, \star_n \in \mathrm{Star}(R)$, and let $\star := \star_1 \wedge \cdots \wedge \star_n$. Then,* $\mathrm{Spec}^\star(R) = \bigcup_i \mathrm{Spec}^{\star_i}(R)$.

*Proof.* If $P = P^{\star_i}$ for some $i$ then $P^\star \subseteq P^{\star_i} = P$ and thus $P = P^\star$. Conversely, if $P = P^\star$ then $P = P^{\star_1} \cap \cdots \cap P^{\star_n}$; since $P$ is prime, it follows that $P = P^{\star_i}$ for some $i$. The claim is proved. □

**Proposition 7.7.** *Let $R$ be a Noetherian domain, and let $\Delta \subseteq \mathrm{Spec}(R)$. Then, the following are equivalent:*

*(i)* $\Delta = \mathrm{Spec}^{v(I)}(R)$ *for some ideal $I$;*
*(ii)* $\Delta = \mathrm{Spec}^{\star}(R)$ *for some $\star = v(I_1) \wedge \cdots \wedge v(I_n)$;*
*(iii)* $\Delta = \mathrm{Spec}^{v}(R) \cup \Delta'$, *for some finite set $\Delta'$.*

*Proof.* (i) $\Longrightarrow$ (ii) is obvious, while (ii) $\Longrightarrow$ (iii) follows from Lemma 7.6.

If (iii) holds, then by [18, Chapter 4, Theorem 21] there is an ideal $I$ whose set of associated primes is $\Delta'$. By Proposition 7.2, $\mathrm{Spec}^{v(I)}(R) = \mathrm{Spec}^{v}(R) \cup \Delta' = \Delta$, and so (i) holds. □

We now characterize when two nondivisorial ideals with $(I : I) = (J : J) = R$ generate the same star operation.

**Theorem 7.8.** *Let $R$ be a Noetherian domain, and let $I, J$ be nondivisorial ideals such that $(I : I) = (J : J) = R$. Then, $v(I) = v(J)$ if and only if $\mathrm{Ass}(I) \cup \mathrm{Spec}^v(R) = \mathrm{Ass}(J) \cup \mathrm{Spec}^v(R)$ and, for every $P \in \mathrm{Ass}(I) \cup \mathrm{Spec}^v(R)$, there is an $a_P \in K$ such that $IR_P = a_P JR_P$.*

*Proof.* Suppose the two conditions hold. By Proposition 7.2, $\mathrm{Ass}(I) \cup \mathrm{Spec}^v(R) = \mathrm{Spec}^{v(I)}(R)$, and thus $\mathrm{Spec}^{v(I)}(R) = \mathrm{Spec}^{v(J)}(R) =: \Delta$. For every ideal $L$, using Proposition 5.1 we have

$$L^{v(I)} = \bigcap_{P \in \Delta} L^{v(I)} R_P = \bigcap_{P \in \Delta} (LR_P)^{v(I)_{R_P}} = \bigcap_{P \in \Delta} (LR_P)^{v(IR_P)}.$$

Since $IR_P$ and $JR_P$ are isomorphic, $(LR_P)^{v(IR_P)} = (LR_P)^{v(JR_P)}$; it follows that $v(I) = v(J)$.

Conversely, suppose $v(I) = v(J) =: \star$. Then, $\mathrm{Spec}^\star(R)$ is equal to both $\mathrm{Ass}(I) \cup \mathrm{Spec}^v(R)$ and $\mathrm{Ass}(J) \cup \mathrm{Spec}^v(R)$, which thus are equal. Note also that $(I : I) = R$ implies that $R_P = (I : I)R_P = (IR_P : IR_P)$ for every prime ideal $P$.

Let now $P \in \mathrm{Spec}^\star(R)$. Since $v(I) = v(J)$, clearly $v(I)_{R_P} = v(J)_{R_P}$, which by Proposition 5.1 implies that $v(IR_P) = v(JR_P)$. However, $PR_P$ is $v(IR_P)$-closed because $P$ is $v(I)$-closed; it follows, by Proposition 4.5, that $IR_P = a_P JR_P$ for some $a_P \in K$, as claimed. □

**Corollary 7.9.** *Let $R$ be an integrally closed Noetherian domain, and let $I, J$ be nondivisorial ideals. Then, $v(I) = v(J)$ if and only if $\mathrm{Ass}(I) \cup X^1(R) = \mathrm{Ass}(J) \cup X^1(R)$ and for every $P \in \mathrm{Ass}(I)$ there is an $a_P \in R_P$ such that $IR_P = a_P JR_P$.*

*Proof.* Since $R$ is integrally closed and Noetherian, we have $(I : I) = R$ for every ideal $I$; furthermore, the divisorial primes are the height 1 primes, and for any such $P$ the localizations $IR_P$ and $JR_P$ are isomorphic since $R_P$ is a DVR. The claim now follows from Theorem 7.8. □

**Example 7.10.** Let $R$ be a Noetherian integrally closed domain, and suppose that $R_M$ is not a UFD for some maximal ideal $M$. Let $P$ be an height 1 prime contained in $M$ such that $PR_M$ is not principal, and let $Q$ be a prime ideal of height bigger than 1 such that $P + Q = R$ (in particular, $Q \nsubseteq M$). We claim that $v(PQ) = v(Q)$ but $PQ$ and $Q$ are not locally isomorphic.

In fact, since they are coprime, $PQ = P \cap Q$, and thus $\mathrm{Ass}(PQ) = \{P, Q\}$ while $\mathrm{Ass}(Q) = \{Q\}$; moreover, $P \nsubseteq Q$ and thus $PQR_Q = QPR_Q = QR_Q$. Since $P \in X^1(R)$, by Corollary 7.9 it follows that $v(PQ) = v(Q)$. However, $QR_M = R_M$ is principal, while $PQR_M = PR_M$, by hypothesis, is not; therefore, $Q$ and $PQ$ are not locally isomorphic. In particular, there cannot be an invertible ideal $L$ such that $Q = LPQ$, because $LR_M$ would be principal and thus $Q$ and $PQ$ would be locally isomorphic.

## References


1. Anderson, D.D.: Star-operations induced by overrings. Comm. Algebra **16**(12), 2535–2553 (1988)
2. Anderson, D.D., Cook, S.J.: Two star-operations and their induced lattices. Comm. Algebra **28**(5), 2461–2475 (2000)
3. Bourbaki, N.: Commutative Algebra. Chapters 1–7. Elements of Mathematics (Berlin). Springer, Berlin, 1989. Translated from the French, Reprint of the 1972 edition
4. Elliott, J.: Semistar operations on Dedekind domains. Comm. Algebra **43**(1), 236–248 (2015)
5. Finocchiaro, C.A., Fontana, M., Spirito, D.: Spectral spaces of semistar operations. J. Pure Appl. Algebra **220**(8), 2897–2913 (2016)
6. Fontana, M., Houston, E., Lucas, T.: Factoring Ideals in Integral Domains. Lecture Notes of the Unione Matematica Italiana, vol. 14. Springer, Heidelberg; UMI, Bologna (2013)
7. Gilmer, R.: Multiplicative Ideal Theory. Marcel Dekker Inc., New York, 1972. Pure and Applied Mathematics, No. 12
8. Hedstrom, J.R., Houston, E.G.: Pseudo-valuation domains. Pacific J. Math. **75**(1), 137–147 (1978)
9. Heinzer, W.J., Huckaba, J.A., Papick, I.J.: $m$-canonical ideals in integral domains. Comm. Algebra **26**(9), 3021–3043 (1998)
10. Houston, E.G., Mimouni, A., Park, M.H.: Integral domains which admit at most two star operations. Comm. Algebra **39**(5), 1907–1921 (2011)
11. Houston, E.G., Mimouni, A., Park, M.H.: Noetherian domains which admit only finitely many star operations. J. Algebra **366**, 78–93 (2012)
12. Houston, E.G., Mimouni, A., Park, M.H.: Integrally closed domains with only finitely many star operations. Comm. Algebra **42**(12), 5264–5286 (2014)
13. Picozza, G.: Star operations on overrings and semistar operations. Comm. Algebra **33**(6), 2051–2073 (2005)
14. Spirito, D.: Star Operations on Numerical Semigroups. Comm. Algebra **43**(7), 2943–2963 (2015)

15. Spirito, D.: Star operations on numerical semigroups: the multiplicity 3 case. Semigroup Forum **91**(2), 476–494 (2015)
16. Spirito, D.: Jaffard families and localizations of star operations. J. Commut. Algebra **11**(2), 265–300 (2019)
17. Wang, F., McCasland, R.L.: On $w$-modules over strong Mori domains. Comm. Algebra **25**(4), 1285–1306 (1997)
18. Zariski, O., Samuel, P.: Commutative algebra. Vol. 1. Springer, New York, Heidelberg, Berlin, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the: edition, p. 28. Graduate Texts in Mathematics, No (1958)

# Tilting Modules and Tilting Torsion Pairs

## Filtrations Induced by Tilting Modules

**Francesco Mattiello, Sergio Pavon and Alberto Tonolo**

**Abstract** Tilting modules, generalising the notion of progenerator, furnish equivalences between pieces of module categories. This paper is dedicated to study how much these pieces say about the whole category. We will survey the existing results in the literature, introducing also some new insights.

**Keywords** Tilting modules · Torsion pairs · $t$-structures · $t$-tree

## 1 Introduction

In 1958, Morita characterised equivalences between the entire categories of left (or right) modules over two rings. Let $A$ be an arbitrary associative ring with $1 \neq 0$. A left $A$-module ${}_AP$ is a *progenerator* if it is projective, finitely generated and generates the category $A$-Mod of left $A$-modules. Set $B := \mathrm{End}({}_AP)$, the covariant functor $\mathrm{Hom}_A(P, ?)$ gives an equivalence between $A$-Mod and $B$-Mod; moreover, any equivalence between modules categories is of this type.

The notion of tilting module has been axiomatised in 1979 by Brenner and Butler [BB], generalising that of progenerator for modules of projective dimension 1. The various forms of generalisations to higher projective dimensions considered until today continue to follow their approach.

F. Mattiello · S. Pavon
Dipartimento di Matematica "Tullio Levi-Civita",
Università degli studi di Padova, Padua, Italy
e-mail: fran.mattiello@gmail.com
e-mail: sergio.pavon@math.unipd.it

A. Tonolo (✉)
Dipartimento di Scienze Statistiche, Università degli studi di Padova, Padua, Italy
e-mail: alberto.tonolo@unipd.it

 
A. Facchini et al. (eds.), *Advances in Rings, Modules and Factorizations*,
Springer Proceedings in Mathematics & Statistics 321,
https://doi.org/10.1007/978-3-030-43416-8_18

A tilting module $T$ of projective dimension $n$ naturally gives rise to $n+1$ corresponding classes of modules in $A$-Mod and $B$-Mod, the Miyashita classes, with $n+1$ equivalences between them. These classes are

$$\mathrm{KE}_e(T) = \{M \in A\text{-Mod} : \mathrm{Ext}^i_A(T, M) = 0\ \forall i \neq e\}$$

$$\mathrm{KT}^e(T) = \{N \in B\text{-Mod} : \mathrm{Tor}^B_i(T, M) = 0\ \forall i \neq e\}, \quad e = 0, 1, ..., n$$

and the $n+1$ equivalences are

$$KE_e(T) \underset{\mathrm{Tor}^B_e(T,?)}{\overset{\mathrm{Ext}^e_A(T,?)}{\rightleftarrows}} KT^e(T)\ , \quad e = 0, 1, ..., n.$$

In the $n = 0$ case (progenerator), there is only one class on each side, and so every module is subject to the equivalence of categories (that of Morita); for $n = 1$, on each side, the two Miyashita classes form torsion pairs, so every module in both $A$-Mod and $B$-Mod can be decomposed in terms of modules in the Miyashita classes: precisely every module admits a composition series of length 2 with composition factors in the Miyashita classes.

For $n > 1$, the Miyashita classes fail to decompose every module; the way to recover a similar decomposition is the subject of this paper.

In Section 2, we define classical $n$-tilting modules and Miyashita classes; we show that they give a torsion pair for $n = 1$, and hence they can be used to decompose every module; we give an example showing that a similar decomposition does not exist for $n > 1$, and characterise those modules which can be decomposed.

In Section 3, we present some previous attempts to recover the decomposition for $n > 1$ as well, by extending the Miyashita classes, due to Jensen, Madsen, Su [11] and to Lo [13]. A useful tool in our analysis will be a characterisation of modules in $\bigcap_{i>e} \mathrm{Ker}\,\mathrm{Ext}^i_A(T, ?)$, $0 \leq e \leq n$ (see Lemma 1), which generalises the characterisation of modules in $\bigcap_{i>0} \mathrm{Ker}\,\mathrm{Ext}^i_A(T, ?)$ given by Bazzoni [3, Lemma 3.2]. These extensions deform in an irreversible way the Miyashita classes, weakening their role.

In Section 4, we recall some introductory notions about the derived category of an abelian category and about $t$-structures.

In Section 5, we drop the finiteness assumptions on the tilting modules, recalling the definition of non classical $n$-tilting modules [2]. In this setting, we recall the definition of the $t$-structure associated to such a module; we then study its interaction with the natural $t$-structure of the derived category.

In Section 6, we exploit the results of Section 5 to construct in the derived category the $t$-tree of a module with respect to a tilting module. This procedure, discovered in the classical tilting case by Fiorot, the first and the third author in [8], solves satisfactorily the decomposition problem for $n > 1$: the classes used for the decomposition intersect the module category exactly in the Miyashita classes. As a result of the work of the previous section, we prove that this construction can be reproduced also in the non classical case.

Throughout the paper, the concrete case considered in Example 1 introduced in Section 2 will be used to illustrate the various attempts to solve the decomposition problem (see Examples 2, 3).

## 2 Classical *n*-tilting Modules

In 1986, Miyashita [14] and Cline, Parshall and Scott [7] gave similar definitions of a *tilting module of projective dimension n*.

**Definition 1** (Miyashita [14]) A left $A$-module $T$ is a classical $n$-tilting module, for some integer $n \geq 0$, if

$p_n$) $T$ has a finitely generated projective resolution of length $n$, i.e. a projective resolution

$$0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow T \longrightarrow 0$$

with the $P_i$ finitely generated;

$e_n$) $T$ is rigid, i.e. $\text{Ext}^i_A(T, T) = 0$ for every $0 < i \leq n$;

$g_n$) the ring $A$ admits a coresolution of length $n$

$$0 \longrightarrow A \longrightarrow T_0 \longrightarrow \cdots \longrightarrow T_n \longrightarrow 0$$

with the $T_i$ finitely generated direct summands of arbitrary coproducts of copies of $T$.

In the case when $n = 0$, $p_0$) says that the module is a finitely generated projective, $e_0$) is empty and $g_0$) says that it is a generator: this is then the definition of a progenerator module. As such, a classical 0-tilting module $T$ induces a Morita equivalence of categories of modules, as follows. Let $B = \text{End}_A(T)$ be its ring of endomorphisms, which acts on the right on $T$, and consider the category $B$-Mod of left $B$-modules. There are functors

$$\begin{aligned} \text{Hom}_A(T, ?) :& \quad A\text{-Mod} \to B\text{-Mod} \\ T \otimes_B ? :& \quad B\text{-Mod} \to A\text{-Mod} \end{aligned}$$

which are category equivalences, with the unit and counit morphisms being those of the adjunction. This is the motivating example for the definition of tilting modules, along with the next case.

In the case when $n = 1$, we find what was originally (see Brenner and Butler [6]) defined as a *tilting module*; we will give a brief and incomplete overview of what is known about them.

Let $T$ be a classical 1-tilting left $A$-module, and let as before $B = \mathrm{End}_A(T)$ be its ring of endomorphisms. In this case, the pair $(\mathrm{Hom}_A(T, ?), T \otimes_B ?)$ does not induce an equivalence of $A$-Mod and $B$-Mod anymore; however, a little less can be proved, as follows.

Define the following pairs of full subcategories of $A$-Mod and $B$-Mod, respectively,

$$\begin{aligned} KE_0(T) &= \left\{X \in A\text{-Mod} :\ \mathrm{Ext}^1_A(T, X) = 0\right\} \\ KE_1(T) &= \{X \in A\text{-Mod} :\ \mathrm{Hom}_A(T, X) = 0\} \\ KT^0(T) &= \left\{Y \in B\text{-Mod} :\ \mathrm{Tor}^B_1(T, Y) = 0\right\} \\ KT^1(T) &= \{Y \in B\text{-Mod} :\ T \otimes_B Y = 0\}\,. \end{aligned}$$

Then we have the following results.

**Theorem 1** (Brenner and Butler [6]) *Let $A$ be a ring, $T$ a classical 1-tilting left $A$-module, $B = \mathrm{End}_A(T)$.*

*i) The pairs $(KE_0(T), KE_1(T))$ and $(KT^1(T), KT^0(T))$ defined above are torsion pairs, respectively, in $A$-Mod and $B$-Mod.*
*ii) There are equivalences of (sub)categories*

$$KE_0(T) \underset{T\otimes_B ?}{\overset{\mathrm{Hom}_A(T,?)}{\rightleftarrows}} KT^0(T)$$

$$KE_1(T) \underset{\mathrm{Tor}^B_1(T,?)}{\overset{\mathrm{Ext}^1_A(T,?)}{\rightleftarrows}} KT^1(T)\ .$$

This theorem shows that the 1-tilting case is slightly more complex than the 0-tilting one. Instead of having an equivalence of the whole categories $A$-Mod and $B$-Mod, we have two pairs of equivalent subcategories, giving a functorial decomposition of every module in its torsion and torsion free parts.

For an arbitrary $n \geq 0$, following Miyashita, we find that every classical $n$-tilting module $T$ gives rise to two sets of $n+1$ full subcategories of $A$-Mod and $B$-Mod, respectively, defined as follows for $e = 0, \ldots, n$:

$$\begin{aligned} KE_e(T) &= \left\{X \in A\text{-Mod} :\ \mathrm{Ext}^i_A(T, X) = 0 \text{ for every } i \neq e\right\} \subset A\text{-Mod} \\ KT^e(T) &= \left\{Y \in B\text{-Mod} :\ \mathrm{Tor}^B_i(T, Y) = 0 \text{ for every } i \neq e\right\} \subset B\text{-Mod} \end{aligned}$$

where conventionally $\mathrm{Ext}^0_A(T, X) = \mathrm{Hom}_A(T, X)$ and $\mathrm{Tor}^B_0(T, Y) = T \otimes_B Y$. As a generalisation of point $(ii)$ of Theorem 1, we may state the following result.

**Theorem 2** (Miyashita [14, Theorem 1.16]) *In the setting above, there are equivalences of (sub)categories, for every $e = 0, \dots, n$:*

$$KE_e(T) \underset{\mathrm{Tor}_e^B(T,?)}{\overset{\mathrm{Ext}_A^e(T,?)}{\rightleftarrows}} KT^e(T)\ .$$

For $n \geq 2$, however, the Miyashita classes do not provide a decomposition of every module, as it used to happen for $n = 1$. This is proved by the existence of simple modules (which can have only a trivial decomposition in the module category) not belonging to any class.

*Example 1* *(*[20, Example 2.1]*)* Let $k$ be an algebraically closed field. Let $A$ be the $k$-algebra associated to the quiver $1 \xrightarrow{a} 2 \xrightarrow{b} 3$ with the relation $b \circ a = 0$. The indecomposable projectives are $\begin{smallmatrix}1\\2\end{smallmatrix}$, $\begin{smallmatrix}2\\3\end{smallmatrix}$, $\begin{smallmatrix}3\end{smallmatrix}$, while the indecomposable injectives are $\begin{smallmatrix}1\end{smallmatrix}$, $\begin{smallmatrix}1\\2\end{smallmatrix}$, $\begin{smallmatrix}2\\3\end{smallmatrix}$. It follows that the module $T = \begin{smallmatrix}2\\3\end{smallmatrix} \oplus \begin{smallmatrix}1\\2\end{smallmatrix} \oplus \begin{smallmatrix}1\end{smallmatrix}$ is a classical 2-tilting module: a $p_2$) resolution is

$$P^\bullet \to T \to 0: \qquad 0 \longrightarrow 0 \oplus 0 \oplus \begin{smallmatrix}3\end{smallmatrix} \longrightarrow 0 \oplus 0 \oplus \begin{smallmatrix}2\\3\end{smallmatrix} \longrightarrow \begin{smallmatrix}2\\3\end{smallmatrix} \oplus \begin{smallmatrix}1\\2\end{smallmatrix} \oplus \begin{smallmatrix}1\\2\end{smallmatrix} \longrightarrow \begin{smallmatrix}2\\3\end{smallmatrix} \oplus \begin{smallmatrix}1\\2\end{smallmatrix} \oplus \begin{smallmatrix}1\end{smallmatrix} \longrightarrow 0\,;$$

$T$ is a direct sum of injectives, so it is rigid; lastly, $A = \begin{smallmatrix}3\end{smallmatrix} \oplus \begin{smallmatrix}2\\3\end{smallmatrix} \oplus \begin{smallmatrix}1\\2\end{smallmatrix}$ and so a $g_2$) co-resolution can be easily found. We shall show that the simple module $\begin{smallmatrix}2\end{smallmatrix}$ does not belong to any of the Miyashita classes.

In order to compute the $\mathrm{Ext}_A^i(T, \begin{smallmatrix}2\end{smallmatrix})$, we apply the contravariant functor $\mathrm{Hom}_A(?, \begin{smallmatrix}2\end{smallmatrix})$ to the resolution $P^\bullet$, obtaining

$$0 \longrightarrow \mathrm{Hom}_A(\begin{smallmatrix}2\\3\end{smallmatrix} \oplus \begin{smallmatrix}1\\2\end{smallmatrix} \oplus \begin{smallmatrix}1\\2\end{smallmatrix}, \begin{smallmatrix}2\end{smallmatrix}) \longrightarrow \mathrm{Hom}_A(0 \oplus 0 \oplus \begin{smallmatrix}2\\3\end{smallmatrix}, \begin{smallmatrix}2\end{smallmatrix}) \longrightarrow \mathrm{Hom}_A(0 \oplus 0 \oplus \begin{smallmatrix}3\end{smallmatrix}, \begin{smallmatrix}2\end{smallmatrix}) \longrightarrow 0$$

which is isomorphic to

$$0 \longrightarrow \mathrm{Hom}_A(\begin{smallmatrix}2\\3\end{smallmatrix}, \begin{smallmatrix}2\end{smallmatrix}) \xrightarrow{\ 0\ } \mathrm{Hom}_A(\begin{smallmatrix}2\\3\end{smallmatrix}, \begin{smallmatrix}2\end{smallmatrix}) \xrightarrow{\ 0\ } 0 \longrightarrow 0\ .$$

Hence, $\mathrm{Hom}_A(T, \begin{smallmatrix}2\end{smallmatrix}) \simeq \mathrm{Ext}_A^1(T, \begin{smallmatrix}2\end{smallmatrix}) \simeq \mathrm{Hom}_A(\begin{smallmatrix}2\\3\end{smallmatrix}, \begin{smallmatrix}2\end{smallmatrix}) \neq 0$ as abelian groups.

Indeed, those modules for which the $KE_i(T)$ (resp. the $KT^i(T)$) provide a decomposition can be characterised in the following way.

**Definition 2** A left $A$-module M (resp. a left $B$-module $N$) is *sequentially static* (resp. *costatic*) if for every $i \neq j \geq 0$,

$$\mathrm{Tor}_i^B(T, \mathrm{Ext}_A^j(T, M)) = 0 \quad (\text{resp. } \mathrm{Ext}_B^i(T, \mathrm{Tor}_j^A(T, N)) = 0).$$

Notice that for an $A$-module $M$ (resp. a $B$-module $N$) to be sequentially static (resp. costatic) means that for every $e = 0, \dots, n$, we have that $\mathrm{Ext}_A^e(T, M)$ belongs to $KT^e$ (resp. $\mathrm{Tor}_e^B(T, N)$ belongs to $KE_e$).

**Proposition 1** *([20, Theorem 2.3]) A left $A$-module $M$ is sequentially static if and only if there exists a filtration*

$$M = M_n \geq M_{n-1} \geq M_{n-2} \geq \cdots \geq M_0 \geq M_{-1} = 0$$

*such that for every $i = 0, \dots, n$, the quotient $M_i/M_{i-1}$ belongs to $KE_i(T)$. In this case, for every such $i$, we have that $M_i/M_{i-1} \simeq \operatorname{Tor}_i^B(T, \operatorname{Ext}_A^i(T, M))$.*

*Dually, a left $B$-module $M$ is sequentially costatic if and only if there exists a filtration*

$$N = N_{-1} \geq N_0 \geq N_1 \geq \cdots \geq N_{n-1} \geq N_n = 0$$

*such that for every $i = 0, \dots, n$, the quotient $N_{i-1}/N_i$ belongs to $KT^i(T)$. In this case, for every such $i$, we have that $N_{i-1}/N_i \simeq \operatorname{Ext}_A^i(T, \operatorname{Tor}_i^B(T, N))$.*

*Remark 1* In Example 1, the module $2$ was not sequentially static. Let us check that

$$\operatorname{Tor}_2^B(T, \operatorname{Hom}_A(T, 2)) \neq 0.$$

The ring $B = \operatorname{End}_A(T)$ (with multiplication the composition left to right) is the $k$-algebra associated to the quiver $4 \xrightarrow{c} 5 \xrightarrow{d} 6$ with the relation $d \circ c = 0$. In detail, the idempotents are the endomorphisms of $T$ induced by the identities of its direct summands, $e_4$ of $1$, $e_5$ of $\begin{smallmatrix}1\\2\end{smallmatrix}$ and $e_6$ of $\begin{smallmatrix}2\\3\end{smallmatrix}$, respectively; and $c$ and $d$ are the endomorphisms of $T$ induced by the morphisms $\begin{smallmatrix}1\\2\end{smallmatrix} \to 1$ and $\begin{smallmatrix}2\\3\end{smallmatrix} \to \begin{smallmatrix}1\\2\end{smallmatrix}$, respectively.

In order to compute the right $B$-module structure of $T$, we notice first that as a $k$-vector space $T$ is generated by five elements: $x \in \begin{smallmatrix}2\\3\end{smallmatrix} \setminus 3$ and $y = bx \in 3$, $v \in \begin{smallmatrix}1\\2\end{smallmatrix} \setminus 2$ and $w = av \in 2$, and $z \in 1$. If we look at how $B$ acts on the right on these elements, we see that $T$ as a right $B$-module is isomorphic to $\begin{smallmatrix}5\\4\end{smallmatrix} \oplus \begin{smallmatrix}6\\5\end{smallmatrix} \oplus 6 = \begin{smallmatrix}v\\z\end{smallmatrix} \oplus \begin{smallmatrix}x\\w\end{smallmatrix} \oplus y$.

To compute $\operatorname{Ext}_A^1(T, 2)$, we consider the injective coresolution of $2$ in $A$-Mod

$$0 \longrightarrow 2 \longrightarrow \begin{smallmatrix}1\\2\end{smallmatrix} \longrightarrow 1 \longrightarrow 0$$

and compute $\operatorname{coker}\left[\operatorname{Hom}_A(T, \begin{smallmatrix}1\\2\end{smallmatrix}) \to \operatorname{Hom}_A(T, 1)\right]$ as left $B$-modules.

The left $B$-module $\operatorname{Hom}_A\left(T, \begin{smallmatrix}1\\2\end{smallmatrix}\right)$ is generated as a $k$-vector space by (the morphisms induced on $T$ by) two morphisms $\begin{smallmatrix}2\\3\end{smallmatrix} \to \begin{smallmatrix}1\\2\end{smallmatrix}$ and $\begin{smallmatrix}1\\2\end{smallmatrix} \to \begin{smallmatrix}1\\2\end{smallmatrix}$. When we look at how $B$ acts on the left on these elements, we see that the module is isomorphic to ${}_B\left(\begin{smallmatrix}5\\6\end{smallmatrix}\right)$. Similarly, it can be seen that $\operatorname{Hom}_A(T, 1)$ as a left $B$-module is isomorphic to $\begin{smallmatrix}4\\5\end{smallmatrix}$, hence the cokernel we are interested in is the simple $4$. To compute $\operatorname{Tor}_2^B(T, 4)$, we now consider the presentation

$$0 \longrightarrow 5 \longrightarrow \begin{smallmatrix}4\\5\end{smallmatrix} \longrightarrow 4 \longrightarrow 0$$

where $\substack{4\\5}$ is a projective left $B$-module. It can be easily seen that $\mathrm{Tor}_2^B(T, 4) \simeq \mathrm{Tor}_1^B(T, 5)$. Take the injective coresolution of ${}_B 5$

$$0 \longrightarrow 6 \longrightarrow \substack{5\\6} \longrightarrow 5 \longrightarrow 0\ ;$$

similarly to what we did to compute $\mathrm{Ext}_A^1(T, 2)$, we can compute $\mathrm{Tor}_1^B(T, 5)$ as the kernel of $T \otimes_B 6 \to T \otimes_B \substack{5\\6}$ as a morphism of left $A$-modules.

If we call $t$ a generator of $6$, with the previous notation for the generators of $T_B$, as a $k$-vector space $T \otimes_B 6$ is generated by $v \otimes t, z \otimes t, x \otimes t, w \otimes t, y \otimes t$. Since however $e_6 t = t$, the only generators of these which are not zero are $x \otimes t = xe_6 \otimes t$ and $y \otimes t = ye_6 \otimes t$. If we look at the action of $A$ on the left of these elements, we deduce that $T \otimes_B 6$ is isomorphic to $\substack{2\\3}$ as a left $A$-module. Similarly, $T \otimes_B \substack{5\\6}$ turns out to be isomorphic to $2$, so in the end

$$\mathrm{Tor}_2^B(T, \mathrm{Hom}_A(T, 2)) \simeq 3 \neq 0.$$

## 3 First Attempts to Recover the Decomposition

In order to recover a decomposition of every module induced by a classical $n$-tilting module, different strategies have been proposed.

In [11], Jensen, Madsen and Su suggested a solution for the $n = 2$ case by enlarging the subcategories $KE_0, KE_1, KE_2$ in the following way. Let $\mathcal{K}_0$ be the full subcategory of cokernels of monomorphisms from objects in $KE_2$ to objects in $KE_0$; let $\mathcal{K}_1$ be $KE_1$; let $\mathcal{K}_2$ be the full subcategory of kernels of epimorphisms from objects in $KE_2$ to objects in $KE_0$:

$$\mathcal{K}_0 = \left\{ \operatorname{coker} f : X_2 \overset{f}{\hookrightarrow} X_0, \quad X_2 \in KE_2, X_0 \in KE_0 \right\}$$
$$\mathcal{K}_1 = KE_1$$
$$\mathcal{K}_2 = \left\{ \ker g : X_2 \overset{g}{\twoheadrightarrow} X_0, \quad X_2 \in KE_2, X_0 \in KE_0 \right\}.$$

By considering the morphisms $f : 0 \hookrightarrow X_0$ and $g : X_2 \twoheadrightarrow 0$, we can see that $KE_i \subset \mathcal{K}_i$ for every $i = 0, 1, 2$, so this is indeed an enlargement.

Now, for $i = 0, 1, 2$, let $\mathcal{E}_i$ be the extension closure of $\mathcal{K}_i$, i.e. the smallest subcategory containing $\mathcal{K}_i$ and closed under extensions.

**Proposition 2** ([*11*, *Corollary 15, Theorem 19, Lemma 24*]) *For any left $A$-module $X$, there exists a unique filtration*

$$0 = X_0 \subseteq X_1 \subseteq X_2 \subseteq X_3 = X$$

*with the quotients* $X_{i+1}/X_i \in \mathcal{E}_i$ *for every* $i = 0, 1, 2$. *Moreover, such a filtration is functorial.*

*Example 2* Let us apply this construction to find a decomposition of the simple module $2$ considered in the Example 1. In a way similar to that used to study the $\mathrm{Ext}^i_A(T, 2), i = 0, 1, 2$, we may prove that $\frac{2}{3}$ belongs to $KE_0$ and $3$ belongs to $KE_2$. Then, $2$ belongs to $\mathcal{K}_0 \subseteq \mathcal{E}_0$, being the cokernel of the monomorphism $3 \to \frac{2}{3}$. Therefore, the trivial filtration $0 \leq 2$ has its only filtration factor in the new class $\mathcal{E}_0$.

In [13], Lo generalised this filtration to the $n > 2$ case as well. After giving a different proof of Proposition 2, he introduced the following subcategories. For a class of objects $\mathcal{S}$, denote by $[\mathcal{S}]$ the extension closure of the full subcategory of quotients of objects of $\mathcal{S}$:

$$[\mathcal{S}] = \langle \{X : \exists (S \twoheadrightarrow X) \text{ for some } S \in \mathcal{S}\}\rangle_{\text{ext}}.$$

This subcategory is closed under quotients ([13, Lemma 5.1]). Then set, for $i = 0, \ldots, n$:

$$\mathcal{T}_i = \left[\mathrm{Ker}\,\mathrm{Ext}^i_A(T, ?) \cap \cdots \cap \mathrm{Ker}\,\mathrm{Ext}^n_A(T, ?)\right]$$
$$\mathcal{F}_i = \mathrm{Ker}\,\mathrm{Hom}_A(\mathcal{T}_i, ?) = \{X : \mathrm{Hom}_A(\mathcal{T}_i, X) = 0\}$$

with our usual convention that $\mathrm{Ext}^0_A = \mathrm{Hom}_A$. Define also $\mathcal{T}_{n+1} = A$-Mod and $\mathcal{F}_{n+1} = 0$.

This provides pairs $(\mathcal{T}_i, \mathcal{F}_i)$ of full subcategories, which are torsion pairs since the $\mathcal{T}_i$'s are closed under extensions and quotients (see Polishchuk [16]). The following easy proposition can then be applied to these torsion pairs.

**Proposition 3** ([13, Theorem 5.3]) *Let* $(\mathcal{T}_i, \mathcal{F}_i)$ *be torsion pairs in* $A$*-Mod, for* $i = 0, \ldots, n+1$, *such that*

$$0 = \mathcal{T}_0 \subseteq \mathcal{T}_1 \subseteq \cdots \subseteq \mathcal{T}_{n+1} = A\text{-}Mod.$$

*Then for every left* $A$*-module* $X$*, there exists a functorial filtration*

$$0 = X_0 \subseteq X_1 \subseteq \cdots \subseteq X_{n+1} = X$$

*such that* $X_i \in \mathcal{T}_i$ *for* $i = 0, \ldots, n+1$ *and* $X_i/X_{i-1} \in \mathcal{T}_i \cap \mathcal{F}_{i-1}$ *for* $i=1, \ldots, n+1$. *Moreover, the* $\mathcal{T}_i \cap \mathcal{F}_{i-1}$ *have pairwise trivial intersection.*

We now prove that the subcategories $\mathcal{T}_i \cap \mathcal{F}_{i-1}$ introduced by Lo are indeed enlargements of the Miyashita classes using the following generalisation of [3, Lemma 3.2], which we find of independent interest.

**Lemma 1** *Let $X$ be a module belonging to $\cap_{i>e} \operatorname{Ker} \operatorname{Ext}_A^i(T, X)$ for some $0 \leq e \leq n$. Then, there exists a sequence of direct summands of coproducts of copies of $T$,*

$$\cdots \longrightarrow T_{-1} \xrightarrow{d_{-1}} T_0 \xrightarrow{d_0} \cdots \longrightarrow T_e \longrightarrow 0$$

*which is exactly everywhere except for degree 0, and having* $\ker d_0 / \operatorname{im} d_{-1} \simeq X$*. In particular, for $e = n$, $\cap_{i>n} \operatorname{Ker} \operatorname{Ext}_A^i(T, X) = A$-Mod and hence $X$ may be any module.*

*Proof* Set $T^{\perp_\infty} := \cap_{i>0} \operatorname{Ker} \operatorname{Ext}^i(T, ?)$ and, for a family of modules $\mathcal{S}$, ${}^{\perp}\mathcal{S} := \operatorname{Ker} \operatorname{Ext}^1(?, \mathcal{S})$. It is well known (see [9], after Definition 5.1.1) that the pair of subcategories $({}^{\perp}(T^{\perp_\infty}), T^{\perp_\infty})$ is a complete hereditary cotorsion pair. This means (see [9, Lemma 2.2.6]) that $X$ (as any other module) admits a special ${}^{\perp}(T^{\perp_\infty})$-precover

$$0 \longrightarrow J \longrightarrow K \longrightarrow X \longrightarrow 0\ .$$

In particular, $J$ belongs to $({}^{\perp}(T^{\perp_\infty}))^{\perp}$, which equals $T^{\perp_\infty}$ by definition of cotorsion pair. Now we can apply [3, Lemma 3.2] to $J$ and [9, Proposition 5.1.9] to $K$ in order to construct a sequence of direct summands of coproducts of copies of $T$

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & T_{-2} & \longrightarrow & T_{-1} & \overset{d_{-1}}{\dashrightarrow} & T_0 & \xrightarrow{d_0} & \cdots & \longrightarrow & T_n & \longrightarrow 0 \\
& & & \downarrow & & \uparrow & & & & & \\
& & & J & \hookrightarrow & K & \overset{\pi}{\twoheadrightarrow} & X & & &
\end{array} \qquad (*)$$

By construction, the first row is a sequence which is exact everywhere except for degree 0, where $\ker d_0 / \operatorname{im} d_{-1} \simeq K/J \simeq X$.

This concludes the proof for the case where $e = n$. Otherwise, it can be easily proved that since by hypothesis $\operatorname{Ext}_A^i(T, X) = 0$ for $i > e$, then for these indices $T_i = 0$: let us show it for $i = n$, then the other cases follow similarly. First, notice that since $\operatorname{Ext}_A^j(T, J) = 0$, one gets $\operatorname{Ext}_A^j(T, K) = \operatorname{Ext}_A^j(T, X)$ for every $j > 0$. Then, if we call $K_j = \ker d_j$ for $j \geq 0$, we have

$$\operatorname{Ext}_A^1(T, K_{n-1}) \cong \operatorname{Ext}_A^n(T, K_0) = \operatorname{Ext}_A^n(T, X) = 0;$$

applying the functor $\operatorname{Hom}_A(T, ?)$ to the short exact sequence

$$0 \to K_{n-1} \to T_{n-1} \to K_n = T_n \to 0$$

we get that $\operatorname{Hom}_A(T, T_{n-1}) \to \operatorname{Hom}_A(T, T_n)$ is an epimorphism and hence all morphisms $T \to T_n$ factorise through $T_{n-1}$. Using the universal property of the coproduct of which $T_n$ is a direct summand, it is easy to prove that this implies that

$0 \to K_{n-1} \to T_{n-1} \to T_n \to 0$ splits. Thus $K_{n-1}$ is a direct summand of a coproduct of copies of $T$. Therefore, we may truncate the sequence $(*)$ as

$$\cdots \longrightarrow T_{n-3} \longrightarrow T_{n-2} \longrightarrow K_{n-1} \longrightarrow 0\ .$$

Notice that this lemma generalises [3, Lemma 3.2], which is the case where $e = 0$.

*Remark 2* We shall prove that $KE_e \subseteq \mathcal{T}_{e+1} \cap \mathcal{F}_e$ for every $e = 0, \ldots, n$. Indeed, it is obvious that $KE_e \subseteq \mathcal{T}_{e+1}$. To see that any $M \in KE_e$ belongs to $\mathcal{F}_e$ as well, we will proceed in subsequent steps.

First, we prove that for every $X \in \bigcap_{i>e-1} \operatorname{Ker}\operatorname{Ext}^i_A(T, ?) \subseteq \mathcal{T}_e$, there are no non zero morphisms $X \to M$. Indeed, if $e = 0$, then $X = 0$; if $e > 0$, consider the sequence

$$T^\bullet := \ \cdots \longrightarrow T_{-1} \xrightarrow{d_{-1}} T_0 \xrightarrow{d_0} \cdots \longrightarrow T_{e-1} \longrightarrow 0$$

given by Lemma 1 applied to $X$. Set $K_j = \ker d_j$ for $j \geq 0$ (and so $K_0 = K$), applying the functor $\operatorname{Hom}(-, M)$ to the epimorphism $K_0 \to X$, one gets

$$\operatorname{Hom}_A(X, M) \hookrightarrow \operatorname{Hom}_A(K_0, M) \cong \operatorname{Ext}^1_A(K_1, M) \cong \cdots$$

$$\cdots \cong \operatorname{Ext}^{e-1}_A(K_{e-1}, M) = \operatorname{Ext}^{e-1}_A(T_{e-1}, M) = 0,$$

and hence $\operatorname{Hom}_A(X, M) = 0$.

Now, if $X'$ is the epimorphic image of some $X \in \bigcap_{i>e-1} \operatorname{Ker}\operatorname{Ext}^i_A(T, ?)$, we have $\operatorname{Hom}_A(X', M) \hookrightarrow \operatorname{Hom}_A(X, M) = 0$ so $\operatorname{Hom}_A(X', M) = 0$ as well. Lastly, if $X''$ is an extension of such epimorphic images, we still find that $\operatorname{Hom}_A(X'', M) = 0$.

This proves the claim that $M$ has no non zero morphisms from objects of $\mathcal{T}_e$, and therefore it belongs to $\mathcal{F}_e$.

The last result of [13] is the proof that for $n = 2$, the filtration procedure of Proposition 3 reduces to that provided by Jensen, Madsen, and Su.

It should be noted that these results, while providing a way to generalise the decomposition of every module found in the $n = 1$ case, do so by introducing enlargements of the Miyashita classes $KE_i$ which are not very natural, at the point that the connection to the tilting object they originate from seems a bit weak.

The rest of the article is devoted to the description of an alternative approach to this enlarging strategy, introduced in [8], which takes place in the derived category $\mathcal{D}(A)$ of $A$-Mod. In the following section, we recall some basic facts about derived categories and $t$-structures.

## 4 Introducing Derived Categories and $t$-structures

Given an abelian category $\mathcal{A}$, one may construct its derived category $\mathcal{D}(\mathcal{A})$ defining objects and morphisms in the following way. As objects, one takes the cochain complexes with terms in $\mathcal{A}$:

$$\cdots \longrightarrow X^n \xrightarrow{d_X^n} X^{n+1} \xrightarrow{d_X^{n+1}} X^{n+2} \longrightarrow \cdots$$

In order to define morphisms, one first takes the quotient of morphisms of complexes modulo those satisfying the *nullohomotopy* condition; the category having these equivalence classes as morphisms is called the *homotopy category*. The step from this to the derived category is performed by an argument of *localisation*; in this way, morphisms of complexes which induce isomorphisms on the cohomologies get an inverse in the derived category.

The category $\mathcal{D}(\mathcal{A})$ so obtained is not abelian anymore, but it is a *triangulated category*. This means that it is equipped with the following structure. First, there is an autoequivalence, whose action on the complex $X^\bullet$ is denoted as $X^\bullet[1]$ and is defined as follows:

$$(X^\bullet[1])^n = X^{n+1} \qquad d^n_{X[1]} = -d_X^{n+1}.$$

This functor is called the *suspension functor*; its natural definition on chain morphisms induces a good definition on morphisms in $\mathcal{D}(\mathcal{A})$. We will sometimes denote this functor also as $\Sigma$; its inverse as $\Sigma^{-1}$ or $?[-1]$; their powers as $\Sigma^i$ or $?[i]$ for $i \in \mathbb{Z}$.

Given this autoequivalence, one calls *triangles* the diagrams of the form

$$X^\bullet \xrightarrow{u} Y^\bullet \xrightarrow{v} Z^\bullet \xrightarrow{w} X[1]$$

such that $v \circ u = 0 = w \circ v$; in $\mathcal{D}(\mathcal{A})$, a particular role is played by the triangles isomorphic (as diagrams) to those of the form

$$X^\bullet \xrightarrow{f} Y^\bullet \longrightarrow \mathrm{Cone}\, f \longrightarrow X[1]$$

where Cone $f$ is defined as the complex having terms $(\mathrm{Cone}\, f)^i = X^{i+1} \oplus Y^i$ and differentials $d^i_{\mathrm{Cone}\, f} = \begin{bmatrix} -d_X^{i+1} & 0 \\ f^{i+1} & d_Y^i \end{bmatrix}$. These triangles are called *distinguished triangles* and are the analogous of short exact sequences in abelian categories.

In a triangulated category, hence also in $\mathcal{D}(\mathcal{A})$, products and coproducts of distinguished triangles, when they exist, are distinguished (see [15, Proposition 1.2.1, and its dual]). In particular, if $\mathcal{A}$ has arbitrary products or coproducts, $\mathcal{D}(\mathcal{A})$ has them as well: they are constructed degree-wise using those of $\mathcal{A}$.

Once we have set our context, we now define the main object which we will work with.

**Definition 3** Let $\mathcal{S} = (\mathcal{S}^{\leq 0}, \mathcal{S}^{\geq 0})$ be a pair of full, strict (i.e. closed under isomorphisms) subcategories of $\mathcal{D}(\mathcal{A})$, and denote $\mathcal{S}^{\leq i} = \mathcal{S}^{\leq 0}[-i]$ and $\mathcal{S}^{\geq i} = \mathcal{S}^{\geq 0}[-i]$, for every $i \in \mathbb{Z}$.

The pair $\mathcal{S}$ is a *t-structure* if it satisfies the following properties:

T1) $\mathcal{S}^{\leq 0} \subseteq \mathcal{S}^{\leq 1}$ and $\mathcal{S}^{\geq 0} \supseteq \mathcal{S}^{\geq 1}$;
T2) $\mathrm{Hom}_{\mathcal{D}(\mathcal{A})}(\mathcal{S}^{\leq 0}, \mathcal{S}^{\geq 1}) = 0$;
T3) For any complex $X^\bullet$ in $\mathcal{D}(\mathcal{A})$, there exist complexes $A^\bullet \in \mathcal{S}^{\leq 0}$ and $B^\bullet \in \mathcal{S}^{\geq 1}$ and morphisms such that

$$A^\bullet \longrightarrow X^\bullet \longrightarrow B^\bullet \longrightarrow A^\bullet[1]$$

is a distinguished triangle in $\mathcal{D}(\mathcal{A})$. This is called an *approximating triangle* of $X^\bullet$.

In this case, $\mathcal{S}^{\leq 0}$ is called an *aisle*, $\mathcal{S}^{\geq 0}$ a *coaisle*. The $t$-structure $\mathcal{S}$ is called *non degenerate* if $\bigcap_{i\in\mathbb{Z}} \mathcal{S}^{\leq i} = 0$ (or equivalently $\bigcap_{i\in\mathbb{Z}} \mathcal{S}^{\geq i} = 0$). The full subcategory $\mathcal{H}_\mathcal{S} = \mathcal{S}^{\leq 0} \cap \mathcal{S}^{\geq 0}$ is called the *heart* of $\mathcal{S}$.

This definition immediately resembles that of a torsion pair in an abelian category. As it holds for torsion pairs, the approximating triangle of a complex with respect to a $t$-structure is functorial, as we are going to state.

Given a $t$-structure $\mathcal{S}$ in $\mathcal{D}(\mathcal{A})$, it can be proved that the embeddings of subcategories $\mathcal{S}^{\leq 0} \subseteq \mathcal{D}(\mathcal{A})$ and $\mathcal{S}^{\geq 0} \subseteq \mathcal{D}(\mathcal{A})$ have a right adjoint $\sigma^{\leq 0} : \mathcal{D}(\mathcal{A}) \to \mathcal{S}^{\leq 0}$ and a left adjoint $\sigma^{\geq 0} : \mathcal{D}(\mathcal{A}) \to \mathcal{S}^{\geq 0}$, respectively.

For $i \in \mathbb{Z}$, let us write $\sigma^{\leq i} = \Sigma^{-i} \circ \sigma^{\leq 0} \circ \Sigma^{i} : \mathcal{D}(\mathcal{A}) \to \mathcal{S}^{\leq i}$ and similarly $\sigma^{\geq i} = \Sigma^{-i} \circ \sigma^{\geq 0} \circ \Sigma^{i} : \mathcal{D}(\mathcal{A}) \to \mathcal{S}^{\geq i}$; $\sigma^{\leq i}$ and $\sigma^{\geq i}$ will be called, respectively, the left and the right *truncation functors at* $i$ with respect to $\mathcal{S}$, for $i \in \mathbb{Z}$.

It can be proved that for every $X^\bullet$ in $\mathcal{D}(\mathcal{A})$, the approximation triangle for $X^\bullet$ provided by the definition of the $t$-structure $\mathcal{S}$ is precisely (isomorphic to):

$$\sigma^{\leq 0}(X^\bullet) \longrightarrow X^\bullet \longrightarrow \sigma^{\geq 1}(X^\bullet) \longrightarrow (\sigma^{\leq 0}(X^\bullet))[1] \ .$$

The truncation functors of $\mathcal{S}$ can be used to define the *$i$-th cohomology* with respect to $\mathcal{S}$. It can be proved that for every $i, j \in \mathbb{Z}$, there is a canonical natural isomorphism $\sigma^{\leq i}\sigma^{\geq j} \simeq \sigma^{\geq j}\sigma^{\leq i}$. Then, for every $i \in \mathbb{Z}$, the functor $H^i_\mathcal{S} = \Sigma^i\sigma^{\leq i}\sigma^{\geq i} \simeq \Sigma^i\sigma^{\geq i}\sigma^{\leq i} : \mathcal{D}(\mathcal{A}) \to \mathcal{H}_\mathcal{S}$ is called the $i$-th *cohomology functor* with respect to the $t$-structure $\mathcal{S}$ (or simply *$\mathcal{S}$-cohomology*).

We introduce now the first $t$-structure in $\mathcal{D}(\mathcal{A})$ we are going to use.

**Definition 4** The *natural* $t$-structure $\mathcal{D}$ of $\mathcal{D}(\mathcal{A})$ has aisle and coaisle:

$$\mathcal{D}^{\leq 0} = \left\{X^\bullet \in \mathcal{D}(\mathcal{A}) : \ H^i(X^\bullet) = 0 \text{ for every } i > 0\right\}$$
$$\mathcal{D}^{\geq 0} = \left\{X^\bullet \in \mathcal{D}(\mathcal{A}) : \ H^i(X^\bullet) = 0 \text{ for every } i < 0\right\}.$$

Notice that by construction, the $i$th $\mathcal{D}$-cohomology of $X^\bullet$ is a complex having zero cohomology everywhere except for degree 0, where it has $H^i(X^\bullet)$, the usual $i$-th cohomology of $X^\bullet$: i.e., $H^i_{\mathcal{D}}(X^\bullet) = H^i(X^\bullet)[0]$.

The original proof that this is indeed a $t$-structure can be found in [5].

We now state the following fundamental theorem about $t$-structures. One may read it with our example $\mathcal{D}$ in mind.

**Theorem 3** *Let $\mathcal{S}$ be a non degenerate $t$-structure in $\mathcal{D}(\mathcal{A})$. Then*

1. *The heart $\mathcal{H}_{\mathcal{S}}$ is an abelian category; moreover, a short sequence*

$$0 \longrightarrow X^\bullet \longrightarrow Y^\bullet \longrightarrow Z^\bullet \longrightarrow 0$$

*in $\mathcal{H}_{\mathcal{S}}$ is exact if and only if there exists a morphism $Z \to X[1]$ in $\mathcal{D}(\mathcal{A})$ such that the triangle*

$$X^\bullet \longrightarrow Y^\bullet \longrightarrow Z^\bullet \longrightarrow X^\bullet[1]$$

*is distinguished.*

2. *Given any distinguished triangle*

$$X^\bullet \longrightarrow Y^\bullet \longrightarrow Z^\bullet \longrightarrow X^\bullet[1]$$

*in $\mathcal{D}(\mathcal{A})$, there is a long exact sequence in $\mathcal{H}_{\mathcal{S}}$*

$$\cdots \longrightarrow H^{i-1}_{\mathcal{S}} Z^\bullet \longrightarrow H^i_{\mathcal{S}} X^\bullet \longrightarrow H^i_{\mathcal{S}} Y^\bullet \longrightarrow H^i_{\mathcal{S}} Z^\bullet \longrightarrow H^{i+1}_{\mathcal{S}} \longrightarrow \cdots$$

As can be easily seen, the heart $\mathcal{H}_{\mathcal{D}}$ of the natural $t$-structure of $\mathcal{D}(\mathcal{A})$ is (equivalent to) $\mathcal{A}$ itself via the embedding $\mathcal{A} \to \mathcal{D}(\mathcal{A})$ defined by

$$X \mapsto X[0] = (\cdots \longrightarrow 0 \longrightarrow X \longrightarrow 0 \longrightarrow \cdots)$$

whose quasi-inverse is $H^0$, the usual 0th-cohomology functor.

As it happens for torsion pairs, the aisle or the coaisle of a $t$-structure is sufficient to characterise the whole $t$-structure. Indeed, we give the following lemma by Keller and Vossieck [12].

**Lemma 2** *Let $\mathcal{R} = (\mathcal{R}^{\leq 0}, \mathcal{R}^{\geq 0})$ be a $t$-structure in $\mathcal{D}(\mathcal{A})$. Then*

$$\mathcal{R}^{\leq 0} = \left\{X^\bullet \in \mathcal{D}(\mathcal{A}) : \operatorname{Hom}_{\mathcal{D}(\mathcal{A})}(X^\bullet, Y^\bullet) = 0 \text{ for all } Y^\bullet \in \mathcal{R}^{\geq 1}\right\}$$
$$\mathcal{R}^{\geq 0} = \left\{Y^\bullet \in \mathcal{D}(\mathcal{A}) : \operatorname{Hom}_{\mathcal{D}(\mathcal{A})}(X^\bullet, Y^\bullet) = 0 \text{ for all } X^\bullet \in \mathcal{R}^{\leq -1}\right\}.$$

We now give the following proposition, which gives a very useful way to construct $t$-structures in the derived category of a Grothendieck category $\mathcal{G}$.

**Proposition 4** *([1, Lemma 3.1, Theorem 3.4]) Let $\mathcal{G}$ be a Grothendieck category. Given any complex $E$ in $\mathcal{D}(\mathcal{G})$, let $\mathcal{U}$ be the smallest* cocomplete pre-aisle *contain-*

*ing E, that is, the smallest full, strict subcategory of $\mathcal{D}(\mathcal{G})$ closed under positive shifts, extensions and coproducts. Then, $\mathcal{U}$ is an aisle and the corresponding coaisle is*

$$\begin{aligned}\mathcal{U}^{\perp} &= \left\{Y^{\bullet} \in \mathcal{D}(\mathcal{G}) : \operatorname{Hom}_{\mathcal{D}(\mathcal{G})}(X^{\bullet}, Y^{\bullet}) = 0 \textit{ for every } X^{\bullet} \in \mathcal{U}[1]\right\} \\ &= \left\{Y^{\bullet} \in \mathcal{D}(\mathcal{G}) : \operatorname{Hom}_{\mathcal{D}(\mathcal{G})}(E, Y^{\bullet}[i]) = 0 \textit{ for every } i < 0\right\}.\end{aligned}$$

*Remark 3* As a first application of this proposition, it is easy to see that if $\mathcal{G}$ has a projective generator $E$, then the natural $t$-structure of $\mathcal{D}(\mathcal{G})$ will be that generated by $E$ (in the sense of the proposition). This will be the case when we will consider $\mathcal{G} = A$-Mod, with $E = A$.

*Remark 4* In the case where the object $E$ is in fact a module, that is, a complex concentrated in degree zero, we shall give a characterisation of the aisle $\mathcal{U}$ generated by $E$.

First, $\mathcal{U}$ contains $E$; and it is closed under positive shifts, hence it contains $E[i]$ for every $i > 0$. $\mathcal{U}$ is closed under arbitrary coproducts; let then $J = \cup_{i>0} J_i$ be a set of indices, and let $E_j = E[i]$ for every $j \in J_i$. Then the coproduct $\coprod_{j\in J} E_j = \coprod_{i>0} E^{(J_i)}[i]$ belongs to $\mathcal{U}$ as well. If $\mathcal{V}$ is the full subcategory of all objects isomorphic to these coproducts, this means that $\mathcal{V} \subseteq \mathcal{U}$. Since $\mathcal{U}$ is also closed under extensions, if we call $\mathcal{V}'$ the extension closure of $\mathcal{V}$, we have $\mathcal{V}' \subseteq \mathcal{U}$ as well. Moreover, since coproducts of distinguished triangles are distinguished, from the fact that $\mathcal{V}$ is closed under arbitrary coproducts follows easily that $\mathcal{V}'$ is as well. Hence, $\mathcal{V}'$ is a cocomplete pre-aisle, and by definition $\mathcal{U} \subseteq \mathcal{V}'$.

In conclusion, objects of $\mathcal{U}$ are isomorphic to complexes having zero terms in positive degrees and coproducts of $E$ in nonpositive degrees.

## 5 $n$-Tilting Objects and Associated $t$-structures

In the following, we are going to work with a generalisation of classical $n$-tilting modules, introduced by Angeleri Hügel and Coelho [2]; the equivalent definition we give is more oriented towards the derived category $\mathcal{D}(A)$ of $A$-Mod, which will be our setting.

**Definition 5** A left $A$-module $T$ is (non necessarily classical) *$n$-tilting* if it satisfies the following properties:

$P_n$) $T$ has projective dimensions at most $n$, i.e. there exists an exact sequence

$$0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow T \longrightarrow 0$$

in $A$-Mod with the $P_i$ projectives;

$E_n$) $T$ is rigid, i.e. $\operatorname{Ext}^i_A(T, T^{(\Lambda)}) = 0$ for every index $0 < i \leq n$ and set $\Lambda$;

$G_n$) $T$ is a *generator* in $\mathcal{D}(A)$, meaning that if for a complex $X^{\bullet}$ we have $\operatorname{Hom}_{\mathcal{D}(A)}(T, X[i]) = 0$ for every $i \in \mathbb{Z}$, then $X^{\bullet} = 0$ in $\mathcal{D}(A)$.

Notice that a classical $n$-tilting module is indeed $n$-tilting: in particular, $p_n$) implies $P_n$), $p_n$) and $e_n$) imply $E_n$) (see the Stacks Project [19, Proposition 15.72.3] and $g_n$) implies $G_n$) (see Positselski and Stovicek [17, Corollary 2.6]).

The discussion about $t$-structures in the previous section is justified by the following construction. Let $T$ be a $n$-tilting left $A$-module and consider the pair $\mathcal{T} = (\mathcal{T}^{\leq 0}, \mathcal{T}^{\geq 0})$ of subcategories of $\mathcal{D}(A)$

$$\mathcal{T}^{\leq 0} = \left\{X^\bullet \in \mathcal{D}(A) : \operatorname{Hom}_{\mathcal{D}(A)}(T, X^\bullet[i]) = 0 \text{ for every } i > 0\right\}$$
$$\mathcal{T}^{\geq 0} = \left\{X^\bullet \in \mathcal{D}(A) : \operatorname{Hom}_{\mathcal{D}(A)}(T, X^\bullet[i]) = 0 \text{ for every } i < 0\right\}.$$

*Remark 5* This is the $t$-structure generated by $T$ in the sense of Proposition 4, as proved in [4, Lemma 3.4], which in turn follows [18, Lemma 4.4]. We provide here another proof.

Let $\mathcal{G} = (\mathcal{G}^{\leq 0}, \mathcal{G}^{\geq 0})$ be the generated $t$-structure. We have $\mathcal{T}^{\geq 0} = \mathcal{G}^{\geq 0}$. For the aisle, notice that $\mathcal{T}^{\leq 0}$ contains $T$ by $(E_n)$; and it is clearly closed under positive shifts, hence it contains any $T[i]$ for $i > 0$. Now, we show that it is closed under arbitrary coproducts of such complexes $T[i]$. Let $J = \cup_{i>0} J_i$ be a set, let $T_j = T[i]$ for every $j \in J_i$, and consider the coproduct $\coprod_{j \in J} T_j = \coprod_{i>0} T^{(J_i)}[i]$. Notice that since by $(P_n)$ $T$ has projective dimension $n$, we have

$$\operatorname{Hom}_{\mathcal{D}(A)}\left(T, \coprod_{j \in J} T_j\right) = \operatorname{Hom}_{\mathcal{D}(A)}\left(T, \coprod_{i>0} T^{(J_i)}[i]\right) = \operatorname{Hom}_{\mathcal{D}(A)}\left(T, \coprod_{1 \leq i \leq n} T^{(J_i)}[i]\right).$$

Now, since $\mathcal{D}(A)$ is an additive category, this is itself isomorphic to

$$\operatorname{Hom}_{\mathcal{D}(A)}\left(T, \prod_{1 \leq i \leq n} T^{(J_i)}[i]\right) \simeq \prod_{1 \leq i \leq n} \operatorname{Hom}_{\mathcal{D}(A)}\left(T, T^{(J_i)}[i]\right) = 0$$

which is zero by property $(E_n)$. Lastly, $\mathcal{T}^{\leq 0}$ is clearly closed under extensions, and so by Remark 4, it contains $\mathcal{G}^{\leq 0}$.

For the inclusion $\mathcal{T}^{\leq 0} \subseteq \mathcal{G}^{\leq 0}$, take an object $X^\bullet \in \mathcal{T}^{\leq 0}$ and consider its approximation triangle with respect to $\mathcal{G}$,

$$A^\bullet \longrightarrow X^\bullet \longrightarrow B^\bullet \xrightarrow{+1} .$$

We have $A^\bullet \in \mathcal{G}^{\leq 0} \subseteq \mathcal{T}^{\leq 0}$; and since $\mathcal{T}^{\leq 0}$ is clearly closed under cones, $B^\bullet \in \mathcal{T}^{\leq 0}$ as well. So in the end $B^\bullet \in \mathcal{T}^{\leq 0} \cap \mathcal{G}^{\geq 1} = \mathcal{T}^{\leq 0} \cap \mathcal{T}^{\geq 1}$ which is 0 by $G_3$).

As a side note, observe that if $T$ is classical $n$-tilting, it induces a triangulated equivalence $R\operatorname{Hom}_A(T, ?) : \mathcal{D}(A) \to \mathcal{D}(B)$ (see [7]); then, by the fact that

$$\operatorname{Hom}_{\mathcal{D}(A)}(T, X^\bullet[i]) = H^i R\operatorname{Hom}_A(T, X^\bullet)$$

we may recognise in $\mathcal{T} := (\mathcal{T}^{\leq 0}, \mathcal{T}^{\geq 0})$ the "pullback" of the natural $t$-structure of $\mathcal{D}(B)$ along $R\operatorname{Hom}_A(T, ?)$.

*Remark 6* Without further study, the $t$-structure $\mathcal{T}$ can be immediately used to review some previous results.

First, we can greatly simplify the proof of Remark 2. In the notation used there, to prove that there are no non zero morphisms $X \to M$, for $X$ in $\cap_{i>e-1} \operatorname{Ker}\operatorname{Ext}^i_A(T, ?)$ and $M$ in $KE_e$, we may just recognise that we have $X = X[0] \in \mathcal{T}^{\leq e-1}$ and $M \in \mathcal{T}^{\geq e}$, and use axiom (T2) of $t$-structures.

Second, we may read our Lemma 1 under a different light: given the characterisation of objects in $\mathcal{T}^{\leq 0}$ as in Remark 4, the lemma can be seen to be the equality

$$\cap_{i>e} \operatorname{Ker}\operatorname{Ext}^i_A(T, ?) = A\text{-Mod} \cap \mathcal{T}^{\leq e}.$$

In the following, $T$ will be a $n$-tilting module; $\mathcal{T}$ will be the associated $t$-structure, as defined above. The solution that we are going to give to our decomposition problem originates from the interaction of the $t$-structure $\mathcal{T}$ with the natural $t$-structure $\mathcal{D}$ of $\mathcal{D}(A)$ (see Definition 4). First, we make an easy observation.

**Proposition 5** *The following inclusions of aisles and coaisles hold:*

$$\mathcal{D}^{\leq -n} \subseteq \mathcal{T}^{\leq 0} \subseteq \mathcal{D}^{\leq 0} \quad \textit{and} \quad \mathcal{D}^{\geq 0} \subseteq \mathcal{T}^{\geq 0} \subseteq \mathcal{D}^{\geq -n}.$$

*Proof* Some of the inclusions are easy to prove: if $X^\bullet \in \mathcal{D}^{\leq -n}$, then for every $i > 0$ we will have $X^\bullet[i] \in \mathcal{D}^{\leq -n-i} \subseteq \mathcal{D}^{\leq -n-1}$, hence $\operatorname{Hom}_{\mathcal{D}(A)}(T, X^\bullet[i]) = 0$ since $T$ has projective dimension $n$. On the other hand, if $X^\bullet \in \mathcal{D}^{\geq 0}$, then for every $i < 0$ we will have $X^\bullet[i] \in \mathcal{D}^{\geq 0-i} \subseteq \mathcal{D}^{\geq 1}$, hence again $\operatorname{Hom}_{\mathcal{D}(A)}(T, X^\bullet[i]) = 0$ since $T \in \mathcal{D}^{\leq 0}$. The other two inclusions can be easily proved from these using Lemma 2.

*Remark 7* With Proposition 5, we are ready to notice an important fact, which will be key later. Take a module $X$ in $KE_e$, for some $e = 0, \ldots, n$; in particular, being a module, it belongs to $A\text{-Mod} \simeq \mathcal{H}_\mathcal{D} \subseteq \mathcal{D}^{\geq 0} \subseteq \mathcal{T}^{\geq 0}$. Moreover, by definition, for every $i = 0, \ldots, e-1$, we have $0 = \operatorname{Ext}^i_A(T, X) \simeq \operatorname{Hom}_{\mathcal{D}(A)}(T, X[i])$, hence $X$ belongs in fact to $\mathcal{T}^{\geq e}$. Lastly, again by definition, for every $i > e$, we have $0 = \operatorname{Ext}^i_A(T, X) \simeq \operatorname{Hom}_{\mathcal{D}(A)}(T, X[i])$, hence $X$ belongs to $\mathcal{T}^{\leq e}$ as well.

This proves that, after identifying $A\text{-Mod} \simeq \mathcal{H}_\mathcal{D}$, for every $e = 0, \ldots, n$ the $e$-th Miyashita class is

$$KE_e = A\text{-Mod} \cap \mathcal{H}_\mathcal{T}[-e].$$

Let us now look at Proposition 5 in the $n = 1$ case. Its proof suggests that we may focus on the inclusions between the aisles (those between the coaisles being their "dual" in the sense of Lemma 2). If $T$ is a 1-tilting module, we will then have

$$\mathcal{D}^{\leq -1} \subseteq \mathcal{T}^{\leq 0} \subseteq \mathcal{D}^{\leq 0}. \tag{$*$}$$

In other words, complexes in $\mathcal{T}^{\leq 0}$ are allowed to have any cohomology (with respect to $\mathcal{D}$, which means the usual complex cohomology $H^i$) in degrees $\leq -1$ and some kind of cohomology in degree 0, while they must have 0 cohomology in higher degrees.

*Remark 8* In this situation, with $T$ a 1-tilting module, we may try to characterise $H^0(X^\bullet)$ for $X^\bullet \in \mathcal{T}^{\leq 0}$. Notice that $X^\bullet$ sits in the approximation triangle with respect to $\mathcal{D}$

$$\delta^{\leq -1}(X^\bullet) \longrightarrow X^\bullet \longrightarrow H^0(X^\bullet)[0] \xrightarrow{+1}$$

where

$H^0(X^\bullet)[0] = H^0_{\mathcal{D}}(X^\bullet) = \delta^{\geq 0}\delta^{\leq 0}(X^\bullet) \simeq \delta^{\geq 0}(X^\bullet)$ since $X^\bullet \in \mathcal{D}^{\leq 0}$. If we apply the homological functor $\mathrm{Hom}_{\mathcal{D}(A)}(T, ?)$ to it, we get the long exact sequence of abelian groups

$$\cdots \longrightarrow \mathrm{Hom}_{\mathcal{D}(A)}(T, X^\bullet[1]) \longrightarrow \mathrm{Hom}_{\mathcal{D}(A)}(T, H^0(X^\bullet)[1]) \longrightarrow \mathrm{Hom}_{\mathcal{D}(A)}(T, \delta^{\leq -1}(X^\bullet)[2]) \longrightarrow \cdots$$

The last term is 0 because $\delta^{\leq -1}(X^\bullet) \in \mathcal{D}^{\leq -1} \subseteq \mathcal{T}^{\leq 0}$; similarly, the first is 0 because $X^\bullet \in \mathcal{T}^{\leq 0}$. This means that

$$\mathrm{Ext}^1_A(T, H^0(X^\bullet)) \simeq \mathrm{Hom}_{\mathcal{D}(A)}(T, H^0(X^\bullet)[1]) = 0$$

as well, i.e. that $H^0(X^\bullet) \in KE_0$. □

The inclusions (∗) are precisely the hypothesis of the following proposition by Polishchuk.

**Proposition 6** (*[16, Lemma 1.1.2]*) *Let $\mathcal{R}, \mathcal{S}$ be two $t$-structures in a triangulated category $\mathcal{C}$ such that*

$$\mathcal{R}^{\leq -1} \subseteq \mathcal{S}^{\leq 0} \subseteq \mathcal{R}^{\leq 0} \qquad \textit{(or equivalently } \mathcal{R}^{\geq 0} \subseteq \mathcal{S}^{\geq 0} \subseteq \mathcal{R}^{\geq -1}\textit{)}.$$

*Then the classes:*

$$\mathcal{X} = \mathcal{H}_{\mathcal{R}} \cap \mathcal{S}^{\leq 0} = \mathcal{R}^{\geq 0} \cap \mathcal{S}^{\leq 0}, \qquad \mathcal{Y} = \mathcal{H}_{\mathcal{R}} \cap \mathcal{S}^{\geq 1} = \mathcal{R}^{\leq 0} \cap \mathcal{S}^{\geq 1}$$

*form a torsion pair $(\mathcal{X}, \mathcal{Y})$ in $\mathcal{H}_{\mathcal{R}}$. $\mathcal{S}$ can be reconstructed from $\mathcal{R}$ and $(\mathcal{X}, \mathcal{Y})$ as*

$$\mathcal{S}^{\leq 0} = \left\{X^\bullet \in \mathcal{R}^{\leq 0} :\ H^0_{\mathcal{R}}(X^\bullet) \in \mathcal{X}\right\}$$
$$\mathcal{S}^{\geq 0} = \left\{X^\bullet \in \mathcal{R}^{\geq -1} :\ H^{-1}_{\mathcal{R}}(X^\bullet) \in \mathcal{Y}\right\}.$$

This procedure to recover $\mathcal{S}$ is called *tilting* of the $t$-structure $\mathcal{R}$ with respect to the torsion pair $(\mathcal{X}, \mathcal{Y})$ in $\mathcal{H}_{\mathcal{R}}$. It was introduced by Happel et al. [10], and it is a central tool in the construction we are going to present.

*Remark 9* It can be proved without too much effort that in our case the torsion pair $(\mathcal{X}, \mathcal{Y})$ in $\mathcal{H}_{\mathcal{D}} \simeq A$-Mod so identified is exactly the pair $(KE_0, KE_1)$ induced by the 1-tilting module $T$; this confirms Remark 8.

We would like to use a procedure analogous to the Happel-Reiten-Smalø tilting of Proposition 6 in order to link $\mathcal{D}$ and $\mathcal{T}$ in the $n > 1$ case. Notice that if we repeat this tilting operation $n$ times, the first and last of the produced $t$-structures will be related by the inclusions of Proposition 5. Indeed, let $\mathcal{R}_0, \dots, \mathcal{R}_n$ be $t$-structures such that $\mathcal{R}_i$ is obtained by tilting $\mathcal{R}_{i-1}$ with respect to some torsion pair on $\mathcal{H}_{\mathcal{R}_{i-1}}$, for every $i = 1, \dots, n$. Then, we have by construction

$$\mathcal{R}_0^{\leq -1} \subseteq \mathcal{R}_1^{\leq 0} \subseteq \mathcal{R}_0^{\leq 0} \quad \text{and} \quad \mathcal{R}_1^{\leq -1} \subseteq \mathcal{R}_2^{\leq 0} \subseteq \mathcal{R}_1^{\leq 0}$$

which combined give

$$\mathcal{R}_0^{\leq -2} \subseteq \mathcal{R}_2^{\leq 0} \subseteq \mathcal{R}_0^{\leq 0}.$$

One can then clearly prove by induction that

$$\mathcal{R}_0^{\leq -n} \subseteq \mathcal{R}_n^{\leq 0} \subseteq \mathcal{R}_0^{\leq 0}.$$

If $T$ is an $n$-tilting $A$-module, we shall show that the associated $t$-structure $\mathcal{T}$ in $\mathcal{D}(A)$ can indeed be constructed from the natural $t$-structure $\mathcal{D}$ with this iterated procedure. To do so, we are going to construct the "intermediate" $t$-structures produced after each tilting.

For $i = 0, \dots, n$, consider the strict full subcategories $\mathcal{D}_i^{\geq} = \mathcal{D}^{\geq -i} \cap \mathcal{T}^{\geq 0}$ (notice that we are working with the coaisles). We have as wanted that

$$\mathcal{D}^{\geq 0} = \mathcal{D}_0^{\geq} \subseteq \mathcal{D}_1^{\geq} \subseteq \cdots \subseteq \mathcal{D}_n^{\geq} = \mathcal{T}^{\geq 0}$$

and $\mathcal{D}_{i-1}^{\geq} \subseteq \mathcal{D}_i^{\geq} \subseteq \mathcal{D}_{i-1}^{\geq}[1]$ for $i = 1, \dots, n$. The only thing needed to proceed with an iterated application of Proposition 6 is to prove that these $\mathcal{D}_i^{\geq}$ are indeed the coaisles of some $t$-structures, for $i = 1, \dots, n-1$.

**Lemma 3** *The $\mathcal{D}_i^{\geq} = \mathcal{D}^{\geq -i} \cap \mathcal{T}^{\geq 0}$ are coaisles of $t$-structures.*

*Proof* As we noticed before (see Remark 3 and the definition of $\mathcal{T}$), we have

$$\mathcal{D}^{\geq -i} = \left\{ Y^\bullet \in \mathcal{D}(A) : \ \mathrm{Hom}_{\mathcal{D}(A)}(A[i], Y^\bullet[j]) = 0 \text{ for every } j < 0 \right\}$$
$$\mathcal{T}^{\geq 0} = \left\{ Y^\bullet \in \mathcal{D}(A) : \ \mathrm{Hom}_{\mathcal{D}(A)}(T, Y^\bullet[j]) = 0 \text{ for every } j < 0 \right\}.$$

Hence, we have

$$\mathcal{D}^{\geq -i} \cap \mathcal{T}^{\geq 0} = \left\{ Y^\bullet \in \mathcal{D}(A) : \ \mathrm{Hom}_{\mathcal{D}(A)}(T \oplus A[i]), Y^\bullet[j]) = 0 \text{ for every } j < 0 \right\}$$

which is the coaisle of the $t$-structure generated by $T \oplus A[i]$ in the sense of Proposition 4.

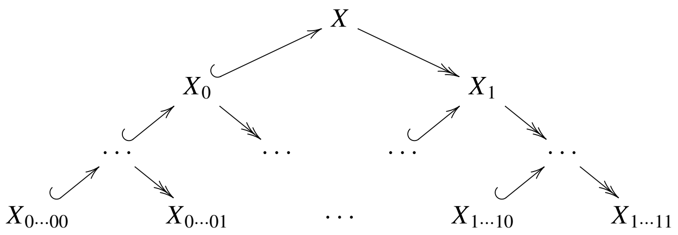
This concludes our previous discussion, making sure that $\mathcal{T}$ can be constructed from $\mathcal{D}$ with (at most) $n$ applications of the procedure of tilting a $t$-structure with respect to a torsion pair on its heart.

## 6 The *t*-tree

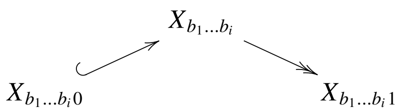
We are now going to exploit this fact to solve our decomposition problem.

First, we characterise the torsion pairs involved. According to Proposition 6, at the $i$-th step, the $t$-structure $\mathcal{D}_i$ (having coaisle $\mathcal{D}_i^{\geq 0} = \mathcal{D}_i^{\geq} = \mathcal{D}^{\geq -i} \cap \mathcal{T}^{\geq 0}$) is tilted with respect to the torsion pair $(\mathcal{X}_i, \mathcal{Y}_i) = (\mathcal{D}_i^{\geq 0} \cap \mathcal{D}_{i+1}^{\leq 0}, \mathcal{D}_i^{\leq 0} \cap \mathcal{D}_{i+1}^{\geq 1})$ in the heart $\mathcal{H}_i$ of $\mathcal{D}_i$, $i = 0, \ldots, n-1$, thus producing the $t$-structure $\mathcal{D}_{i+1}$.

**Theorem 4** *Let $T$ be a $n$-tilting left $A$-module. We can associate to each left $A$-module $X$ a tree (we call it the $t$-tree of $X$ with respect to the $t$-structure induced by the tilting module $T$)*




*with $n+1$ rows, where*

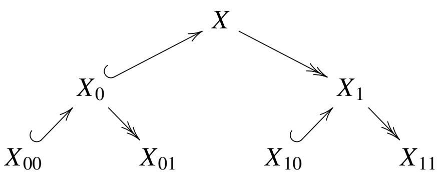



*is the short exact sequence obtained decomposing $X_{b_1\ldots b_i}$ with respect to the torsion pair $(\mathcal{X}_i[-(b_1+\cdots+b_i)], \mathcal{Y}_i[-(b_1+\cdots+b_i)])$ in $\mathcal{H}_i[-(b_1+\cdots+b_i)]$.*

*Proof* We may regard the left $A$-module $X$ as a complex concentrated in degree 0, $X[0]$ in the heart $\mathcal{H}_{\mathcal{D}} = \mathcal{H}_0$. The first torsion pair $(\mathcal{X}_0, \mathcal{Y}_0)$ provides then a decomposition

$$X_0 \hookrightarrow X \twoheadrightarrow X_1 \quad \text{in } \mathcal{H}_0$$

with $X_0 \in \mathcal{X}_0$, $X_1 \in \mathcal{Y}_0$. Notice that by construction $\mathcal{X}_0 \subseteq \mathcal{H}_1$ and $\mathcal{Y}_0 \subseteq \mathcal{H}_1[-1]$ (see Proposition 6); this means that we can use $(\mathcal{X}_1, \mathcal{Y}_1)$ and $(\mathcal{X}_1[-1], \mathcal{Y}_1[-1])$ to further decompose $X_0$ and $X_1$, respectively, obtaining



with the exact sequences in the respective abelian categories:

$$X_0 \hookrightarrow X \twoheadrightarrow X_1 \quad \text{in } \mathcal{H}_0$$

$$X_{00} \hookrightarrow X_0 \twoheadrightarrow X_{01} \quad \text{in } \mathcal{H}_1 \qquad\qquad X_{10} \hookrightarrow X_1 \twoheadrightarrow X_{11} \quad \text{in } \mathcal{H}_1[-1]$$

Now, notice again that since $\mathcal{X}_1 \subseteq \mathcal{H}_2$ and $\mathcal{Y}_1 \subseteq \mathcal{H}_2[-1]$, we have that $X_{00} \in \mathcal{H}_2$, $X_{01}, X_{10} \in \mathcal{H}_2[-(0+1)] = \mathcal{H}_2[-(1+0)]$ and $X_{11} \in \mathcal{H}_2[-(1+1)]$.

Inductively, by decomposing each $X_{b_1 \ldots b_i}$ with respect to the torsion pair $(\mathcal{X}_i[-(b_1 + \cdots + b_i)], \mathcal{Y}_i[-(b_1 + \cdots + b_i)])$ in $\mathcal{H}_i[-(b_1 + \cdots + b_i)]$ we obtain objects $X_{b_1 \ldots b_i 0} \in \mathcal{H}_{i+1}[-(b_1 + \cdots + b_i)]$ and $X_{b_1 \ldots b_i 1} \in \mathcal{H}_{i+1}[-(b_1 + \cdots + b_i + 1)]$.

After $n$ steps, we obtain the complete diagram.

We claim that Theorem 4 solves our decomposition problem. Indeed, by construction each object $X_{b_1 \cdots b_n}$ in the last row (called a *t-leaf*) belongs to $\mathcal{H}_n[-(b_1 + \cdots + b_n)] = \mathcal{H}_{\mathcal{T}}[-(b_1 + \cdots + b_n)]$: as noted in Remark 7, these shifted hearts are extensions of the Miyashita classes: $KE_{b_1 + \cdots + b_n} = A\text{-Mod} \cap \mathcal{H}_{\mathcal{T}}[-(b_1 + \cdots + b_n)]$. Moreover, these shifted hearts are obtained by adding only non-module objects (i.e., objects of $\mathcal{D}(A)$ outside of $\mathcal{H}_{\mathcal{D}}$) to the corresponding Miyashita class; for this reason, they are less artificial than other enlargments, and instead shed a new light on the Miyashita classes. The latter can indeed be regarded as the piece of the shifted hearts of $\mathcal{T}$ visible in the category of modules.

*Example 3* We recall one last time the situation considered in Example 1 to show an application of the construction of the $t$-tree; we will do it for the simple module $2$ again.

First, a computation shows that the indecomposable complexes in $\mathcal{D}(A)$ are (shifts of)

$$\left\{ 1,\ 2,\ 3,\ \substack{1\\2},\ \substack{2\\3},\ \substack{2\\3} \to \substack{1\\2} \right\}.$$

Since we know that $\mathcal{D}^{\geq 0} \subseteq \mathcal{T}^{\geq 0}$, any bounded below complex will belong to $\mathcal{T}^{\geq 0}$, up to shifiting it enough to the right. We can then check for each of the indecomposable complexes what is their leftmost shift which still belongs to $\mathcal{T}^{\geq 0}$; with an easy computation, the following is the result:

$$\mathcal{T}^{\geq 0} = \left\langle 1,\ 2,\ 3[2],\ \substack{1\\2},\ \substack{2\\3},\ \substack{2\\3} \to \overset{\bullet}{\substack{1\\2}} \right\rangle$$

where the dot over a complex indicates its degree 0. The angle brackets will be used to denote the closure under direct sums and negative shifts.

Following the construction, we can compute the intermediate coaisles:

$$\mathcal{D}_0^{\geq 0} = \left\langle 1\,,\ 2\,,\ 3\,,\ \begin{smallmatrix}1\\2\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix},\ \begin{smallmatrix}\bullet\\2\\3\end{smallmatrix} \to \begin{smallmatrix}1\\2\end{smallmatrix} \right\rangle = \mathcal{D}^{\geq 0}$$
$$\mathcal{D}_1^{\geq 0} = \left\langle 1\,,\ 2\,,\ 3\,[1],\ \begin{smallmatrix}1\\2\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix} \to \begin{smallmatrix}\bullet\\1\\2\end{smallmatrix} \right\rangle$$
$$\mathcal{D}_2^{\geq 0} = \left\langle 1\,,\ 2\,,\ 3\,[2],\ \begin{smallmatrix}1\\2\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix} \to \begin{smallmatrix}\bullet\\1\\2\end{smallmatrix} \right\rangle = \mathcal{T}^{\geq 0}.$$

Now we compute the hearts of the respective $t$-structures: to do this, we use Lemma 2. An object $X$ of $\mathcal{D}_i^{\geq 0}$ will belong to $\mathcal{H}_i$ if and only if $\mathrm{Hom}_{\mathcal{D}(A)}(X, Y) = 0$ for every $Y \in \mathcal{D}_i^{\geq 1} = \mathcal{D}_i^{\geq 0}[-1]$. In particular, it is easy to see that we must look for objects of the heart only among the "leftmost shifts" we have listed. The resulting computation gives (only indecomposable objects are listed)

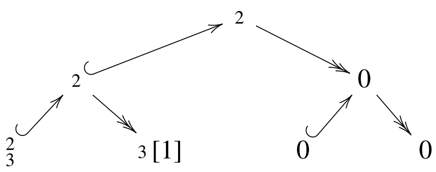
$$\mathcal{H}_0 = \left\{ 1\,,\ 2\,,\ 3\,,\ \begin{smallmatrix}1\\2\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix} \right\} = \mathcal{H}_{\mathcal{D}} = A\text{-Mod}$$
$$\mathcal{H}_1 = \left\{ 1\,,\ 2\,,\ 3\,[1],\ \begin{smallmatrix}1\\2\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix} \to \begin{smallmatrix}\bullet\\1\\2\end{smallmatrix} \right\}$$
$$\mathcal{H}_2 = \left\{ 1\,,\ 3\,[2],\ \begin{smallmatrix}1\\2\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix} \to \begin{smallmatrix}\bullet\\1\\2\end{smallmatrix} \right\} = \mathcal{H}_{\mathcal{T}}.$$

Notice that neither $2$ nor its shifts belong to $\mathcal{H}_{\mathcal{T}}$, which means exactly that it does not belong to any Miyashita class.

Lastly, we can compute the torsion pairs $(\mathcal{X}_i, \mathcal{Y}_i)$ in $\mathcal{H}_i$, for $i = 0, 1$. We have

$$\mathcal{X}_0 = \mathcal{H}_0 \cap \mathcal{H}_1 = \left\{ 1\,,\ 2\,,\ \begin{smallmatrix}1\\2\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix} \right\}, \qquad \mathcal{Y}_0 = \mathcal{H}_0 \cap \mathcal{H}_1[-1] = \{ 3 \}$$
$$\mathcal{X}_1 = \mathcal{H}_1 \cap \mathcal{H}_2 = \left\{ 1\,,\ \begin{smallmatrix}1\\2\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix},\ \begin{smallmatrix}2\\3\end{smallmatrix} \to \begin{smallmatrix}\bullet\\1\\2\end{smallmatrix} \right\}, \qquad \mathcal{Y}_1 = \mathcal{H}_1 \cap \mathcal{H}_2[-1] = \{ 3\,[1] \}.$$

The $t$-tree for the module $2$ is then




where the bottom left exact sequence is that associated to the distinguished triangle

$$\begin{smallmatrix}2\\3\end{smallmatrix} \longrightarrow 2 \longrightarrow 3\,[1] \xrightarrow{+1} .$$

Notice that this triangle can be shifted to become $3 \longrightarrow {\scriptstyle 2 \atop 3} \longrightarrow 2 \xrightarrow{+1}$, which can be read as a short exact sequence of modules. This says that $2$ is realised as the cokernel of the monomorphism $3 \to {\scriptstyle 2 \atop 3}$, which is what was found following Jensen et al. in Example 2.

We conclude with a remark about the construction presented above, giving a possible direction for future developments.

*Remark 10* Notice that while our motivation comes from an $n$-tilting $A$-module, the construction of the $t$-tree only relies on the existence of some $t$-structures $\mathcal{D}_i$, for $i = 0, \ldots, n$, having the property that $\mathcal{D}_i^{\geq 0} \subseteq \mathcal{D}_{i+1}^{\geq 0} \subseteq \mathcal{D}_i^{\geq -1}$. Therefore, it can be replicated in an arbitrary triangulated category $\mathcal{C}$, given such $t$-structures: to any object in the heart $\mathcal{H}_0$ of $\mathcal{D}_0$, it is possible to associate a tree-like diagram with $n+1$ rows having leaves in the shifts $\mathcal{H}_n[-e]$ of the heart $\mathcal{H}_n$ of $\mathcal{D}_n$, for $e = 0, \ldots, n$. It is of natural interest to investigate other situations in which such $t$-structures may appear.

## References

1. Alonso Tarrío, L., Jeremías López, A., Souto Salorio, M.J.: Construction of $t$-structures and equivalences of derived categories. Trans. Amer. Math. Soc. **355**(6), 2523–2543 (2003). https://doi.org/10.1090/S0002-9947-03-03261-6
2. Angeleri Hügel, L., Coelho, F.U.: Infinitely generated tilting modules of finite projective dimension. Forum Math. **13**(2), 239–250 (2001). https://doi.org/10.1515/form.2001.006
3. Bazzoni, S.: A characterization of $n$-cotilting and $n$-tilting modules. J. Algebra **273**(1), 359–372 (2004). https://doi.org/10.1016/S0021-8693(03)00432-0
4. Bazzoni, S.: The $t$-structure induced by an $n$-tilting module. Trans. Amer. Math. Soc. **371**(9), 6309–6340 (2019). https://doi.org/10.1090/tran/7488
5. Beĭlinson, A.A., Bernstein, J., Deligne, P.: Faisceaux pervers. In: Analysis and Topology on Singular Spaces, I (Luminy, 1981). In: *Astérisque*, vol. 100, pp. 5–171. Soc. Math. France, Paris (1982)
6. Brenner, S., Butler, M.C.R.: Generalizations of the Bernstein-Gel'fand-Ponomarev reflection functors. In: Representation theory, II (Proceedings of the Second International Conference, Carleton University, Ottawa, ON, 1979). Mathematics, vol. 832, pp. 103–169. Springer, Berlin and New York (1980)
7. Cline, E., Parshall, B., Scott, L.: Derived categories and Morita theory. J. Algebra **104**(2), 397–409 (1986). https://doi.org/10.1016/0021-8693(86)90224-3
8. Fiorot, L., Mattiello, F., Tonolo, A.: A classification theorem for t-structures. J. Algebra **465**, 214–258 (2016). https://doi.org/10.1016/j.jalgebra.2016.07.008. URL http://www.sciencedirect.com/science/article/pii/S0021869316301843
9. Göbel, R., Trlifaj, J.: Approximations and endomorphism algebras of modules. In: De Gruyter Expositions in Mathematics, vol. 41. Walter de Gruyter GmbH & Co. KG, Berlin (2006). https://doi.org/10.1515/9783110199727
10. Happel, D., Reiten, I., Smalø, S.O.: Tilting in abelian categories and quasitilted algebras. Mem. Amer. Math. Soc. **120**(575), viii+ 88 (1996). https://doi.org/10.1090/memo/0575
11. Jensen, B.T., Madsen, D.O., Su, X.: Filtrations in abelian categories with a tilting object of homological dimension two. J. Algebra Appl. **12**(2), 1250149, 15 (2013). https://doi.org/10.1142/S0219498812501496

12. Keller, B., Vossieck, D.: Aisles in derived categories. Bull. Soc. Math. Belg. Sér. A **40**(2), 239–253 (1988). Deuxième Contact Franco-Belge en Algèbre, Faulx-les-Tombes (1987)
13. Lo, J.: Torsion pairs and filtrations in abelian categories with tilting objects. J. Algebra Appl. **14**(8), 1550121, 16 (2015). https://doi.org/10.1142/S0219498815501212
14. Miyashita, Y.: Tilting modules of finite projective dimension. Math. Z. **193**(1), 113–146 (1986). https://doi.org/10.1007/BF01163359
15. Neeman, A.: Triangulated categories. In: Annals of Mathematics Studies, vol. 148. Princeton University Press, Princeton, NJ (2001). https://doi.org/10.1515/9781400837212
16. Polishchuk, A.: Constant families of $t$-structures on derived categories of coherent sheaves. Mosc. Math. J. **7**(1), 109–134, 167 (2007)
17. Positselski L., Stovicek J.: The tilting-cotilting correspondence, arXiv:1710.02230. To appear in International Mathematics Research Notices (2017). https://doi.org/10.1093/imrn/rnz116
18. Stovicek, J.: Derived equivalences induced by big cotilting modules. Adv. Math. **263** (2013). https://doi.org/10.1016/j.aim.2014.06.007
19. The Stacks project authors: The stacks project (2018). https://stacks.math.columbia.edu
20. Tonolo, A.: Tilting modules of finite projective dimension: sequentially static and costatic modules. J. Algebra Appl. **1**(3), 295–305 (2002). https://doi.org/10.1142/S0219498802000197