Progress in Commutative Algebra 2

Progress in Commutative Algebra 2

Closures, Finiteness and Factorization

edited by
Christopher Francisco
Lee Klingler
Sean Sather-Wagstaff
Janet C. Vassilev

Preface

This collection of papers in commutative algebra stemmed out of the 2009 Fall Southeastern American Mathematical Society Meeting which contained three special sessions in the field:

- Special Session on Commutative Ring Theory, a Tribute to the Memory of James Brewer, organized by Alan Loper and Lee Klingler;
- Special Session on Homological Aspects of Module Theory, organized by Andy Kustin, Sean Sather-Wagstaff, and Janet Vassilev; and
- Special Session on Graded Resolutions, organized by Chris Francisco and Irena Peeva.

Much of the commutative algebra community has split into two camps, for lack of a better word: the Noetherian camp and the non-Noetherian camp. Most researchers in commutative algebra identify with one camp or the other, though there are some notable exceptions to this. We had originally intended this to be a Proceedings Volume for the conference as the sessions had a nice combination of both Noetherian and non-Noetherian talks. However, the project grew into two Volumes with invited papers that are blends of survey material and new research. We hope that members from the two camps will read each others' papers and that this will lead to increased mathematical interaction between the camps.

As the title suggests, this volume, Progress in Commutative Algebra II, contains surveys on aspects of closure operations, finiteness conditions and factorization. Contributions to this volume have come mainly from speakers in the first and second sessions and from invited articles on closure operations, test ideals, Noetherian rings without finite normaliztion and non-unique factorization. The collection documents some current trends in two of the most active areas of commutative algebra.

Closure operations on ideals and modules are a bridge between Noetherian and non-Noetherian commutative algebra. The Noetherian camp typically study structures related to a particular closure operation such as the core or the test ideal or how particular closure operations yield nice proofs of hard theorems. The non-Noetherian camp approach closure operations from the view of multiplicative ideal theory and the relationship to Kronecker function rings. This volume contains a nice guide to closure operations by Epstein, but also contains an article on test ideals by Schwede and Tucker and one by Enescu which discusses the action of the Frobenius on finite dimensional vector spaces both of which are related to tight closure.

Finiteness properties of rings and modules or the lack of them come up in all aspects of commutative algebra. For instance, the division between the Noetherian and the

non-Noetherian crowd comes down to the property that all ideals in a Noetherian ring are finitely generated, by definition. However, in the study of non-Noetherian rings it is much easier to find a ring having a finite number of prime ideals. We have included papers by Boynton and Sather-Wagstaff and by Watkins that discuss the relationship of rings with finite Krull dimension and their finite extensions. Finiteness properties in commutative group rings are discussed in Glaz and Schwarz's paper. And Olberding's selection presents us with constructions that produce rings whose integral closure in their field of fractions is not finitely generated.

The final three papers in this volume investigate factorization in a broad sense. The first paper by Celikbas and Eubanks-Turner discusses the partially ordered set of prime ideals of the projective line over the integers. We have also included a paper on zero divisor graphs by Coykendall, Sather-Wagstaff, Sheppardson and Spiroff. The final paper, by Chapman and Krause, concerns non-unique factorization.

The first session was a Tribute to the Memory of James Brewer. As many of the authors participated in this session, we dedicate this volume to Brewer's memory. Enjoy!

March 2012   Sean Sather-Wagstaff
                                                            Chris Francisco
                                                            Lee Klingler
                                                          Janet C. Vassilev

Contents

Jim Coykendall, Sean Sather-Wagstaff, Laura Sheppardson, and Sandy Spiroff
On Zero Divisor Graphs

Scott T. Chapman and Ulrich Krause
A Closer Look at Non-unique Factorization via Atomic Decay and Strong Atoms

A Guide to Closure Operations
in Commutative Algebra

Neil Epstein

Abstract. This article is a survey of closure operations on ideals in commutative rings, with an emphasis on structural properties and on using tools from one part of the field to analyze structures in another part. The survey is broad enough to encompass the radical, tight closure, integral closure, basically full closure, saturation with respect to a fixed ideal, and the v-operation, among others.

Keywords. Closure Operation, Tight Closure, Integral Closure, Star-operation.

2010 Mathematics Subject Classification. Primary: 13-02; Secondary: 13A15, 13A35, 13B22, 13A99.

1 Introduction

There have been quite a few books and survey articles on tight closure (e.g. [40, 49, 50, 71, 72]), on integral closure (e.g. [51, 73, 74]), and on star-operations on integral domains (e.g. [23; 25, Chapters 32 and 34] but as far as this author knows, no such article on closure operations in general. However, several authors (e.g. [9, 19, 75]) have recently found it useful to consider closure operations as a subject in itself, so I write this article as an attempt to provide an overall framework. This article is intended both for the expert in one closure operation or another who wants to see how it relates to the rest, and for the lay commutative algebraist who wants a first look at what closure operations are. For the most part, this article will not go into the reasons why any given closure operation is important. Instead, I will concentrate on the structural aspects of closure operations, how closure operations arise, how to think about them, and how to analyze them.

　The reader may ask: "If the only closure operation I am interested in is c, why should I care about other closure operations?" Among other reasons: the power of analogical thinking is central to what mathematicians do. If the d-theorists have discovered or used a property of their closure operation d, the c-theorist may use this to investigate the analogous property for c, *and may not have thought to do so without knowledge of* d-*closure*. Morover, what holds trivially for one closure operation can be a deep theorem (or only hold in special cases) for another – and vice versa. A good example is persistence (see Section 4.3).

In most survey articles, one finds a relatively well-defined subject and a more-or-less linear progression of ideas. The subject exists as such in the minds of those who practice it before the article is written, and the function of the article is to introduce new people to the already extant system of ideas. The current article serves a somewhat different function, as the ideas in this paper are not linked sociologically so much as axiomatically. Indeed, there are at least three socially distinct groups of people studying these things, some of whom seem barely to be aware of each other's existence. In this article, one of my goals is to bridge that gap.

The structure of the article is as follows: In Section 2, I introduce the notion of closures, eleven typical examples, and some non-examples. In Section 3, I exhibit six simple constructions and show how all the closure operations from Section 2 arise from these. The next section, Section 4, concerns properties that closures may have; it comprises more than 1/4 of the paper! In it, we spend a good bit of time on star- and semi-prime operations, after which we devote a subsection each to forcing algebras, persistence, homological conjectures, tight closure-like properties, and (homogeneous) equational closures. The short Section 5 explores a tightly related set of notions involving what happens when one looks at the collection of *sub*ideals that have the same closure as a given ideal. In Section 6, we explore ring properties that arise from certain ideals being closed. Finally in Section 7, we talk about various ways to extend to closures on (sub)*modules*. Beyond the material in Sections 2 and 3, the reader may read the remaining sections in almost any order.

Throughout this paper, R is a commutative ring with unity. At this point, one would normally either say that R will be assumed Noetherian, or that R will not necessarily be assumed to be Noetherian. However, one of the reasons for the gap mentioned above is that people are often scared off by such statements. It is true that many of the examples I present here seem to work best (and are most studied) in the Noetherian context. On the other hand, I have also included some of the main examples and constructions that are most interesting in the non-Noetherian case. As my own training is among those who work mainly with Noetherian rings, it probably is inevitable that I will sometimes unknowingly assume a ring is Noetherian. In any case, the article should remain accessible and interesting to all readers.

2 What Is a Closure Operation?

2.1 The Basics

Definition 2.1.1. Let R be a ring. A *closure operation* cl on a set of ideals $\mathcal{I}$ of R is a set map cl : $\mathcal{I} \to \mathcal{I}$ ($I \mapsto I^{\mathrm{cl}}$) satisfying the following conditions:

 (i) (Extension) $I \subseteq I^{\mathrm{cl}}$ for all $I \in \mathcal{I}$.

 (ii) (Idempotence) $I^{\mathrm{cl}} = (I^{\mathrm{cl}})^{\mathrm{cl}}$ for all $I \in \mathcal{I}$.

(iii) (Order-preservation) If $J \subseteq I$ are ideals of $\mathcal{I}$, then $J^{\mathrm{cl}} \subseteq I^{\mathrm{cl}}$.

If $\mathcal{J}$ is the set of *all* ideals of R, then we say that cl is a closure operation *on* R. We say that an ideal $I \in \mathcal{J}$ is cl-*closed* if $I = I^{\mathrm{cl}}$.

As far as I know, this concept is due to E. H. Moore [60], who defined it (over a century ago!) more generally for subsets of a set, rather than ideals of a ring. Moore's context was mathematical analysis. His has been the accepted definition of "closure operation" in lattice theory and universal algebra ever since (e.g. [5, V.1] or [12, 7.1]). Oddly, this general definition of closure operation does not seem to have gained currency in commutative algebra until the late 1980s [62, 64], although more special structures already had standard terminologies associated to them (see 4.1).

Example 2.1.2 (Examples of closures). The reader is invited to find his/her favorite closure(s) on the following list. Alternately, the list may be skipped and referred back to when an unfamiliar closure is encountered in the text.

(i) The *identity closure*, sending each ideal to itself, is a closure operation on R. (In multiplicative ideal theory, this is usually called the d-*operation*.)

(ii) The *indiscrete closure*, sending each ideal to the unit ideal R, is also a closure operation on R.

(iii) The *radical* is the first nontrivial example of a closure operation on an arbitrary ring R. It may be defined in one of two equivalent ways. Either

$$\sqrt{I} := \{f \in R \mid \exists \text{ a positive integer } n \text{ such that } f^n \in I\}$$

or

$$\sqrt{I} := \bigcap \{\mathfrak{p} \in \mathrm{Spec}\, R \mid I \subseteq \mathfrak{p}\}.$$

The importance of the radical is basic in the field of algebraic geometry, due to Hilbert's Nullstellensatz (cf. any introductory textbook on algebraic geometry).

(iv) Let α be a fixed ideal of R. Then α-*saturation* is a closure operation on R. Using the usual notation of $(- : \alpha^\infty)$, we may define it as follows:

$$(I : \alpha^\infty) := \bigcup_{n \in \mathbb{N}} (I : \alpha^n) = \{r \in R \mid \exists n \in \mathbb{N} \text{ such that } \alpha^n r \subseteq I\}$$

This operation is important in the study of *local cohomology*. Indeed,

$$H^0_\alpha(R/I) = \frac{(I : \alpha^\infty)}{I}.$$

(v) The *integral closure* is a closure operation as well. One of the many equivalent definitions is as follows: For an element $r \in R$ and an ideal I of R,[1] $r \in I^-$ if

---

[1] Some may find my choice of notation surprising. Popular notations for integral closure include I_a and $\overline{I}$. I avoid the first of these because it looks like a variable subscript, as the letter a does not seem to stand for anything. The problem with the second notation is that it is overly ambiguous. Such notation can mean integral closure of rings, integral closure of ideals, a quotient module, and so forth. So in my articles, I choose to use the I^- notation to make it more consistent with the notation of other closure operations (such as tight, Frobenius, and plus closures).

there exist $n \in \mathbb{N}$ and $a_i \in I^i$ for $1 \leq i \leq n$ such that

$$r^n + \sum_{i=1}^{n} a_i r^{n-i} = 0.$$

Integral closure is a big topic. See for instance the books [51, 74].

(vi) Let R be an integral domain. Then *plus closure* is a closure operation. It is traditionally linked with tight closure (see below), and defined as follows: For an ideal I and an element $x \in R$, we say that $x \in I^+$ if there is some injective map $R \to S$ of integral domains, which makes S a finite R-module, such that $x \in IS$. (See Section 3.2 (vi) for general R.)

(vii) Let R be a ring of prime characteristic $p > 0$. Then *Frobenius closure* is a closure operation on R. To define this, we need the concept of bracket powers. For an ideal I, $I^{[p^n]}$ is defined to be the ideal generated by all the p^nth powers of elements of I. For an ideal I and an element $x \in R$, we say that $x \in I^F$ if there is some $n \in \mathbb{N}$ such that $x^{p^n} \in I^{[p^n]}$.

(viii) Let R be a ring of prime characteristic $p > 0$. Then *tight closure* is a closure operation on R. For an ideal I and an element $x \in R$, we say that $x \in I^*$ if there is some power $e_0 \in \mathbb{N}$ such that the ideal $\bigcap_{e \geq e_0} (I^{[p^e]} : x^{p^e})$ is not contained in any minimal prime of R.

(ix) Let R be a complete local domain. For an R-algebra S, we say that S is *solid* if $\mathrm{Hom}_R(S, R) \neq 0$. We define *solid closure* on R by saying that $x \in I^\star$ if $x \in IS$ for some solid R-algebra S. (See 3.2(ix) for general R.)

(x) Let Δ be a multiplicatively closed set of ideals. The Δ-*closure* [64] of an ideal I is $I^\Delta := \bigcup_{K \in \Delta}(IK : K)$. Ratliff [64] shows close connections between Δ-closure and integral closure for appropriate choices of Δ.

(xi) If $(R, \mathfrak{m})$ is local, and I is $\mathfrak{m}$-primary, then the *basically full closure* [31] of I is $I^{\mathrm{bf}} := (I\mathfrak{m} : \mathfrak{m})$. (Note: This is a closure operation even for non-$\mathfrak{m}$-primary ideals I. However, only for $\mathfrak{m}$-primary I does it produce the smallest so-called "basically full" ideal that contains I.)

Additional examples of closures include the v-, t-, and w-operations (4.1), various tight closure imitators (4.5), continuous and axes closures [8], natural closure [20], and weak subintegral closure [77]. (See the references for more details on these last four.)

Some properties follow from the axiomatic definition of a closure operation:

Proposition 2.1.3. *Let R be a ring and* cl *a closure operation. Let I be an ideal and* $\{I_\alpha\}_{\alpha \in \mathcal{A}}$ *a set of ideals.*

(i) *If every I_α is* cl-*closed, so is $\bigcap_\alpha I_\alpha$.*

(ii) $\bigcap_\alpha I_\alpha{}^{\mathrm{cl}}$ *is* cl-*closed.*

(iii) I^{cl} *is the intersection of all* cl-*closed ideals that contain* I.

(iv) $\left(\sum_\alpha I_\alpha{}^{\mathrm{cl}}\right)^{\mathrm{cl}} = \left(\sum_\alpha I_\alpha\right)^{\mathrm{cl}}$.

Proof. Let I and $\{I_\alpha\}$ be as above.

(i) For any $\beta \in \mathscr{A}$, we have $\bigcap_\alpha I_\alpha \subseteq I_\beta$, so since cl is order-preserving, we have $(\bigcap_\alpha I_\alpha)^{\mathrm{cl}} \subseteq I_\beta{}^{\mathrm{cl}} = I_\beta$. Since this holds for any β, we have $(\bigcap_\alpha I_\alpha)^{\mathrm{cl}} \subseteq \bigcap_\beta I_\beta = \bigcap_\alpha I_\alpha$.

(ii) This follows directly from part (i).

(iii) Let J be an ideal such that $I \subseteq J = J^{\mathrm{cl}}$. Then by order-preservation, $I^{\mathrm{cl}} \subseteq J^{\mathrm{cl}} = J$, so I^{cl} is contained in the given intersection. But since $I^{\mathrm{cl}} = (I^{\mathrm{cl}})^{\mathrm{cl}}$ is one of the ideals being intersected, the conclusion follows.

(iv) '$\supseteq$': By the Extension property, $I_\alpha{}^{\mathrm{cl}} \supseteq I_\alpha$, so $\sum_\alpha I_\alpha{}^{\mathrm{cl}} \supseteq \sum_\alpha I_\alpha$. Then the conclusion follows from order-preservation.

'$\subseteq$': For any $\beta \in \mathscr{A}$, $I_\beta \subseteq \sum_\alpha I_\alpha \subseteq (\sum_\alpha I_\alpha)^{\mathrm{cl}}$, so by order-preservation and idempotence, $I_\beta{}^{\mathrm{cl}} \subseteq ((\sum_\alpha I_\alpha)^{\mathrm{cl}})^{\mathrm{cl}} = (\sum_\alpha I_\alpha)^{\mathrm{cl}}$. Since this holds for all $\beta \in \mathscr{A}$, we have $\sum_\alpha I_\alpha{}^{\mathrm{cl}} \subseteq (\sum_\alpha I_\alpha)^{\mathrm{cl}}$. $\qquad\square$

We finish the subsection on "basics" by giving two alternate characterizations of closure operations on R:

Remark 2.1.4. Here is a "low-tech" way of looking at closure operations, due essentially to Moore [60]. Namely, giving a closure operation is *equivalent* to giving a collection $\mathcal{C}$ of ideals such that the intersection of any subcollection is also in $\mathcal{C}$.

For suppose cl is a closure operation on R. Let $\mathcal{C}$ be the class of cl-closed ideals. That is, $I \in \mathcal{C}$ iff $I = I^{\mathrm{cl}}$. By Proposition 2.1.3 (i), the intersection of any subcollection of ideals in $\mathcal{C}$ is also in $\mathcal{C}$.

Conversely, suppose $\mathcal{C}$ is a collection of ideals for which the intersection of any subcollection is in $\mathcal{C}$. For an ideal I, let $I^{\mathrm{cl}} := \bigcap\{J \mid I \subseteq J \in \mathcal{C}\}$. All three of the defining properties of closure operations follow easily. Hence, cl is a closure operation.

The applicability of this observation is obvious: Given any collection of ideals in a ring, one may obtain a closure operation from it by extending it to contain all intersections of the ideals in the collection, and letting these be the closed ideals. The resulting closure operation may then be used to analyze the property that defined the original class of ideals.

Remark 2.1.5. On the other hand, here is a "high-tech" way of looking at closure operations. Let R be a ring, and $\mathcal{C}$ be the *category* associated to the partially ordered set of ideals of R. Then a closure operation on R is the same thing as a *monad in the category* $\mathcal{C}$ (see [58, VI.1] for the definition of monad in a category). It is easy to see that any monad in a poset is idempotent, and the theory of idempotent monads is

central in the study of so-called "localization functors" in algebraic topology (thanks to G. Biedermann and G. Raptis, who mention [1, Chapter 2] as a good source, for pointing me in this direction).

2.2 Not-quite-closure Operations

It should be noted that the three given axioms of closure operations are independent of each other; many operations on ideals satisfy two of the axioms without satisfying the third. For example, the operation on ideals that sends every ideal to the 0 ideal is idempotent (condition (ii)) and is order-preserving (condition (iii)), but of course is not extensive unless R is the zero ring.

For an operation that is extensive (i) and order-preserving (iii), but is not idempotent, let f be a fixed element (or ideal) of R, and consider the operation $I \mapsto (I : f)$. This is almost never idempotent. For example one always has $((f^2 : f) : f) = (f^2 : f^2) = R$ of course, but if f is any nonzero element of the Jacobson radical of R, then $(f^2 : f) \neq R$.

Another non-idempotent operation that is extensive and order-preserving is the so-called "α-tight closure", for a fixed ideal α [28], denoted $(\cdot)^{*\alpha}$. By definition, $x \in I^{*\alpha}$ if there is some $e_0 \in \mathbb{N}$ such that the ideal $\bigcap_{e \geq e_0} (I^{[p^e]} : \alpha^{p^e} x^{p^e})$ is not contained in any minimal prime. In their Remark 1.4, Hara and Yoshida note that if $\alpha = (f)$ is a principal ideal, then $I^{*\alpha} = (I^* : \alpha)$, an operation which we have already noted fails to be idempotent. (For a similarly-defined operation which actually *is* a closure operation, see [79].)

Consider the operation which sends each ideal I to its *unmixed part* I^{unm} [50]. This is defined by looking at the primary ideals (commonly called *components*) in an irredundant minimal primary decomposition of I, and then intersecting those components that have *maximum dimension*. Although the decomposition is not uniquely determined, the components of maximum dimension are, so this is a well-defined operation. Moreover, this operation is extensive (i) and idempotent (ii) (since all the components of I^{unm} already have the same dimension), but is *not order-preserving* in general. For an example, let $R = k[x, y]$ be a polynomial ring in two variables over a field k, and let $J := (x^2, xy)$ and $I := (x^2, xy, y^2)$. Then $J \subseteq I$, but $J^{\mathrm{unm}} = (x) \nsubseteq I^{\mathrm{unm}} = I$. Similar comments apply in the 3-variable case when $J = (xy, xz)$ and $I = (y, z)$.

For another extensive, idempotent operation which is not order-preserving, consider the "Ratliff–Rush closure" (or "Ratliff–Rush operation"), given in [65], defined on so-called *regular ideals* (where an ideal I of R is *regular* if it contains an R-regular element), defined by $\tilde{I} := \bigcup_{n=1}^{\infty} (I^{n+1} : I^n)$. In [30, 1.11] (resp. in [29, 1.1]), the domain $R := k[\![x^3, x^4]\!]$ (resp. $R := k[x, y]$) is given where k is any field and x, y indeterminates over k, along with nonzero ideals $J \subseteq I$ of R such that $\tilde{J} \nsubseteq \tilde{I}$.

Many of the topics and questions explored in this article could be applied to these not-quite-closure operations as well, but additional care is needed.

3 Constructing Closure Operations

There are, however, some actions one can take which always produce closure operations.

3.1 Standard Constructions

Construction 3.1.1. Let U be an R-module. Then the operation $I \mapsto I^{\mathrm{cl}} := \{f \in R \mid fU \subseteq IU\} = (IU :_R U)$ gives a closure operation on R. Extension and order-preservation are clear. As for idempotence, suppose $f \in (I^{\mathrm{cl}})^{\mathrm{cl}}$. Then $fU \subseteq I^{\mathrm{cl}}U$. But for any $g \in I^{\mathrm{cl}}$, $gU \subseteq IU$, whence $I^{\mathrm{cl}}U \subseteq IU$, so $fU \subseteq IU$ as required.

As we shall see, this is a very productive way to obtain closure operations, especially when U is an R-algebra. For example, letting $\mathfrak{a}$ be an ideal of R and $U := R/\mathfrak{a}$, we see that the assignment $I \mapsto I + \mathfrak{a}$ gives a closure operation. On the other hand, letting $U := \mathfrak{a}$, the resulting closure operation becomes $I \mapsto (I\mathfrak{a} : \mathfrak{a})$, which is the basis for the Δ-*closures* of [64] and for the *basically full closure* of [31].

Construction 3.1.2. We give here a variant on Construction 3.1.1.

Let $\phi : R \to S$ be a ring homomorphism and let d be a closure operation on S. For ideals I of R, define $I^{\mathrm{c}} := \phi^{-1}((\phi(I)S)^{\mathrm{d}})$. (One might loosely write $I^{\mathrm{c}} := (IS)^{\mathrm{d}} \cap R$.) Then c is a closure operation on R.

Extension and order-preservation are clear. As for idempotence, if $f \in (I^{\mathrm{c}})^{\mathrm{c}}$, then $\phi(f) \in ((I^{\mathrm{c}})S)^{\mathrm{d}} \subseteq ((IS)^{\mathrm{d}})^{\mathrm{d}} = (IS)^{\mathrm{d}}$, so that $f \in I^{\mathrm{c}}$.

Construction 3.1.3. Let $\{c_\lambda\}_{\lambda \in \Lambda}$ be an *arbitrary collection* of closure operations on ideals of R. Then $I^{\mathrm{c}} := \bigcap_{\lambda \in \Lambda} I^{c_\lambda}$ gives a closure operation as well.[2]

Again, extension and order-preservation are clear. As for idempotence, suppose $f \in (I^{\mathrm{c}})^{\mathrm{c}}$. Then for every $\lambda \in \Lambda$, we have $f \in (I^{\mathrm{c}})^{c_\lambda}$. But since $I^{\mathrm{c}} \subseteq I^{c_\lambda}$ and c_λ preserves order, we have

$$f \in (I^{\mathrm{c}})^{c_\lambda} \subseteq (I^{c_\lambda})^{c_\lambda} = I^{c_\lambda},$$

where the last property follows from the idempotence of c_λ. Since $\lambda \in \Lambda$ was chosen arbitrarily, $f \in I^{\mathrm{c}}$ as required.

For the next construction, we need to mention the natural partial order on closure operations on a ring R. Namely, if c and d are closure operations, we write c $\leq$ d if for every ideal I, $I^{\mathrm{c}} \subseteq I^{\mathrm{d}}$.

Construction 3.1.4. Let $\{c_\lambda\}_{\lambda \in \Lambda}$ be a *directed set* of closure operations. That is, for any $\lambda_1, \lambda_2 \in \Lambda$, there exists some $\mu \in \Lambda$ such that $c_{\lambda_i} \leq c_\mu$ for $i = 1, 2$. Moreover, assume that R is Noetherian. Then $I^{\mathrm{c}} := \bigcup_{\lambda \in \Lambda} I^{c_\lambda}$ gives a closure operation.

---

[2] Similar considerations in the context of star-operations on integral domains are used in [2] to give lattice structures on certain classes of closure operations.

First note that I^c is indeed an ideal. It is the sum $\sum_{\lambda \in \Lambda} I^{c\lambda}$. After this, extension and order-preservation are clear. Next, we note that for any ideal I, there is some $\mu \in \Lambda$ such that $I^c = I^{c\mu}$. To see this, we use the fact that I^c is finitely generated along with the directedness of the set $\{c_\lambda \mid \lambda \in \Lambda\}$. Namely, $I^c = (f_1, \ldots, f_n)$; each $f_i \in I^{c\lambda_i}$; then let c_μ be such that $c_{\lambda_i} \le c_\mu$ for $i = 1, \ldots, n$.

To show idempotence, take any ideal I. By what we just showed, there exist $\lambda_1, \lambda_2 \in \Lambda$ such that $(I^c)^c = (I^c)^{c\lambda_1}$ and $I^c = I^{c\lambda_2}$. Choose $\mu \in \Lambda$ such that $c_{\lambda_i} \le c_\mu$ for $i = 1, 2$. Then

$$(I^c)^c = (I^{c\lambda_2})^{c\lambda_1} \subseteq (I^{c\mu})^{c\mu} = I^{c\mu} \subseteq I^c.$$

Construction 3.1.5. Let d be an operation on (ideals of) R that satisfies properties (i) and (iii) of Definition 2.1.1, but is not idempotent. Let $\mathcal{S}$ be the set of all closure operations on R defined by the property that $c \in \mathcal{S}$ if and only if $I^d \subseteq I^c$ for all ideals I of R. Then by Construction 3.1.3, the assignment $I \mapsto I^{d^\infty} := \bigcap_{c \in \mathcal{S}} I^c$ is itself a closure operation, called the *idempotent hull* of d [15, Section 4.6]. It is obviously the smallest closure operation lying above d.

If R is Noetherian, it is equivalent to do the following: Let $d^1 := d$, and for each integer $n \ge 2$, we inductively define d^n by setting $I^{d^n} := (I^{d^{n-1}})^d$. Let $I^{d'} := \bigcup_n I^{d^n}$ for all I. One may routinely check that d' is an extensive, order-preserving operation on ideals of R, and idempotence follows from the ascending chain condition on the ideals $\{I^{d^n}\}_{n \in \mathbb{N}}$. Clearly, $I^{d'} = I^{d^\infty}$.

Construction 3.1.6. This construction is only relevant when R is not necessarily Noetherian.

Let c be a closure operation. Then we define c_f by setting

$$I^{c_f} := \bigcup \{J^c \mid J \text{ a finitely generated ideal such that } J \subseteq I\}.$$

This is a closure operation: Extension follows from looking at the principal ideals (x) for all $x \in I$. Order-preservation is obvious. As for idempotence, suppose $z \in (I^{c_f})^{c_f}$. Then there is some finitely generated ideal $J \subseteq I^{c_f}$ such that $z \in J^c$. Let $\{z_1, \ldots, z_n\}$ be a finite generating set for J. Since each $z_i \in I^{c_f}$, there exist finitely generated ideals $K_i \subseteq I$ such that $z_i \in K_i^c$. Now let $K := \sum_{i=1}^n K_i$. Then $J \subseteq K^c$, so that

$$z \in J^c \subseteq (K^c)^c = K^c,$$

and since K is a finitely generated sub-ideal of I, it follows that $z \in I^{c_f}$.

If $c = c_f$, we say that c is of *finite type*. Clearly c_f is of finite type for any closure operation c, and it is the largest finite-type closure operation d such that $d \le c$. Connected with this, we have the following:

Proposition 3.1.7. *Let* c *be a closure operation of finite type on* R. *Then every* c-*closed ideal is contained in a* c-*closed ideal that is maximal among* c-*closed ideals.*

The proof is a standard Zorn's lemma argument. The point is that the union of a chain of c-closed ideals is c-closed because c is of finite type.

3.2 Common Closures as Iterations of Standard Constructions

Here we will show that essentially all the closures we gave in Example 2.1.2 result as iterations of the constructions just given:

  (i) The *identity* needs no particular construction.

 (ii) The *indiscrete closure* is an example of Construction 3.1.1, by letting $U = 0$.

(iii) As for the *radical*, we use the characterization of it being the intersection of the prime ideals that contain the ideal. Consider the maps $\pi_{\mathfrak{p}} : R \to R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} =: \kappa(\mathfrak{p})$ for prime ideals $\mathfrak{p}$. Note that

$$\pi_{\mathfrak{p}}^{-1}(I\kappa(\mathfrak{p})) = \begin{cases} \mathfrak{p}, & \text{if } I \subseteq \mathfrak{p}, \\ R, & \text{otherwise.} \end{cases}$$

Let $I^{\mathfrak{p}} := \pi_{\mathfrak{p}}^{-1}(I\kappa(\mathfrak{p}))$. This is an instance of Construction 3.1.1 with $U = \kappa(\mathfrak{p})$, and the intersection of all such closures (Construction 3.1.3) is the radical. That is, $\sqrt{I} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} I^{\mathfrak{p}}$.

 (iv) The $\mathfrak{a}$-*saturation* may be obtained in one of two ways. Assuming one already has the extensive, order-preserving operation $(- : \mathfrak{a})$, then applying Construction 3.1.5 yields the $\mathfrak{a}$-saturation.

Alternately, let $\{a_{\lambda} \mid \lambda \in \Lambda\}$ be a generating set for $\mathfrak{a}$, with each $a_{\lambda} \neq 0$. Let $\ell_{\lambda} : R \to R_{a_{\lambda}}$ be the localization map. Then each $(I : a_{\lambda}^{\infty}) = \ell_{\lambda}^{-1}(IR_{a_{\lambda}}) =: I^{\lambda}$ is an instance of Construction 3.1.1 (or 3.1.2, if you like), and we may apply Construction 3.1.3 to get $(I : \mathfrak{a}^{\infty}) = \bigcap_{\lambda \in \Lambda}(I : a_{\lambda}^{\infty}) = \bigcap_{\lambda \in \Lambda} I^{\lambda}$.

  (v) For *integral closure*, let $\mathfrak{p}$ be a minimal prime of R, let V be a valuation ring (or if $R/\mathfrak{p}$ is Noetherian, it's enough to let V be a rank 1 discrete valuation ring) between $R/\mathfrak{p}$ and its fraction field, let $j_V : R \to V$ be the natural map, and let $I^V := j_V^{-1}(IV)$ (which gives a closure operation via Construction 3.1.1 with $U = V$). Then it is a theorem (e.g. [51, Theorem 6.8.3]) that $I^- = \bigcap_{\text{all such } V} I^V$, which is an application of Construction 3.1.3.

 (vi) For *plus closure*, *when R is an integral domain*, let Q be its fraction field, $\overline{Q}$ an algebraic closure of Q, and let R^+ be the integral closure of R in $\overline{Q}$. That is, R^+ consists of all elements of $\overline{Q}$ that satisfy a *monic* polynomial over R. Then we let $I^+ := IR^+ \cap R$, by way of Construction 3.1.1 with $U = R^+$.

In the general case, where R is not necessarily a domain, for each minimal prime $\mathfrak{p}$ of R we let $\pi_{\mathfrak{p}} : R \to R/\mathfrak{p}$ be the natural surjection. Then $I^+ := \bigcap_{\text{all such } \mathfrak{p}} \pi_{\mathfrak{p}}^{-1}((IR/\mathfrak{p})^+)$, via Construction 3.1.2.

(vii) For *Frobenius closure* (when R has positive prime characteristic p), we introduce the left R-modules ${}^e R$ for all $e \in \mathbb{N}$. ${}^e R$ has the same additive group structure as R (with elements being denoted ${}^e r$ for each $r \in R$), and R-module structure given as follows: For $a \in R$ and ${}^e r \in {}^e R$, $a \cdot {}^e r = {}^e (a^{p^e} r)$. Let $f_e : R \to {}^e R$ be the R-module map given by $a \mapsto a \cdot {}^e 1 = {}^e(a^{p^e})$. Let F_e be the closure operation given by $I^{F_e} := f_e^{-1}(I \cdot {}^e R)$, via Construction 3.1.1. Note that this is a *totally ordered set* (and hence a directed set) of closure operations, in that $F_e \leq F_{e+1}$ for all e, due to the R-module maps ${}^e R \to {}^{e+1} R$ given by ${}^e r \mapsto {}^{e+1}(r^p)$. Thus, we may use Construction 3.1.4 to get $I^F := \bigcup_{e \in \mathbb{N}} I^{F_e}$.

(viii) For *tight closure* (when R has positive prime characteristic p), we cannot use these constructions directly. However, recall the theorem [37, Theorem 8.6] that under quite mild assumptions on R (namely the same ones that guarantee persistence of tight closure, see 4.3), $I^* = I^\star$, and use the constructions for solid closure below.

(ix) For *solid closure* (when R is a complete local domain), letting $i_S : R \to S$ for solid R-algebras S and $I^S := i_S^{-1}(IS)$ by way of Construction 3.1.1 with $U = S$, we note that this is a directed set of closure operations, since [37, Proposition 2.1a] if S and T are solid R-algebras, so is $S \otimes_R T$. Thus, we have $I^\star = \bigcup_{\text{all such } i_S} I^S$ via Construction 3.1.4.

For general R: Let $\mathfrak{m}$ be a maximal ideal of R, $\widehat{R}^{\mathfrak{m}}$ the completion of $R_{\mathfrak{m}}$ at its maximal ideal, $\mathfrak{p}$ a minimal prime of $\widehat{R}^{\mathfrak{m}}$, and $u_{\mathfrak{m},\mathfrak{p}} : R \to \widehat{R}^{\mathfrak{m}}/\mathfrak{p}$ the natural map. Then we use Constructions 3.1.3 and 3.1.2 to get $I^\star := \bigcap_{\text{all such pairs } \mathfrak{m},\mathfrak{p}} u_{\mathfrak{m},\mathfrak{p}}^{-1}((I\widehat{R}^{\mathfrak{m}}/\mathfrak{p})^\star)$.

(x) For Δ-*closure*, first note that for any ideal $K \in \Delta$, $I^K := (IK : K)$ gives a closure operation via Construction 3.1.1 with $U = K$. Next, note that the closure operations $\{(-)^K \mid K \in \Delta\}$ form a *directed set*, since for any $H, K \in \Delta$, $I^H + I^K \subseteq I^{KH}$. Thus, Construction 3.1.4 applies to give $I^\Delta := \bigcup_{K \in \Delta} I^K$.

(xi) For *basically full closure*, we merely apply Construction 3.1.1 with $U = \mathfrak{m}$.

4 Properties of Closures

4.1 Star-, Semi-prime, and Prime Operations

Definition 4.1.1. Let cl be a closure operation for a ring R. We say that cl is

(i) *semi-prime* [63] if for all ideals I, J of R, we have $I \cdot J^{\text{cl}} \subseteq (IJ)^{\text{cl}}$. (Equivalently, $(I^{\text{cl}} J^{\text{cl}})^{\text{cl}} = (IJ)^{\text{cl}}$ for all I, J.)

(ii) a *star-operation* [25, Chapter 32 and see below] if for every ideal J and every non-zerodivisor x of R, $(xJ)^{\text{cl}} = x \cdot (J^{\text{cl}})$.

(iii) *prime* [55, 56, 64] if it is a semi-prime star-operation.

Sociological Comment. In the literature of so-called "multiplicative ideal theory" (which is, roughly, that branch of commutative algebra that uses [25] as its basic textbook), the definition of *star-operation* is somewhat different from the above. Namely, one assumes first that R is an integral domain, one defines star-operations on *fractional ideals of R*. However, when R is a domain, it is equivalent to do as I have done above. Moreover, the terminology of star-operations is different from the terminology of this article. For instance, if c is a star-operation on a domain R, then I^c is not called the c-closure, but rather the c-*envelope* (or sometimes c-*image*) of I, and if $I = I^c$, then I is said to be a c-*ideal*. For the sake of self-containedness, I have elected rather to use the terminology I was raised on.

The field of closure operations on Noetherian rings has remained nearly disjoint from the field of star- (and "semistar-") operations on integral domains. I think this is largely because the two groups of people have historically been interested in very different problems and baseline assumptions. Multiplicative ideal theorists do not like to assume their rings are Noetherian, for example. But I feel it would save a good deal of energy if the two fields would come together to some extent. After all, there are very reasonable assumptions under which tight, integral, plus, and Frobenius closures are prime- (and hence star-) operations (see below). This provides the star-operation theorists with a fresh infusion of star-operations to study, and it provides those who study said closures with a fresh arsenal of tools with which to study them.

I take the point of view natural to one of my training, in which one generalizes from integral domains to general commutative rings.

First note the following:

Lemma 4.1.2. *Let* cl *be a closure operation on a ring R.*

(i) cl *is a semi-prime operation if and only if for all $x \in R$ and ideals $J \subseteq R$, we have $x \cdot J^{cl} \subseteq (xJ)^{cl}$.*

(ii) *If R is an integral domain, then* cl *is a star-operation if and only if it is prime.*

Proof. If cl is a semi-prime operation, then for any $x \in R$ and ideal $J \subseteq R$, we have

$$x \cdot J^{cl} = (x) \cdot J^{cl} \subseteq ((x)J)^{cl} = (xJ)^{cl}.$$

Conversely, suppose $xJ^{cl} \subseteq (xJ)^{cl}$ for all x and J. Let I be an ideal of R, and let $\{a_\lambda\}_{\lambda \in \Lambda}$ be a generating set for I. Then

$$I \cdot J^{cl} = \sum_{\lambda \in \Lambda} a_\lambda \cdot J^{cl} \subseteq \sum_{\lambda} (a_\lambda J)^{cl} \subseteq \left(\sum_{\lambda} a_\lambda J \right)^{cl} = (IJ)^{cl},$$

so that cl is semi-prime.

Now suppose R is an integral domain. By definition any prime operation must be a star-operation. So let cl be a star-operation on R. To see that it is semi-prime,

we use part (i). For any $x \in R$, either $x = 0$ or x is a non-zerodivisor. Clearly $0 \cdot J^{\mathrm{cl}} = 0 \subseteq 0^{\mathrm{cl}} = (0J)^{\mathrm{cl}}$. And if x is a non-zerodivisor, then $x \cdot J^{\mathrm{cl}} = (xJ)^{\mathrm{cl}}$ by definition of star-operation. $\qquad \square$

One reason why the star-operation property is useful is as follows: any star-operation admits a unique extension to the set of fractional ideals of R (where a *fractional ideal* is defined to be a submodule M of Q, the total quotient ring of R, such that for some non-zerodivisor f of R, $fM \subseteq R$). Namely, if cl is a star-operation and M is a fractional ideal, an element $x \in Q$ is in M^{cl} if $fx \in (fM)^{\mathrm{cl}}$, where f is a non-zerodivisor of R such that $fM \subseteq R$. After this observation, another important property of star-operations is that if two fractional ideals M, N are isomorphic, their closures are isomorphic as well.

Star-operations are important in the study of so-called *Kronecker function rings* (for a historical and topical overview of this connection, see [23]). However, the star-operation property is somewhat limiting. For instance, I leave it as an exercise for the reader to show that if R is a local Noetherian ring, then the radical operation on R is a star-operation if and only if depth $R = 0$. The only star-operation on a rank 1 discrete valuation ring is the identity. On the other hand, it is well known that integral closure is a star-operation on R if and only if R is normal. This is true of tight closure as well:

Proposition 4.1.3. *Consider the following property for a closure operation* cl*:*

$$\text{For any non-zerodivisor } x \in R \text{ and any ideal } I, \ I^{\mathrm{cl}} = ((xI)^{\mathrm{cl}} : x). \qquad (\#)$$

(i) *A closure operation* cl *is a star-operation if and only if it satisfies* (#) *and* $(x)^{\mathrm{cl}} = (x)$ *for all non-zerodivisors* $x \in R$.

(ii) *Closure operations that satisfy* (#) *include plus-closure (when R is a domain), integral closure, tight closure (in characteristic $p > 0$), and Frobenius closure.*

Proof. (i) Suppose cl is a star-operation, x is a non-zerodivisor, and I an ideal. Then $(x)^{\mathrm{cl}} = ((x)R)^{\mathrm{cl}} = x \cdot R^{\mathrm{cl}} = (x)$, and $((xI)^{\mathrm{cl}} : x) = (x(I^{\mathrm{cl}}) : x)$ (since cl is a star-operation) $= I^{\mathrm{cl}}$ (since x is a non-zerodivisor).

Conversely, suppose cl satisfies (#) and that all principal ideals generated by non-zerodivisors are cl-closed. For a non-zerodivisor x and ideal I, we have $x \cdot I^{\mathrm{cl}} = x \cdot ((xI)^{\mathrm{cl}} : x) \subseteq (xI)^{\mathrm{cl}}$, so we need only show that $(xI)^{\mathrm{cl}} \subseteq x \cdot I^{\mathrm{cl}}$. So suppose $g \in (xI)^{\mathrm{cl}}$. Since $xI \subseteq (x)$, it follows that $g \in (x)^{\mathrm{cl}} = (x)$, so $g = xf$ for some $f \in R$. Thus, $xf \in (xI)^{\mathrm{cl}}$, so $f \in ((xI)^{\mathrm{cl}} : x) = I^{\mathrm{cl}}$, whence $g = xf \in x \cdot I^{\mathrm{cl}}$ as required.

(ii) (Frobenius closure): Let $g \in ((xI)^F : x)$. Then $xg \in (xI)^F$, so there is some $q = p^n$ such that

$$x^q g^q = (xg)^q \in (xI)^{[q]} = x^q I^{[q]}.$$

Since x^q is a non-zerodivisor, $g^q \in I^{[q]}$, whence $g \in I^F$.

(Tight closure): The proof is similar to the Frobenius closure case.

(Plus closure): If $xg \in (xI)^+$, then there is some module-finite domain extension $R \subseteq S$ such that $xg \in xIS$. But since x is a non-zero element of the domain S (hence a non-zerodivisor on S), it follows that $g \in IS$, whence $g \in I^+$.

(Integral closure): Suppose $xg \in (xI)^-$. Then there is some $n \in \mathbb{N}$ and elements $a_i \in (xI)^i$ ($1 \leq i \leq n$) such that

$$(xg)^n + \sum_{i=1}^n a_i (xg)^{n-i} = 0.$$

But each $a_i \in (xI)^i = x^i I^i$, so for some $b_i \in I^i$ (for each i), we have $a_i = x^i b_i$. Then the displayed equation yields:

$$x^n \left(g^n + \sum_{i=1}^n b_i g^{n-i} \right) = 0,$$

and since x^n is a non-zerodivisor, it follows that $g \in I^-$. □

Semi-prime operations, however, are ubiquitous. (In fact, some authors [54] even include the property in their basic definition of what a closure operation is!) One can, of course, cook up a non-semi-prime closure operation, even on a rank 1 discrete valuation ring [75, Example 2.3]. However, *essentially all the examples and constructions explored so far yield semi-prime operations*, in the following sense (noting that all of the following statements have easy proofs):

- Any closure arising from Construction 3.1.1 is semi-prime.
- In Construction 3.1.2, if d is a semi-prime operation on S, then c is a semi-prime operation on R.
- In Construction 3.1.3, if every c_λ is semi-prime, then so is c.
- In Construction 3.1.4, if every c_λ is semi-prime, then so is c.
- In Construction 3.1.5, if $I \cdot J^d \subseteq (IJ)^d$ for all ideals I, J of R, then d^∞ is semi-prime.
- In Construction 3.1.6, if c is semi-prime, then so is c_f.
- Hence by 3.2, all of the closures from Example 2.1.2 are semi-prime.[3]

Here are some nice properties of semi-prime closure operations:

Proposition 4.1.4. *Let* cl *be a semi-prime closure operation on R. Let I, J be ideals of R, and W a multiplicatively closed subset of R.*

(i) *$(I : J)^{\text{cl}} \subseteq (I^{\text{cl}} : J)$. Hence if I is cl-closed, then so is $(I : J)$.*

(ii) *$(I^{\text{cl}} : J)$ is cl-closed.*

---

[3] One need not go through solid closure to show that tight closure must always be semi-prime.

(iii) *If R is Noetherian and I is* cl-*closed, then* $(I W^{-1} R) \cap R$ *is* cl-*closed.*

(iv) *If R is Noetherian and I is* cl-*closed, then all the* minimal primary components *of I are* cl-*closed. Hence, if $I = I^{\mathrm{cl}}$ has no embedded components, it has a primary decomposition by* cl-closed *ideals.*

 (v) *The maximal elements of the set* $\{I \mid I^{\mathrm{cl}} = I \neq R\}$ *are prime ideals.*

Proof. (i) Let $f \in (I : J)^{\mathrm{cl}}$. Then $Jf \subseteq J(I : J)^{\mathrm{cl}} \subseteq (J \cdot (I : J))^{\mathrm{cl}} \subseteq I^{\mathrm{cl}}$.
   (ii) follows directly from part (i).
   (iii) Let $J := (I W^{-1} R) \cap R$. Then $J = \{f \in R \mid \exists w \in W \text{ such that } wf \in I\}$. But J is finitely generated (since R is Noetherian); say $J = (f_1, \ldots, f_n)$. Then for each $1 \le i \le n$, there exists $w_i \in W$ such that $w_i f_i \in I$. Let $w := \prod_{i=1}^{n} w_i$. Then $wJ \subseteq I$, so $J \subseteq (I : w)$. But it is obvious that $(I : w) \subseteq J$, so $J = (I : w)$. Then the conclusion follows from part (i).
   (iv) The minimal primary components of I look like $I R_P \cap R$, for each minimal prime P over I. Then the conclusion follows from part (iii).
   (v) Let I be such a maximal element. Let $x, y \in R$ such that $xy \in I$ and $y \notin I$. Then $(I : x)$ is a cl-closed ideal (by part (i)) that properly contains I (since $y \in (I : x) \setminus I$), so since I is maximal among proper cl-closed ideals, it follows that $(I : x) = R$, which means that $x \in I$. □

Finally, here is a construction on semi-prime operations:

Construction 4.1.5. Let c be a semi-prime closure operation on R. Let c_f-Max R (see Construction 3.1.6 for the definition of c_f) denote the set of c_f-closed ideals which are maximal among the set of all c_f-closed ideals. By Proposition 4.1.4 (v), c_f-Max R consists of prime ideals, and by Proposition 3.1.7, every c_f-closed ideal is contained in a member of c_f-Max R. Then we define c_w as follows:

$$I^{c_w} := \{x \in R \mid \forall \mathfrak{p} \in c_f\text{-Max } R, \ \exists d \in R \setminus \mathfrak{p} \text{ such that } dx \in I\}.$$

In other words, I^{c_w} consists of all the elements of R that land in the extension of I to all localizations $R \to R_{\mathfrak{p}}$ for $\mathfrak{p} \in c_f$-Max R. As this arises from Constructions 3.1.1 and 3.1.3, c_w is a semi-prime closure operation.

   Moreover, $c_w \le c_f$. To see this, let $x \in I^{c_w}$. Then for all $\mathfrak{p} \in c_f$-Max R, there exists $d_{\mathfrak{p}} \in R \setminus \mathfrak{p}$ with $d_{\mathfrak{p}} x \in I$. Let J be the ideal generated by the set $\{d_{\mathfrak{p}} \mid \mathfrak{p} \in c_f\text{-Max } R\}$. Then $J x \subseteq I$ and $J^{c_f} = R$, so since c_f is semi-prime, we have

$$x = 1 \cdot x \in R(x) = J^{c_f}(x) \subseteq (J x)^{c_f} \subseteq I^{c_f}.$$

If R is a domain, and c is a star-operation (i.e. prime), then this construction is essentially due to [3], who show that in this context c_w distributes over finite intersections, is of finite type, and is the *largest* star-operation d of finite type that distributes over finite intersection such that d $\le$ c.

The v-operation

Arguably the most important star-operation (at least in the theory of star-operations *per se*) is the so-called v-operation. Classically it was only defined when R is a domain [25, Chapters 16, 32, 34], but it works in general. Most star-operations in the literature (among those that are identified as star-operations) are based in one way or another on the v-operation:

Definition 4.1.6. Let R be a ring and Q its total quotient ring. For an ideal I, the set I_v is defined to be the intersection of all cyclic R-submodules M of Q such that $I \subseteq M$.

Proposition 4.1.7. (i) v *is a star-operation.*

(ii) *For any star-operation* cl *on R, $I^{cl} \subseteq I_v$ for all ideals I of R. (That is, v is the largest star-operation on R.)*

(iii) *There exists a ring R for which* v *is* not *semi-prime (and hence not prime).*

Proof. It is easy to see that v is a closure operation. For the star-operation property, let x be a non-zerodivisor and I an ideal of R. Let $a \in I_v$. Let M be a cyclic submodule of Q that contains xI. Then $M = R \cdot \frac{r}{s}$ for some $r, s \in R$ with s a non-zerodivisor. Moreover, $xI \subseteq M$ implies that $I \subseteq R \cdot \frac{r}{sx}$. Since $a \in I_v$, we have $a \in R \cdot \frac{r}{sx}$ as well, so that $xa \in R \cdot \frac{r}{s} = M$. Thus, $xa \in (xI)_v$ as required.

For the opposite inclusion, we first note that principal ideals are v-closed because they are cyclic R-submodules of Q. Now let $a \in (xI)_v$. Since $xI \subseteq (x)$, we have $a \in (xI)_v \subseteq (x)_v = (x)$, so $a = xb$ for some $b \in R$. Let $M = R \cdot \frac{r}{s}$ be a cyclic submodule of Q that contains I. Then $xI \subseteq xM = R \cdot \frac{xr}{s}$, so since $a \in (xI)_v$, it follows that $xb = a \in xM = R \cdot \frac{xr}{s} = x \cdot R \cdot \frac{r}{s}$. Since x is a non-zerodivisor on Q, we can cancel it to get $b \in R \cdot \frac{r}{s} = M$, whence $b \in I_v$. Thus, $a = xb \in x \cdot I_v$, as required.

Now let cl be an arbitrary star-operation on R, and I an ideal. Let $M = R \cdot \frac{r}{s}$ be a cyclic submodule of R that contains I (so that $r, s \in R$ and s is not a zerodivisor). Then $sI \subseteq rR = (r)$, so that

$$s \cdot I^{cl} = (sI)^{cl} \subseteq (r)^{cl} = (r).$$

That is, $I^{cl} \subseteq R \cdot \frac{r}{s} = M$. Thus, $I^{cl} \subseteq I_v$.

For the counterexample, let

$$R := k[X, Y]/(X^2, XY, Y^2) = k[x, y],$$

where k is a field and X, Y are indeterminates over k (with the images in R denoted x, y respectively). Let $\mathfrak{m} := (x, y)$ be the unique maximal ideal of R. Since R is an Artinian local ring, it is equal to its own total ring of quotients, and so the cyclic R-submodules of said ring of quotients are just the principal ideals of R. Since $\mathfrak{m}$ is not contained in any proper principal ideal of R, we have $\mathfrak{m}_v = R$. Thus, $\mathfrak{m} \cdot \mathfrak{m}_v =$

$\mathfrak{m} \cdot R = \mathfrak{m}$. On the other hand, $(\mathfrak{m}\mathfrak{m})_v = (\mathfrak{m}^2)_v = 0_v = 0$, which shows that $\mathfrak{m} \cdot \mathfrak{m}_v \nsubseteq (\mathfrak{m}\mathfrak{m})_v$, whence v is not semi-prime. $\qquad\qquad\qquad\qquad\qquad \square$

Remark 4.1.8. When R is an integral domain, parts (i) and (ii) of the above Proposition are well known (and since by Lemma 4.1.2, any star-operation on a domain is prime, the analogue of (iii) is false). Two other well-known properties of the v-operation in the domain case are as follows:

- $\mathrm{Hom}_R(\mathrm{Hom}_R(I, R), R) \cong I_v$ as R-modules. For this reason, the v-operation is sometimes also called the *reflexive hull* operation on ideals.

- $I_v = (I^{-1})^{-1}$. (Recall that for a fractional ideal J of R, $J^{-1} := \{x \in Q \mid xJ \subseteq R\}$, where Q is the quotient field of R.) For this reason, the v-operation is sometimes also called the *divisorial closure*.

These ideas have obvious connections to Picard groups and divisor class groups.

The t- and w-operations (see e.g. [80]) should be mentioned here as well. By definition, t := v_f (via Construction 3.1.6). When R is a domain, the w-operation is defined by w := v_w (by Construction 4.1.5). So if R is a domain, then t is semi-prime, but otherwise it need not be (as the counterexample in Proposition 4.1.7 shows), and w may not even be well-defined in the non-domain case.

4.2 Closures Defined by Properties of (Generic) Forcing Algebras

Let R be a ring, I a (finitely generated) ideal and $f \in R$. Then a *forcing algebra* [37] for $[I; f]$ consists of an R-algebra A such that (the image of) $f \in IA$. In particular, given a generating set $I = (f_1, \ldots, f_n)$, one may construct the *generic forcing algebra A* for the data $[f_1, \ldots, f_n; f]$, given by

$$A := R[T_1, \ldots, T_n] \Big/ \Big(f + \sum_{i=1}^{n} f_i T_i \Big).$$

Clearly A is a forcing algebra for $[I; f]$. Moreover, if B is any other forcing algebra for $[I; f]$, there is an R-algebra map $A \to B$. To see this, if $f \in IB$, then there exist $b_1, \ldots, b_n \in B$ such that $f + \sum_{i=1}^{n} f_i b_i = 0$. Then we define the map $A \to B$ by sending each $T_i \mapsto b_i$.

Many closure operations may be characterized by properties of generic forcing algebras. This viewpoint is explored in some detail in [9], where connections are also made with so-called *Grothendieck topologies*. We list a few (taken from [9]), letting $f, I := (f_1, \ldots, f_n)$, and A be as above:

- $f \in I$ (the identity closure of I) if and only if R is a forcing algebra for $[f; I]$. That is, $f \in I$ if and only if there is an R-algebra map $A \to R$. In geometric terms, one says that the structure map Spec $A \to$ Spec R has a *section*.

- $f \in \sqrt{I}$ if and only if $f \in IK$ for all fields K that are R-algebras, if and only if the ring map $R \to A$ has the *lying-over* property, if and only if the map Spec $A \to$ Spec R is *surjective* (as a set map).

- $f \in I^-$ if and only if $f \in IV$ for all rank-1 discrete valuations of R (appropriately defined), if and only if for all such V, there is an R-algebra map $A \to V$. It is not immediately obvious, but this is equivalent to the topological property that the map Spec $A \to$ Spec R is *universally submersive* (also called a *universal topological epimorphism*).

- If R has prime characteristic $p > 0$, $f \in I^F$ if and only if $f \in IR_\infty$, if and only if there is an R-algebra map $A \to R_\infty$.

The final closure to note in this context is solid closure (the connection of which to tight closure has already been noted). For simplicity, let $(R, \mathfrak{m})$ be a complete local domain of dimension d. We have $f \in I^\star$ if and only if there is some solid R-algebra S such that $f \in IS$, i.e. iff there is an R-algebra map $A \to S$. Hochster [37, Corollary 2.4] showed in turn that this is equivalent to the condition that $H^d_\mathfrak{m}(A) \neq 0$. (!) This viewpoint brings in all sorts of cohomological tools into the study of solid closure, and hence tight closure in characteristic p. Such tools were crucial in the proof that tight closure does not always commute with localization [10].

4.3 Persistence

Although it is possible to do so, usually one does not define a closure operation one ring at a time. The more common thing to do is define the closure operation for a whole class of rings. In such cases, the most important closure operations are *persistent*:

Definition 4.3.1. Let $\mathcal{R}$ be a subcategory of the category of commutative rings; let c be a closure operation defined on the rings of $\mathcal{R}$. We say that c is *persistent* if for any ring homomorphism $\phi : R \to S$ in $\mathcal{R}$ and any ideal I of R, one has $\phi(I^c)S \subseteq (\phi(I)S)^c$.

Common choices for $\mathcal{R}$ are

- All rings and ring homomorphisms.
- Any full subcategory of the category of rings.
- Graded rings and graded homomorphisms.
- Local rings and local homomorphisms.

For instance, it is easy to show that radical and integral closure are persistent on the category of all rings (as are the identity and indiscrete closures), and that Frobenius closure is persistent on characteristic p rings. Tight closure is persistent along maps $R \to S$ of characteristic p rings, as long as either $R/\sqrt{0}$ is F-finite or R is essentially of finite type over an excellent local ring, although this is truly a deep theorem [44]. On the other hand, tight closure is persistent on the category of equal characteristic 0

rings because of the way it is defined (see the discussion after Theorem 4.5.1). Saturation (with respect to the maximal ideal) is persistent on the category of local rings and local homomorphisms, as well as on the category of graded rings and graded homomorphisms over a fixed base field.

Plus closure is also persistent on the category of integral domains, as is evident from the fact that the operation of taking absolute integral closure of the domains involved is *weakly functorial*, in the sense that any such map $R \to S$ extends (not necessarily uniquely) to a map $R^+ \to S^+$ [42, p. 139]. This argument may be extended to show that plus closure is persistent on the category of *all* rings as well, by considering minimal primes.

Basically full closure, however, is not persistent, even if we restrict to complete local rings of dimension one, $\mathfrak{m}$-primary ideals, and local homomorphisms $R \to S$ such that S becomes a finite R-module. For a counterexample, let k be any field, let x, y, z be analytic indeterminates over k, let $R := k[[x, y]]/(x^2, xy)$, $I := yR$, $S := k[[x, y, z]]/(x^2, xy, z^2)$, and let the map $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ be the obvious inclusion. Then $I^{\mathrm{bf}} = (\mathfrak{m}y :_R \mathfrak{m}) = (x, y)$ because x is killed by all of $\mathfrak{m}$. But $x \notin (IS)^{\mathrm{bf}} = (\mathfrak{n}y :_S \mathfrak{n})$ because $zx \in \mathfrak{n}x \setminus \mathfrak{n}y$. (Indeed, IS is a basically full ideal of S.)

4.4 Axioms Related to the Homological Conjectures

A treatment of closure operations would not be complete without mentioning the so-called "homological conjectures" (for which we assume all rings are Noetherian). So named by Mel Hochster, these comprise a complex list of reasonable-sounding statements that have been central to research in commutative algebra since the 1970s. For the original treatment, see [35]. For a more modern treatment, see [39]. Rather than trying to cover the topic comprehensively, consider the following two conjectures:

Conjecture 4.4.1 (Direct Summand Conjecture). *Let $R \to S$ be an injective ring homomorphism, where R is a regular local ring, such that S is module-finite over R. Then R is a direct summand of S, considered as R-modules.*

Conjecture 4.4.2 (Cohen–Macaulayness of Direct Summands conjecture). *Let $A \to R$ be a ring homomorphism which makes A a direct summand of R, and suppose R is regular. Then A is Cohen–Macaulay.*

Assuming a "sufficiently good" closure operation in mixed characteristic, these conjectures would be theorems. Indeed, they *are* theorems in equal characteristic, a fact which can be seen as a consequence of the existence of tight closure, as discussed in Section 4.5 (although the proof in equal characteristic of Conjecture 4.4.1 predated tight closure by some 15 years [34], as did a proof of some special cases of Conjecture 4.4.2 that come from invariant theory [46]).

Consider the following axioms for a closure operation cl on a category $\mathcal{R}$ of Noetherian rings:

(i) (Persistence) For ring maps $R \to S$ in $\mathcal{R}$, we have $I^{\mathrm{cl}}S \subseteq (IS)^{\mathrm{cl}}$.

(ii) (Tightness) If R is a regular ring in $\mathcal{R}$, then $I^{\mathrm{cl}} = I$ for all ideals I of R.

(iii) (Plus-capturing) If $R \to S$ is a module-finite extensions of integral domains in $\mathcal{R}$ and I is any ideal of R, then $IS \cap R \subseteq I^{\mathrm{cl}}$. (i.e. $I^{+} \subseteq I^{\mathrm{cl}}$)

(iv) (Colon-capturing) Let R be a *local* ring in $\mathcal{R}$ and $x_1, \ldots, x_d$ a system of parameters. Then for all $0 \le i \le d - 1$, $(x_1, \ldots, x_i) : x_{i+1} \subseteq (x_1, \ldots, x_i)^{\mathrm{cl}}$.

Notation. Let $d \in \mathbb{N}$, and let a, b be numbers such that either $a = b$ is a rational prime number, $a = b = 0$, or $a = 0$ and b is a rational prime number. For any such triple (d, a, b), let $\mathcal{R}_{d,a,b}$ be the category of complete local domains $(R, \mathfrak{m})$ such that $\dim R = d$, $\operatorname{char} R = a$, and $\operatorname{char}(R/\mathfrak{m}) = b$.

Proposition 4.4.3. *Let (d, a, b) be a triple as above.*

Suppose a closure operation cl *exists on the category $\mathcal{R}_{d,a,b}$ that satisfies conditions* (i)*,* (ii)*, and* (iii) *above. Then the Direct Summand Conjecture holds in the category $\mathcal{R}_{d,a,b}$.*

Proof. Let $R \to S$ be a module-finite injective ring homomorphism in $\mathcal{R}_{d,a,b}$, where R is a regular local ring. Let I be any ideal of R. Then $I \subseteq IS \cap R \subseteq I^{\mathrm{cl}} = I$ by properties (iii) and (ii). That is, $R \to S$ is *cyclically pure*. But then by [36], since R is a Noetherian domain it follows that $R \to S$ is *pure*. Since S is module-finite over R, it follows that R is a direct summand of S [47, Corollary 5.3]. ☐

Proposition 4.4.4. *Let (d, a, b) be as above.*

Suppose a closure operation cl *exists on the category $\mathcal{R}_{d,a,b}$ that satisfies conditions* (i)*,* (ii)*, and* (iv) *above. Then Conjecture* 4.4.2 *holds in the category $\mathcal{R}_{d,a,b}$.*

Proof. Let $A \to R$ be a local ring homomorphism of Noetherian local rings such that A is a direct summand of R, and suppose R is regular. Let $x_1, \ldots, x_d$ be a system of parameters for A, and pick some $0 \le i < d$. Then

$$(x_1, \ldots, x_i) : x_{i+1} \subseteq (x_1, \ldots, x_i)^{\mathrm{cl}} \subseteq (x_1, \ldots, x_i)^{\mathrm{cl}} R \cap A$$

$$\subseteq ((x_1, \ldots, x_i)R)^{\mathrm{cl}} \cap A = (x_1, \ldots, x_i)R \cap A = (x_1, \ldots, x_i).$$

Thus, A is Cohen–Macaulay. ☐

Remark 4.4.5. These ideas are closely related to Hochster's *big Cohen–Macaulay modules* conjecture. Indeed, Conjecture 4.4.1 holds when R has a so-called 'big Cohen–Macaulay module' (see e.g. [39, the final remark of §4]). When R is a complete local domain, Dietz [14] has given axioms for a persistent, residual closure operation on *R-modules* (see Section 7 for the basics on module closures) that are equivalent to the existence of a big Cohen–Macaulay module over R.

4.5 Tight Closure and Its Imitators

Tight closure has been used, among other things, to carry out the program laid out in Section 4.4 in cases where the ring contains a field. Indeed, we have the following:

Theorem 4.5.1 ([41, 45]). *Consider the category* $\mathcal{R} := \mathcal{R}_{d,p,p}$*, where* d *is any nonnegative integer and* $p \geq 0$ *is either a prime number or zero. Then we have*

(i) *(Persistence) For ring maps* $R \to S$ *in* $\mathcal{R}$*, we have* $I^* S \subseteq (IS)^*$*.*

(ii) *(Tightness) If* R *is a regular ring in* $\mathcal{R}$*, then* $I^* = I$ *for all ideals* I *of* R*.*

(iii) *(Plus-capturing) If* $R \to S$ *is a module-finite extensions of integral domains in* $\mathcal{R}$ *and* I *is any ideal of* R*, then* $IS \cap R \subseteq I^*$*. (i.e.* $I^+ \subseteq I^*$*)*

(iv) *(Colon-capturing) Let* R *be a* local *ring in* $\mathcal{R}$ *and* $x_1, \ldots, x_d$ *a system of parameters. Then for all* $0 \leq i \leq d-1$*,* $(x_1, \ldots, x_i) : x_{i+1} \subseteq (x_1, \ldots, x_i)^*$*.*

(v) *(Briançon–Skoda property) For any* $R \in \mathcal{R}$ *and any ideal* I *of* R*,*

$$(I^d)^- \subseteq I^* \subseteq I^-.$$

Hence, by Propositions 4.4.3 *and* 4.4.4*, both the Direct Summand Conjecture and Conjecture* 4.4.2 *hold in equal characteristic.*

Tight closure is defined (in [45]) for finitely generated $\mathbb{Q}$-algebras by a process of "reduction to characteristic p", a time-honored technique that we will not get into here (but see Definition 6.3.1 for a baby version of it). Next, tight closure was defined on arbitrary (excellent) $\mathbb{Q}$-algebras in an "equational" way (see Section 4.6), and then Artin approximation must be employed to demonstrate that it has the properties given in Theorem 4.5.1. This is a long process, so various attempts have been made to give a closure operation in equal characteristic 0 that circumvents it. More importantly, though, people have been trying to obtain a closure operation in *mixed* characteristic that has the right properties.

The first such attempt was probably solid closure [37], already discussed. Unfortunately, it fails tightness for regular rings of dimension 3 [67]. Parasolid closure [7] (a variant of solid closure) agrees with tight closure in characteristic p, and it has all the right properties in equal characteristic 0, but is not necessarily easier to work with than tight closure, and it may or may not have the right properties in mixed characteristic. Other at least partially successful attempts include parameter tight closure [38], diamond closure [48] and dagger closure (defined in [43], but shown to satisfy tightness just recently in [11]).

The most successful progress on the homological conjectures since the advent of tight closure theory is probably represented by Heitmann's proof [33] of the direct summand conjecture (Conjecture 4.4.1) for $\mathcal{R}_{3,0,p}$ (i.e. in mixed characteristic in dimension 3), which he does according to the program laid out above. Indeed, he shows the analogue of Theorem 4.5.1 when $\mathcal{R} = \mathcal{R}_{3,0,p}$ and tight closure is replaced everywhere with *extended plus closure*, denoted epf, first defined in his earlier paper [32].

(So in fact, his proof works to show the dimension 3 version of Conjecture 4.4.2 as well.)

4.6 (Homogeneous) Equational Closures and Localization

Let cl be a closure operation on some category $\mathcal{R}$ of rings. We say that cl *commutes with localization* in $\mathcal{R}$ if for any ring R and any multiplicative set $W \subseteq R$ such that the localization map $R \to W^{-1}R$ is in $\mathcal{R}$, and for any ideal I of R, we have $I^{\mathrm{cl}}(W^{-1}R) = (IW^{-1}R)^{\mathrm{cl}}$.

Tight closure does not commute with localization [10], unlike Frobenius closure, plus closure, integral closure, and radical. In joint work with Mel Hochster [21], we investigated what it is that makes a persistent closure operation commute with localization, and in so doing we construct a tight-closure-like operation that *does* commute with localization. Our closure is in general smaller than tight closure, though in many cases (see below), it does in fact coincide with tight closure.

To do this, we introduce the concepts of *equational* and *homogeneous(ly equational)* closure operations. The former notion is given implicitly in [45], where Hochster and Huneke define the characteristic 0 version of tight closure in an equational way.

In the following, we let Λ be a fixed base ring. Often $\Lambda = \mathbb{F}_p$, $\mathbb{Z}$, or $\mathbb{Q}$.

Definition 4.6.1. Let $\mathcal{F}$ be the category of *finitely generated* Λ-algebras, and let c be a persistent closure operation on $\mathcal{F}$. Then the *equational* version of c, denoted ceq, is defined on the category of *all* Λ-algebras as follows: Let R be a Λ-algebra, $f \in R$, and I an ideal of R. Then $f \in I^{\mathrm{ceq}}$ if there exists $A \in \mathcal{F}$, an ideal J of A, $g \in A$, and a Λ-algebra map $\phi : A \to R$ such that $g \in J^{\mathrm{c}}$, $\phi(g) = f$, and $\phi(J) \subseteq I$.

Let $\mathcal{G}$ be the category of finitely generated $\mathbb{N}$-*graded* Λ-algebras A which have the property that $[A]_0 = \Lambda$. Let c be a persistent closure operation on $\mathcal{G}$. Then the *homogeneous(ly equational)* version of c, denoted ch, is defined on the category of *all* Λ-algebras as follows: Let R be a Λ-algebra, $f \in R$, and I an ideal of R. Then $f \in I^{\mathrm{ch}}$ if there exists $A \in \mathcal{G}$, a *homogeneous* ideal J of A, a *homogeneous* element $g \in A$, and a Λ-algebra map $\phi : A \to R$ such that $g \in J^{\mathrm{c}}$, $\phi(g) = f$, and $\phi(J) \subseteq I$.

If c is a closure operation on Λ-algebras, we say it is *equational* if one always has $I^{\mathrm{c}} = I^{\mathrm{ceq}}$, or *homogeneous* if one always has $I^{\mathrm{c}} = I^{\mathrm{ch}}$.

In [21], we prove the following theorem:

Theorem 4.6.2. *Suppose* c *is a homogeneous closure operation. Then it commutes with arbitrary localization. That is, if R is a Λ-algebra, I an ideal, and W a multiplicative subset of R, then $(W^{-1}I)^{\mathrm{c}} = W^{-1}(I^{\mathrm{c}})$.*

In particular, *homogeneous tight closure* ($I^{*\mathrm{h}}$) commutes with localization. The following theorem gives circumstances under which $I^{*} = I^{*\mathrm{h}}$. Parts (i) and (iii) involve cases where tight closure was already known to commute with localization,

thus providing a "reason" that it commutes in these cases. Part (ii) gives a reason why the coefficient field in Brenner and Monsky's counterexample is transcendental over $\mathbb{F}_2$.

Theorem 4.6.3. *Let R be an excellent Noetherian ring which is either of prime characteristic $p > 0$ or of equal characteristic 0.*

(i) *If I is a parameter ideal (or more generally, if R/I has* finite phantom projective dimension *as an R-module), then $I^* = I^{*h}$.*

(ii) *If R is a finitely generated and positively-graded k-algebra, where k is an algebraic extension of $\mathbb{F}_p$ or of $\mathbb{Q}$, and I is an ideal generated by forms of positive degree, then $I^* = I^{*h}$.*

(iii) *If R is a* binomial ring *over any field k (that is, $R = k[X_1, \ldots, X_n]/J$, where the X_j are indeterminates and J is generated by polynomials with at most two terms each), then for any ideal I of R, $I^* = I^{*h}$.*

5 Reductions, Special Parts of Closures, Spreads, and Cores

5.1 Nakayama Closures and Reductions

Definition 5.1.1. [18] Let $(R, \mathfrak{m})$ be a Noetherian local ring. A closure operation c on ideals of R is *Nakayama* if whenever J, I are ideals such that $J \subseteq I \subseteq (J + \mathfrak{m}I)^c$, it follows that $J^c = I^c$.

It turns out that many closure operations are Nakayama. For example, integral closure [61], tight closure [18], plus closure [17], and Frobenius closure [19] are all Nakayama closures under extremely mild conditions. The fact that the identity closure is Nakayama is a special case of the classical Nakayama lemma (which is where the name of the condition comes from). However, radical is not Nakayama. For example, if $R = k[\![x]\!]$ (the ring of power series in one variable over a field k), $J = 0$, and $I = (x) = \mathfrak{m}$, then clearly $J \subseteq I \subseteq \sqrt{J + \mathfrak{m}I}$, but the radical ideals J and I are distinct.

Definition 5.1.2. Let R be a ring, c a closure operation on R, and $J \subseteq I$ ideals. We say that J is a c-*reduction* of I if $J^c = I^c$. A c-reduction $J \subseteq I$ is *minimal* if for all ideals $K \subsetneq J$, K is not a c-reduction of I.

For any Nakayama closure c, one can make a very strong statement about the existence of minimal c-reductions:

Lemma 5.1.3 ([18, Lemma 2.2]). *If cl is a Nakayama closure on R and I an ideal, then for any cl-reduction J of I, there is a minimal cl-reduction K of I contained in J. Moreover, in this situation any minimal generating set of K extends to a minimal generating set of J.*

This is another reason to see that radical is not Nakayama, as, for instance, the ideal (x) in the example above has no minimal $\sqrt{\ }$-reductions at all.

5.2 Special Parts of Closures

Consider the following notion from [19]:

Definition 5.2.1. Let $(R, \mathfrak{m})$ be a Noetherian local ring and c a closure operation on R. Let $\mathcal{I}$ be the set of all ideals of R. Then a set map csp : $\mathcal{I} \to \mathcal{I}$ is a *special part of* c if it satisfies the following properties for all $I, J \in \mathcal{I}$:

 (i) (Trapped) $\mathfrak{m}I \subseteq I^{\mathrm{csp}} \subseteq I^{\mathrm{c}}$,

 (ii) (Depends only on the closure) $(I^{\mathrm{c}})^{\mathrm{csp}} = I^{\mathrm{csp}}$,

 (iii) (Order-preserving) If $J \subseteq I$ then $J^{\mathrm{csp}} \subseteq I^{\mathrm{csp}}$,

 (iv) (Special Nakayama property) If $J \subseteq I \subseteq (J + I^{\mathrm{csp}})^{\mathrm{c}}$, then $I \subseteq J^{\mathrm{c}}$.

Of course, any closure operation c that admits a special part csp must be a Nakayama closure. Examples of special parts of closures include:

 • "Special tight closure" (first defined by Adela Vraciu in [78]), when R is excellent and of prime characteristic p:

$$I^{*\mathrm{sp}} := \{f \in R \mid x^{q_0} \in (\mathfrak{m}I^{[q_0]})^* \text{ for some power } q_0 \text{ of } p\}.$$

 • The special part of Frobenius closure (see [19]), when R has prime characteristic p:

$$I^{F\,\mathrm{sp}} := \{f \in R \mid x^{q_0} \in \mathfrak{m}I^{[q_0]} \text{ for some power } q_0 \text{ of } p\}.$$

 • The special part of integral closure (see [19]):

$$I^{-\mathrm{sp}} := \{f \in R \mid x^n \in (\mathfrak{m}I^n)^- \text{ for some } n \in \mathbb{N}\}.$$

 • The special part of plus closure (when R is a domain) (see [17]):

$$I^{+\mathrm{sp}} := \{f \in R \mid f \in \mathrm{Jac}(S)IS \text{ for some module-finite} \\ \text{domain extension } R \to S\},$$

 where $\mathrm{Jac}(S)$ is the Jacobson radical of S

All of these are in fact special parts of the corresponding closures. Moreover, we have the following:

Proposition 5.2.2.
 • *If $(R, \mathfrak{m})$ has a perfect residue field, then $I^F = I + I^{F\,\mathrm{sp}}$ for all ideals I* [19].
 • *If $(R, \mathfrak{m})$ is a Henselian domain with algebraically closed residue field, then $I^+ = I + I^{+\mathrm{sp}}$ for all ideals I* [17].

- If $(R, \mathfrak{m})$ is either an excellent, analytically irreducible domain with algebraically closed residue field, or an excellent normal domain with perfect residue field, then $I^* = I + I^{*\mathrm{sp}}$ for all ideals I [18, 52].

This property is called *special* c-*decomposition*, and goes back to the theorem of Huneke and Vraciu [52] on tight closure, and K. Smith's theorem [70, Theorem 2.2] as a kind of pre-history. Of course integral closure fails this property rather badly. Nevertheless, special c-decompositions allow for the following, matroidal proof of the existence of the notion of "spread" in such circumstances:

Theorem 5.2.3. *Suppose* c *is a closure with a special part* csp. *Suppose the following property holds:*

(α) $I^{\mathrm{c}} = I + I^{\mathrm{csp}}$ *for all ideals I of R.*

Let I be an arbitrary ideal. Then every minimal c-*reduction of I is generated by the same number of elements: the* c-*spread $\ell^{\mathrm{c}}(I)$ of I.*

Proof. Let J, K be minimal c-reductions of I. Say $\{a_1, \ldots, a_n\}$ is a minimal generating set for J, $\{b_1, \ldots, b_r\}$ is a minimal generating set for K, and $n \leq r$.

Claim. There is a reordering of the a_j's in such a way that for each $0 \leq i \leq n$, we have $I \subseteq L_i^{\mathrm{c}}$, where $L_i := (a_1, \ldots, a_i, b_{i+1}, \ldots, b_n)$.

Proof of Claim. We proceed by descending induction on i. If $i = n$ there is nothing to prove. So assume that $I \subseteq L_i^{\mathrm{c}}$ for some $1 \leq i \leq n$. We need to show that $I \subseteq L_{i-1}^{\mathrm{c}}$. It suffices to show that $a_i \in L_{i-1}^{\mathrm{c}}$, since this would imply that $L_i \subseteq L_{i-1}^{\mathrm{c}}$.

Note that $b_i \in I^{\mathrm{c}} = L_i^{\mathrm{c}} = L_i + L_i^{\mathrm{csp}}$ (by property (α)). Hence, there exist $r_j, s_j \in R$ such that

$$b_i + \sum_{j=i+1}^{n} r_j b_j + \sum_{j=1}^{i} s_j a_j \in L_i^{\mathrm{csp}}.$$

If all the $s_j \in \mathfrak{m}$, then

$$b_i + \sum_{j=i+1}^{n} r_j b_j \in (\mathfrak{m}L_i + L_i^{\mathrm{csp}} = L_i^{\mathrm{csp}} = I^{\mathrm{csp}}) \cap K = K^{\mathrm{csp}} \cap K = \mathfrak{m}K,$$

contradicting the fact that the b_j form a minimal generating set for K. Hence, by reordering the a_j, we may assume that $s_i \notin \mathfrak{m}$.

Thus, $a_i \in L_{i-1} + L_i^{\mathrm{csp}}$. It then follows from the special Nakayama property that $a_i \in L_{i-1}^{\mathrm{c}}$, as required.   □

Applying the Claim with $i = 0$ gives that $I \subseteq L_0^{\mathrm{c}} = (b_1, \ldots, b_n)^{\mathrm{c}}$. But since K was a *minimal* c-reduction of I, it follows that $(b_1, \ldots, b_n) = K = (b_1, \ldots, b_r)$, whence $n = r$.   □

Remark 5.2.4. Integral closure does not satisfy quite the same matroidal properties shared by plus closure, tight closure, and Frobenius closure, but it does so 'generically' as shown in [6].

It is natural to ask the following: Suppose c is a closure operation with well-defined c-spread ℓ^c. If one picks a random collection of $\ell^c(I)$ elements of $I/\mathfrak{m}I$, will their lifts to I generate a minimal c-reduction of I? This is unknown in general, but at least for integral closure and tight closure, the answer is often "yes":

Proposition 5.2.5. *Let I be an ideal of the Noetherian local ring $(R, \mathfrak{m})$. Suppose we are in one of the following situations:*

- *[61, Theorem 5.1] R has infinite residue field, and c = integral closure.*
- *[24, Theorem 4.5] char $R = p > 0$ prime, R is excellent and normal with infinite perfect residue field, and c = tight closure.*

Let $\ell := \ell^c(I)$. Then there is a Zariski-open subset $U \subseteq (I/\mathfrak{m}I)^\ell$ such that whenever $x_1, \ldots, x_\ell \in I$ are such that $(x_1 + \mathfrak{m}I, \ldots, x_\ell + \mathfrak{m}I) \in U$, the ideal $(x_1, \ldots, x_\ell)$ is a minimal c-reduction of I.

As soon as one knows that minimal c-reductions exist in the sense given in Lemma 5.1.3 (thus, for any Nakayama closure c), one can investigate the c-core of an ideal, which is by definition the intersection of all its (minimal) c-reductions. When c = integral closure (in which case we just call this object the *core*), this notion was first investigated by Rees and Sally [66]. They showed that if R is a *regular local ring* of dimension d, then for any ideal I, $(I^d)^- \subseteq \mathrm{core}(I)$. Fouli and Vassilev [24] have investigated the relationship between the core and the $*$-core of ideals in rings of prime characteristic p.

In joint work with Holger Brenner, we are developing a related notion (which one could call "specific c-closure" $c\sigma$), which we show in many cases coincides with csp, defined as follows: Let c be a closure operation defined by certain properties of generic forcing algebras (see Section 4.2). That is, let $(R, \mathfrak{m})$ be local and for $f \in R$ and an ideal $I = (f_1, \ldots, f_n)$ of R, let $A = R[T_1, \ldots, T_n]/(f + \sum_{i=1}^n f_i T_i)$. Consider the ideal $\mathfrak{n} := \mathfrak{m}A + (T_1, \ldots, T_n)$ of A. Suppose that $\mathcal{P}$ is a property of R-algebras such that $f \in I^c$ if and only if A has property $\mathcal{P}$. We say that f is in the *specific* c-*closure* of I if $A_{\mathfrak{n}}$ also has property $\mathcal{P}$. In the cases where both are defined, we can show that $I^{csp} \subseteq I^{c\sigma}$. Moreover, we show that $F\mathrm{sp} = F\sigma$ in general, that $+\mathrm{sp} = +\sigma$ in Henselian domains (e.g. complete local domains), and that $*\mathrm{sp} = \star\sigma$ in normal local domains of prime characteristic with perfect residue field.

6 Classes of Rings Defined by Closed Ideals

A typical reason that a closure operation is studied in the first place is often that the closedness of certain classes of ideals is related (and often equivalent) to the ring hav-

ing certain desirable properties. In the following, we will give examples based on various closure operations.

6.1 When Is the Zero Ideal Closed?

When $c = F, +, *, \star, \sqrt{}$, or $-$, we have $0^c = \sqrt{0}$, the *nilradical* of the ring. Hence, in these cases, the zero ideal is closed iff the ring is *reduced*.

For a local ring $(R, \mathfrak{m})$, we have $(0 : \mathfrak{m}^\infty) = H^0_{\mathfrak{m}}(R)$. So the zero ideal is $\mathfrak{m}$-saturated iff depth $R \geq \min\{\dim R, 1\}$ (that is, iff R is an (S_1) ring).

6.2 When Are 0 and Principal Ideals Generated by Non-zerodivisors Closed?

Example (Radical). For a Noetherian ring R, the answer here is: "R is a product of fields". First, note that if R is a product of fields, all ideals are radical. Conversely, R is a Noetherian ring where 0 and all principal ideals generated by non-zerodivisors are radical. As noted above, the fact that 0 is radical means that R is reduced. Now take any non-zerodivisor z of R. We have $z \in \sqrt{(z^2)} = (z^2)$ (since z^2 is a non-zerodivisor), so there is some $r \in R$ with $z = rz^2$. That is, $z(1 - rz) = 0$. Since z is a non-zerodivisor, this means that $rz = 1$, so that z is a unit. Hence R is *a reduced ring in which all non-zerodivisors are units*, and thus a product of fields.

When R is reduced, this condition may be written: $R = Q(R)$.

Example (Integral and tight closures). Recall that for reduced rings, tight closure and integral closure coincide for principal ideals. So in these cases, we may look at integral closure, in which case the answer is: "R is integrally closed in its total ring of fractions".

For suppose R is integrally closed in its total ring Q of fractions. Let $f \in R$ be a non-zerodivisor, and suppose $g \in (f)^-$. Then we have an equation of the form

$$g^n + a_1 f g^{n-1} + \cdots + a_n f^n = 0,$$

where $a_1, \ldots, a_n \in R$. Dividing through by f^n, we get the equation:

$$(g/f)^n + a_1(g/f)^{n-1} + \cdots + a_n = 0,$$

which shows that the element $g/f \in Q$ is integral over R. But this means that $g/f \in R$, whence $g \in (f)$. The converse statement follows the same steps in reverse.

For reduced rings, this condition may be written: $R = R^+ \cap Q(R)$.

Example (Frobenius closure). For a Noetherian ring of characteristic $p > 0$, the answer here is: "R is weakly normal"[4]. To see this, recall first [53, Proposition 1] that a Noetherian ring R is weakly normal if and only if the following conditions hold (where Q is the total quotient ring of R):

---
[4] Weak normality has a complicated history. The reader may consult the recent guide, [76].

(i) R is reduced.

(ii) For every $f \in Q$ such that $f^2, f^3 \in R$, one has $f \in R$.

(iii) For every $f \in Q$ such that there exists a prime integer n with $f^n, nf \in R$, one has $f \in R$.

Suppose first that R is weakly normal. The fact that R is reduced means that 0 is Frobenius closed. So let z be a non-zerodivisor of R and suppose $y \in (z)^F$. Then there is some $a \in R$ and $q = p^e$ such that $y^{p^e} \in (z^{p^e})$ as an ideal of R. In $Q(R)$, this means that $(y/z)^{p^e} = ((y/z)^{p^{e-1}})^p \in R$. But we also have $p \cdot (y/z)^{p^{e-1}} = 0 \in R$, so by condition (iii) above, it follows that $(y/z)^{p^{e-1}} \in R$, i.e., $y^{p^{e-1}} \in (z^{p^{e-1}})$. By induction on e, it follows that $y \in (z)$.

Conversely, suppose that 0 and every principal ideal generated by a non-zerodivisor is Frobenius closed. Condition (i) follows from 0 being Frobenius closed. For condition (ii), note that there exist integers $a, b \in \mathbb{N}$ such that $2a + 3b = p$. So if $f^2, f^3 \in R$, it follows that $f^p = (f^2)^a (f^3)^b \in R$ as well. But $f = y/z$ for some $y, z \in R$, where z is a non-zerodivisor, so $f^p \in R$ means that $y^p \in (z^p)$, so that $y \in (z)^F = (z)$, whence $f \in R$. As for condition (iii), let f, n be as given. If $n \neq p$, then the image of n in R is a unit, so that the fact that $nf \in R$ means that $f \in R$ automatically. So we may assume that $n = p$. But then $f^p \in R$, which means that $y^p \in (z^p)$ (where $f = y/z$ for some non-zerodivisor z), whence $y \in (z)^F = (z)$ and $f \in R$.

6.3 When Are Parameter Ideals Closed (Where R Is Local)?

For this subsection and the next, we need the following definitions (which represent a special case of "reduction to characteristic p"):

Definition 6.3.1. Let $\mathcal{P}$ be a property of positive prime characteristic rings. Let R be a finitely generated K-algebra, where K is a field of characteristic 0. That is, $R = K[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$. Let A be the $\mathbb{Z}$-subalgebra of K generated by the *coefficients* of the polynomials $f_1, \ldots, f_m$. Let $R_A := A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$. We say that R is *of $\mathcal{P}$-type* (resp. *dense $\mathcal{P}$-type*) if there is a nonempty Zariski-open subset U of the maximal ideal space of A (resp. an infinite set U of maximal ideals of A) such that for all $\mu \in U$, the ring $R_A \otimes_A A/\mu$ has property $\mathcal{P}$.

Example (Frobenius closure). Suppose $(R, \mathfrak{m})$ is a local *Cohen–Macaulay* ring of prime characteristic $p > 0$. Consider the map $R \to {}^1R$ defined in Section 3.2 (vii). By definition R is *F-injective* if the induced maps on local cohomology $H^i_\mathfrak{m}(R) \to H^i_\mathfrak{m}({}^1R)$ are injective. All parameter ideals are Frobenius closed if and only if R is F-injective.

Moreover, there are connections to characteristic 0 singularity theory. Namely, if R is a reduced, finitely generated $\mathbb{Q}$-algebra (or $\mathbb{C}$-algebra) of dense F-injective *type*, then Spec R has only *Du Bois singularities* [68]. (A converse is not known.)

Example (Tight closure). By definition, a ring R of prime characteristic $p > 0$ is *F-rational* if every parameter ideal is tightly closed.

The connection to characteristic 0 singularity theory is very strong. Indeed, it was shown by [26, 69] (Smith showed one direction and Hara showed the converse) that a finitely generated $\mathbb{Q}$-algebra (or $\mathbb{C}$-algebra) R is of F-rational *type* if and only if Spec R has only *rational singularities*.

Example (Integral closure). Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then every parameter ideal is integrally closed if and only if R is either a field or a rank 1 discrete valuation ring.

As usual, one direction is clear: if R is a field or a rank 1 DVR, then *every* ideal is integrally closed. So we prove the converse. We already know that R must be a normal domain (from the integral closure example in Section 6.2), so we need only show that dim $R \leq 1$. Accordingly, suppose dim $R \geq 2$. Let x, y be part of a system of parameters. Then x^2, y^2 is also part of a system of parameters. Thus, we have

$$xy \in (x^2, y^2)^- = (x^2, y^2),$$

But this is easily seen to contradict the fact that x, y are a regular sequence (which in turn arises from the fact that R is normal, hence (S_2).)

6.4 When Is Every Ideal Closed?

Example (Frobenius closure). For a Noetherian ring R of prime characteristic, we say that R is *F-pure* if the map $R \to {}^1R$ defined in Section 3.2 (vii) is a *pure* map of R-modules – that is, when tensored with any other R-module, the resulting map is always injective. This is easily seen to be equivalent to the condition that Frobenius closure on *modules* is trivial, which for excellent rings is then equivalent to the condition that all ideals are Frobenius closed (by [36, Theorem 1.7], since the rings in question must be reduced as $(0)^F$ is the nilradical of the ring).

Again, there is a connection to characteristic 0 singularity theory. Namely, if R is normal, $\mathbb{Q}$-Gorenstein, and characteristic 0 of dense F-pure type, then Spec R has only *log canonical singularities* [27]. (No converse is known.)

Example (Tight closure). For a Noetherian ring R of prime characteristic, we say that R is *weakly F-regular* if every ideal of R is tightly closed. It is called *F-regular* if $R_{\mathfrak{p}}$ is weakly F-regular for all prime ideals $\mathfrak{p}$. (Or equivalently, $W^{-1}R$ is weakly F-regular for all multiplicative sets $W \subset R$.) One of the outstanding open problems of tight closure theory is whether these two concepts are equivalent. The problem is open even for finitely generated algebras over a field.

In any case, we again have a connection to characteristic 0 singularity theory. Namely, if R is normal, $\mathbb{Q}$-Gorenstein, and characteristic 0, then R has F-regular *type* if and only if Spec R has only *log terminal singularities* [27].

Example (Integral closure). As shown earlier, assuming that R is Noetherian, all ideals are integrally closed iff R is a Dedekind domain. (More generally, all ideals are integrally closed iff R is a *Prüfer domain*.)

Example (The v-operation). Let R be a Noetherian domain. Then [59, Theorem 3.8] all ideals are v-closed (equivalently t-closed) if and only if R is Gorenstein of Krull dimension ≤ 1 (iff Q/R is an injective R-module, where Q is the total quotient ring of R).

7 Closure Operations on (Sub)modules

Whenever an author writes about a closure operation on (ideals of) rings that extends to a closure operation on (sub)modules, a choice must be made. Either the operation is defined generally for all submodules, after which all proofs and statements are made for modules and the statements about ideals follow as a corollary, or everything is done first exclusively on ideals and only afterwards is the reader shown how to extend it to the module case. I have opted for the latter option.

Definition 7.0.1. Let R be a ring and $\mathcal{M}$ a category of R-modules. A *closure operation on $\mathcal{M}$* is a collection of maps $\{\mathrm{cl}_M \mid M \in \mathcal{M}\}$, such that for any submodule $L \subseteq M$ of a module $M \in \mathcal{M}$, $\mathrm{cl}_M(L) := L_M^{\mathrm{cl}}$ is a submodule of M, such that the following properties hold:

 (i) (Extension) $L \subseteq L_M^{\mathrm{cl}}$ for all submodules $L \subseteq M \in \mathcal{M}$.

 (ii) (Idempotence) $L_M^{\mathrm{cl}} = (L_M^{\mathrm{cl}})_M^{\mathrm{cl}}$ for all submodules $L \subseteq M \in \mathcal{M}$.

 (iii) (Order-preservation) If $M \in \mathcal{M}$ and $K \subseteq L \subseteq M$ are submodules, then $K_M^{\mathrm{cl}} \subseteq L_M^{\mathrm{cl}}$. If moreover $L \in \mathcal{M}$, then $K_L^{\mathrm{cl}} \subseteq K_M^{\mathrm{cl}}$.

Some other properties of closure operations on modules are given below:

Definition 7.0.2. Let cl be a closure operation on a category $\mathcal{M}$ of R-modules. We say that cl is

 (i) *functorial* if whenever $g : M \to N$ is a morphism in $\mathcal{M}$, then for any submodule $L \subseteq M$, we have $g(L_M^{\mathrm{cl}}) \subseteq g(L)_N^{\mathrm{cl}}$.

 (ii) *semi-prime* if whenever $L \subseteq M$ are modules with $M \in \mathcal{M}$ and I is an ideal, we have $I \cdot L_M^{\mathrm{cl}} \subseteq (IL)_M^{\mathrm{cl}}$.

 (iii) *weakly hereditary* if whenever $L \subseteq M \subseteq N$ are submodules such that $M, N \in \mathcal{M}$, if $L = L_M^{\mathrm{cl}}$ and $M = M_N^{\mathrm{cl}}$ then $L = L_N^{\mathrm{cl}}$.

 (iv) *hereditary* if whenever $L \subseteq M \subseteq N$ are submodules such that $M, N \in \mathcal{M}$, then $L_N^{\mathrm{cl}} \cap M = L_M^{\mathrm{cl}}$.

(v) *residual* if whenever $\pi : P \twoheadrightarrow M$ is a surjection of modules in $\mathcal{M}$, and $N \subseteq P$ is a submodule, we have

$$N_P^{\mathrm{cl}} = \pi^{-1}(\pi(N)_M^{\mathrm{cl}})$$

Remark 7.0.3. [5] We note here that any functorial closure is semi-prime, provided that for any $x \in R$ and $M \in \mathcal{M}$, the endomorphism $\mu_x : M \to M$ (defined by multiplying by the element x) is in $\mathcal{M}$. To see this, let $L \subseteq M$ be a submodule and $x \in I$. Then $x \cdot L_M^{\mathrm{cl}} = \mu_x(L_M^{\mathrm{cl}}) \subseteq (\mu_x(L))_M^{\mathrm{cl}} = (xL)_M^{\mathrm{cl}}$. But by order-preservation, $(xL)_M^{\mathrm{cl}} \subseteq (IL)_M^{\mathrm{cl}}$ for any $x \in I$. Thus, we have

$$I \cdot L_M^{\mathrm{cl}} = \sum_{x \in I} x \cdot L_M^{\mathrm{cl}} \subseteq \sum_{x \in I} (xL)_M^{\mathrm{cl}} \subseteq (IL)_M^{\mathrm{cl}}.$$

For systematic reasons, one usually assumes that a closure operation is functorial. The disadvantage, of course, is that there is no way to extend a non-semi-prime closure on R to a functorial module closure on $\mathcal{M}$ (e.g. the v-operation on certain non-domains, as in Proposition 4.1.7 (iii)).

Remark 7.0.4. Given a closure operation on (ideals of) R that one wants to extend to a (functorial) closure on a category $\mathcal{M}$ of R-modules, one typically must make a choice: should the resulting operation be *weakly hereditary* or *residual*? Most closure operations on modules do not satisfies both conditions (but see Section 7.1 below).

Among integral closure-theorists, the usual goal has been to construct a *weakly hereditary* operation (so that for instance, if J is a reduction of an integrally closed ideal I, then the integral closure of J as a *submodule* of I is required to be I itself). See [16], or [51, Chapter 16] for a general discussion.

On the other hand, tight closure-theorists have gone the *residual* route (so that for instance, to compute the tight closure of an ideal I, one may take the tight closure of 0 in the R-submodule R/I and contract back). See [49, Appendix 1]. For a *residual* version of integral closure, see [22], by the present author and Bernd Ulrich.

Lemma 7.0.5 (Taken from [21]). *Let $\mathcal{F}$ (resp. $\mathcal{F}_{\mathrm{fin}}$) be the category of free (resp. finitely generated free) R-modules. Let* cl *be a functorial closure operation on $\mathcal{F}$ (resp. $\mathcal{F}_{\mathrm{fin}}$). Then* cl *extends uniquely to a* residual *closure operation on the category of all (resp. all finitely generated) R-modules if and only if for all (resp. for all finitely generated) R-modules F_1, F_2 and submodules $L_1 \subseteq F_1$, $L_2 \subseteq F_2$, we have*

$$(L_1 \oplus L_2)_{F_1 \oplus F_2}^{\mathrm{cl}} = (L_1)_{F_1}^{\mathrm{cl}} \oplus (L_2)_{F_2}^{\mathrm{cl}}.$$

We omit the easy proof. As for the construction: For a (f.g.) R-module M, let $\pi : F \to M$ be a surjection from a (f.g.) R-module F, and let $L_M^{\mathrm{cl}} := \pi(\pi^{-1}(L)_F^{\mathrm{cl}})$.

Indeed, this is the way that tight closure, Frobenius closure, and plus closure are defined on modules. First they were defined for free modules, and then extended to a residual operation in the way outlined above.

---

[5] Thanks to Holger Brenner for pointing this out.

Remark 7.0.6. All but one of the constructions from Section 3 can be extended to make *residual* closure operations. Namely:

- Construction 3.1.1 may be extended as follows: Fix an R-module U as before, and let $L \subseteq M$ be R-modules. We say that $f \in L_M^{\text{cl}}$ if the image of the map $U \otimes_R (Rf \hookrightarrow M)$ is contained in the image of the map $U \otimes_R (L \hookrightarrow M)$. This always yields a residual and functorial closure operation.

- Construction 3.1.2 may be extended similarly. That is, if $\phi : R \to S$ is a ring homomorphism and d is a closure operation on S-modules, then for R-modules $L \subseteq M$, let $j_M : M \to S \otimes_R M$ be the natural map, and for $z \in M$, we declare that $z \in L_M^{\text{c}}$ if the image (under j_M) of z is in the d-closure (in $S \otimes_R M$) of the image of the map $S \otimes_R (L \hookrightarrow M)$. Then c is a closure operation, semi-prime if d is, functorial if d is, and residual if d is.

- Constructions 3.1.3, 3.1.4, and 3.1.5 may be extended in the obvious way to modules, and the resulting operation is semi-prime (resp. residual, resp. functorial) if the operations it is based on are.

In this way (via Section 3.2), all the closure operations from Example 2.1.2 may be extended to residual, functorial closure operations on modules. This yields the usual definitions of Frobenius, plus, solid, tight, and basically full closures, and also of the α-saturation. The resulting extension of integral closure is of course not the usual (weakly hereditary) definition, but rather the residual, "liftable integral closure" from [22]. The extension of radical is the one mentioned in [9].

An analogue of Proposition 4.1.4 (i)–(iv) is also available for semi-prime closure operations on modules.

One more construction should be mentioned:

Construction 7.0.7. Let c be a closure operation on a module category $\mathcal{M}$. We define the *finitistic* c-closure of a submodule $L \subseteq M$ by setting

$$L_M^{\text{cfg}} := \bigcup \{L_N^{\text{c}} \mid L \subseteq N \subseteq M \text{ such that } N/L \text{ is finitely generated and } N \in \mathcal{M}\}$$

For a closure operation c, one may ask what the difference is, if any, between the closure operations c and cfg. This is very important in tight closure theory, for instance, in the question of whether weak F-regularity and F-regularity coincide. Indeed, if $(R, \mathfrak{m})$ is an F-finite Noetherian local ring of characteristic p and E is the injective hull of the residue field $R/\mathfrak{m}$, then R is weakly F-regular if and only if $0_E^{*\text{fg}} = 0$ [41, Proposition 8.23], but it is F-regular if $0_E^* = 0$ [57, follows from Proposition 2.4.1]. Thus, the two concepts would coincide if $0_E^* = 0_E^{*\text{fg}}$.

7.1 Torsion Theories

A functorial closure operation on modules that is both residual and weakly hereditary is essentially equivalent to the notion of a *torsion theory* (see [13] for torsion theories,

the book [4] for the connection with preradicals, or [9, Section 6] for a connection with Grothendieck topologies). We briefly outline the situation below, as this provides a fertile source of residual closure operations:

Definition 7.1.1. Let $\mathcal{M}$ be a category of R-modules which is closed under taking quotient modules, and let $\mathbf{r} : \mathcal{M} \to \mathcal{M}$ be a subfunctor of the identity functor (That is, it assigns to each $M \in \mathcal{M}$ a submodule $\mathbf{r}(M) \in \mathcal{M}$ of M, and every map $g : M \to N$ in $\mathcal{M}$ restricts to a map $\mathbf{r}(g) : \mathbf{r}(M) \to \mathbf{r}(N)$.) Then we say that $\mathbf{r}$ is a *preradical*.

   A preradical $\mathbf{r}$ is called a *radical* if for any $M \in \mathcal{M}$, we have $\mathbf{r}(M/\mathbf{r}(M)) = 0$.
   A radical $\mathbf{r}$ is *idempotent* if $\mathbf{r} \circ \mathbf{r} = \mathbf{r}$.
   A radical $\mathbf{r}$ is *hereditary* if for any submodule inclusion $L \subseteq M$ with $L, M \in \mathcal{M}$, we have $L \cap \mathbf{r}(M) = \mathbf{r}(L)$.

Definition 7.1.2. Let $\mathcal{M}$ be an Abelian category. Then a *torsion theory* is a pair $(\mathcal{T}, \mathcal{F})$ of classes of objects of $\mathcal{M}$ (called the *torsion* objects and the *torsion-free* objects, respectively), such that:

 (i) $\mathcal{T} \cap \mathcal{F} = \{0\}$,

 (ii) $\mathcal{T}$ is closed under isomorphisms and quotient objects,

(iii) $\mathcal{F}$ is closed under isomorphisms and subobjects, and

(iv) For any object $M \in \mathcal{M}$, there is a short exact sequence

$$0 \to T \to M \to F \to 0$$

   with $T \in \mathcal{T}$ and $F \in \mathcal{F}$.

(Recall that the T and F in the short exact sequence are unique up to isomorphism.)
   A torsion theory $(\mathcal{T}, \mathcal{F})$ is *hereditary* if $\mathcal{T}$ is also closed under taking subobjects.

Proposition 7.1.3. *Given an Abelian category $\mathcal{M}$ of R-modules, the following structures are equivalent:*

   • *a functorial, residual closure operation on $\mathcal{M}$.*

   • *a radical on $\mathcal{M}$.*

Moreover, the closure operation is weakly hereditary *if and only if the radical is* idempotent. *In this case, the structures are equivalent to specifying a* torsion theory *on $\mathcal{M}$. In this case, the closure operation is hereditary iff the radical is hereditary iff the torsion theory is hereditary.*

Proof. Instead of a complete proof, we show the correspondences below and leave the elementary proofs to the reader.

   If c is a functorial, residual closure operation on $\mathcal{M}$, we define a radical $\mathbf{r}$ on $\mathcal{M}$ by letting $\mathbf{r}(M) := 0_M^c$ for any $M \in \mathcal{M}$.

   If $\mathbf{r}$ is a radical on $\mathcal{M}$, we define a closure operation on $\mathcal{M}$ by letting $L_M^c := \pi^{-1}(\mathbf{r}(M/L))$ for any $L \subseteq M$, where $\pi : M \to M/L$ is the canonical surjection.

Given an idempotent radical $\mathbf{r}$ on $\mathcal{M}$, we define a torsion theory by letting $\mathcal{T} :=$ $\{\mathbf{r}(M) \mid M \in \mathcal{M}\}$ and $\mathcal{F} := \{M \in \mathcal{M} \mid \mathbf{r}(M) = 0\}$. Conversely, given a torsion theory $(\mathcal{T}, \mathcal{F})$, we let $\mathbf{r}(M) := T$, where $0 \to T \to M \to F \to 0$ is a short exact sequence with $T \in \mathcal{T}$ and $F \in \mathcal{F}$. □

The literature on torsion theories is immense. At the time of publication, I could not find the first place where it is shown that specifying a *hereditary* radical is equivalent to specifying a certain kind of filter of ideals, but this is nevertheless true, and was known by the late 1960s.

None of tight closure, plus closure, Frobenius closure, or radical (as given in Remark 7.0.6) are weakly hereditary; hence none of them provide examples of torsion theories. However, we have the following illustrative examples:

- For any ideal $\mathfrak{a}$ of R, the $\mathfrak{a}$-*saturation* (defined by $L_M^c := (L :_M \mathfrak{a}^\infty) = \{z \in M \mid \exists n \in \mathbb{N}$ such that $\mathfrak{a}^n z \subseteq L\}$) is a hereditary, residual, functorial closure operation on R-modules, and thus provides an example of a hereditary torsion theory on R-modules. (The corresponding radical is $H_\mathfrak{a}^0(-)$.)

- Let R be a commutative ring that contains at least one non-zerodivisor x that is not a unit, and let Q be its total ring of quotients (so that in particular, $Q \neq R$). Recall that a module M is *divisible* if for every non-zerodivisor r of R, the map $M \to M$ given by multiplication with r is *surjective*. Any module has a unique *largest* divisible submodule, since any sum of divisible submodules of a module is divisible. Consider the assignment $\mathbf{d}$ given by $\mathbf{d}(M) :=$ the largest divisible submodule of M. Then this is a weakly hereditary radical that is not hereditary. Hence, it defines a weakly hereditary residual closure operation that is not hereditary, hence a non-hereditary torsion theory. To see that it is not hereditary, note that $\mathbf{d}(Q) \cap R = R$ but $1 \notin \mathbf{d}(R)$ since x is not a unit.

Bibliography

[1] Adams, J. F., Localisation and completion. Chicago: Department of Mathematics. University of Chicago; 1975. arXiv:math.AT/1012.5020v3.

[2] Anderson, D. D., Anderson, D. F., Examples of star operations on integral domains. Comm Algebra. 1990;18:1621–1643.

[3] Anderson, D. D., Cook, S. J., Two star-operations and their induced lattices. Comm Algebra. 2000;28:2461–2475.

[4] Bican, L., Kepka, T., Němec, P., Rings, modules, and preradicals. vol. 75 of Lecture notes in pure and applied mathematics. New York: Dekker; 1982.

[5] Birkhoff, G., Lattice theory. 3rd ed. vol. 25 of American Mathematical Society collo-
     quium publications. Providence, RI: American Mathematical Society; 1967.

[6] Brennan, J. P., Epstein, N., Noether normalizations, reductions of ideals, and matroids.
     Proc Amer Math Soc. 2011;139:2671–2680.

[7] Brenner, H., How to rescue solid closure. J Algebra. 2003;265:579–605.

[8] _____ , Continuous solutions to algebraic forcing equations. Internat J Math. To appear.
     arXiv:math.AC/0608611v2. 2006.

[9] _____ , Grothendieck topologies and ideal closure operations. arXiv:math.AG/
     0612471v1. 2006.

[10] Brenner, H., Monsky, P., Tight closure does not commute with localization. Ann of Math
     (2). 2010;171:571–588.

[11] Brenner, H., Stäbler, A., Dagger closure in regular rings containing a field.
     arXiv:math.AC/1103.1786. 2011.

[12] Davey, B. A., Priestley, H. A., Introduction to lattices and order. 2nd ed. New York:
     Cambridge University Press; 2002.

[13] Dickson, S. E., A torsion theory for Abelian categories. Trans Amer Math Soc. 1966;
     121:223–235.

[14] Dietz, G. D., A characterization of closure operations that induce big Cohen–Macaulay
     modules. Proc Amer Math Soc. 2010;138:3849–3862.

[15] Dikranjan, D., Tholen, W., Categorical structure of closure operators. vol. 346 of Mathe-
     matics and its applications. Dordrecht: Kluwer; 1995.

[16] Eisenbud, D., Huneke, C., Ulrich, B., What is the Rees algebra of a module?. Proc Amer
     Math Soc. 2003;131:701–708.

[17] Epstein, N., Closure operators in commutative algebra: tight closure, phantom depth, and
     $*$-spread [PhD thesis]. University of Kansas; 2005.

[18] _____ , A tight closure analogue of analytic spread. Math Proc Cambridge Philos Soc.
     2005;139:371–383.

[19] _____ , Reductions and special parts of closures. J Algebra. 2010;323:2209–2225.

[20] Epstein, N., Hochster, M., Continuous closure, axes closure, and natural closure.
     arXiv:math.AC/1106.3462v1. 2011.

[21] _____ , Homogeneous equational closures, tight closure, and localization. In prepara-
     tion. 2011.

[22] Epstein, N., Ulrich, B., Liftable integral closure. Preprint. 2010.

[23] Fontana, M., Loper, K. A., A historical overview of Kronecker function rings, Nagata
     rings, and related star and semistar operations. In: Multiplicative ideal theory in commu-
     tative algebra. New York: Springer; 2006. p. 169–187.

[24] Fouli, L., Vassilev, J. C., The cl-core of an ideal. Math Proc Cambridge Philos Soc. 2010;
     149:247–262.

[25] Gilmer, R., Multiplicative ideal theory. vo. 12 of Pure and applied mathematics. New York: Dekker; 1972.

[26] Hara, N., A characterization of rational singularities in terms of injectivity of Frobenius maps. Amer J Math. 1998;120:981–996.

[27] Hara, N., Watanabe, K.-I., F-regular and F-pure rings vs. log terminal and log canonical singularities. J Algebraic Geom. 2002;11:363–392.

[28] Hara, N., Yoshida, K.-I., A generalization of tight closure and multiplier ideals. Trans Amer Math Soc. 2003;355:3143–3174.

[29] Heinzer, W. J., Johnston, B., Lantz, D., Shah, K., Coefficient ideals in and blowups of a commutative Noetherian domain. J Algebra. 1993;162:355–391.

[30] Heinzer, W. J., Lantz, D., Shah, K., The Ratliff–Rush ideals in a Noetherian ring. Comm Algebra. 1992;20:591–622.

[31] Heinzer, W. J., Ratliff Jr, L. J., Rush, D. E., Basically full ideals in local rings. J Algebra. 2002;250:371–396.

[32] Heitmann, R. C., Extensions of plus closure. J Algebra. 2001;238:801–826.

[33] ――――, The direct summand conjecture in dimension three. Ann of Math (2). 2002;156: 695–712.

[34] Hochster, M., Contracted ideals from integral extensions of regular rings. Nagoya Math J. 1973;51:25–43.

[35] ――――, Topics in the homological theory of modules over commutative rings. vol. 24 of CBMS regional conference series in mathematics. Providence, RI: American Mathematical Society; 1975.

[36] ――――, Cyclic purity versus purity in excellent Noetherian rings. Trans Amer Math Soc. 1977;231:463–488.

[37] ――――, Solid closure, Commutative algebra: syzygies, multiplicities, and birational algebra. Proceedings, 1992, South Hadley, MA. vol. 159 of Contemporary mathematics. Providence, RI: American Mathematical Society; 1994. p. 103–172.

[38] ――――, Parameter-like sequences and extensions of tight closure. Proceedings, Commutative Ring Theory and Applications; 2001, Fez. vol. 231 of Lecture notes in pure and applied mathematics. New York: Dekker; 2003. p. 267–287.

[39] ――――, Current state of the homological conjectures. http://www.math.utah.edu/vigre/ minicourses/algebra/hochster.pdf. 2004.

[40] ――――, Tight closure theory and characteristic p methods [with an appendix by Leuschke, G. J.]. In: Trends in commutative algebra. vol. 51 of Mathematical Sciences Research Institute publication. Cambridge: Cambridge University Press; 2004. p. 181–210.

[41] Hochster, M., Huneke, C., Tight closure, invariant theory, and the Briançon–Skoda theorem. J Amer Math Soc. 1990;3:31–116.

[42] ――――, Absolute integral closures are big Cohen–Macaulay algebras in characteristic p. Bull Amer Math Soc. 1991;24:137–143.

[43] _____ , Tight closure and elements of small order in integral extensions. J Pure Appl Algebra. 1991;71:233–247.

[44] _____ , F-regularity, test elements, and smooth base change. Trans Amer Math Soc. 1994;346:1–62.

[45] _____ , Tight closure in equal characteristic zero, book-length. Preprint. 1999.

[46] Hochster, M., Roberts, J. L., Rings of invariants of reductive groups acting on regular rings are Cohen–Macaulay. Adv Math. 1974;13:115–175.

[47] _____ , The purity of Frobenius and local cohomology. Adv Math. 1976;21:117–172.

[48] Hochster, M., Vélez, J. D., Diamond closure. Proceedings Algebra, Arithmetic and Geometry with Applications; 2000, West Lafayette, IN. Berlin: Springer; 2004. p. 511–523.

[49] Huneke, C., Tight closure and its applications. vol. 88 of CBMS regional conference series in mathematics. Providence, RI: American Mathematical Society; 1996.

[50] _____ , Tight closure, parameter ideals, and geometry. In: Six lectures on commutative algebra; 1996, Bellaterra. vol. 166 of Progress in mathematics. Basel: Birkhäuser; 1998. p. 187–239.

[51] Huneke, C., Swanson, I., Integral closure of ideals, rings, and modules. vol. 336 of London Mathematical Society lecture note series. Cambridge: Cambridge University Press; 2006.

[52] Huneke, C., Vraciu, A., Special tight closure. Nagoya Math J. 2003;170:175–183.

[53] Itoh, S., On weak normality and symmetric algebras. J Algebra. 1983;85:40–50.

[54] Kirby, D., Closure operations on ideals and submodules. J Lond Math Soc. 1969;44:283–291.

[55] Krull, W., Idealtheorie. Berlin: Springer; 1935.

[56] _____ , Beiträge zur Arithmetik kommutativer Integritätsbereiche. Math, Z. 1936;41:545–577.

[57] Lyubeznik, G., Smith, K. E., Strong and weak F-regularity are equivalent for graded rings. Amer J Math. 1999;121:1279–1290.

[58] Mac Lane, S., Categories for the working mathematician. 2nd ed. vol. 5 of Graduate texts in mathematics New York: Springer-Verlag; 1998.

[59] Matlis, E., Reflexive domains. J Algebra. 1968;8:1–33.

[60] Moore, E. H., Introduction to a form of general analysis. In: The New Haven mathematical colloquium. New Haven: Yale University Press; 1910. p. 1–150.

[61] Northcott, D. G., Rees, D., Reductions of ideals in local rings. Proc Cambridge Philos Soc. 1954;50:145–158.

[62] Okon, J. S., Ratliff Jr, L. J., Filtrations, closure operations, and prime divisors. Math Proc Cambridge Philos Soc. 1988;104:31–46.

[63] Petro, J. W., Some results on the asymptotic completion of an ideal. Proc Amer Math Soc. 1964;15:519–524.

[64] Ratliff Jr, L. J., Δ-closures of ideals and rings. Trans Amer Math Soc. 1989;313:221–247.

[65] Ratliff Jr, L. J., Rush, D. E., Two notes on reductions of ideals. Indiana Univ Math J. 1978;27:929–934.

[66] Rees, D., Sally, J. D., General elements and joint reductions. Michigan Math J. 1988;35: 241–254.

[67] Roberts, P. C., A computation of local cohomology. Proceedings, Commutative Algebra: Syzygies, Multiplicities, and Birational Algebra; 1992, South Hadley, MA. vol. 159 of Contemporary Mathematics. Providence, RI: American Mathematical Society; 1994. p. 351–356.

[68] Schwede, K., F-injective singularities are Du Bois. Amer J Math. 2009;131:445–473.

[69] Smith, K. E., F-rational rings have rational singularities. Amer J Math. 1997;119:159– 180.

[70] ———, Tight closure in graded rings. J Math Kyoto Univ. 1997;37:35–53.

[71] ———, An introduction to tight closure. Proceedings, Geometric and Combinatorial Aspects of Commutative Algebra; 1999, Messina. vol. 217 of Lecture notes in pure and applied mathematics. New York: Dekker; 2001. p. 353–377.

[72] ———, Tight closure and vanishing theorems. Proceedings, School on Vanishing Theorems and Effective Results in Algebraic Geometry; 2000, Trieste. vol. 6 of ICTP lecture notes, Trieste: Abdus Salam International Center for Theoretical Physics; 2001. p. 149– 213.

[73] Vasconcelos, W. V., Arithmetic of blowup algebras. vol. 195 of London Mathematical Society lecture note series. Cambridge: Cambridge University Press; 1994.

[74] ———, Integral closure – Rees algebras, multiplicities, algorithms. Springer monographs in mathematics. Berlin: Springer-Verlag; 2005.

[75] Vassilev, J. C., Structure on the set of closure operations of a commutative ring. J Algebra. 2009;321:2737–2753.

[76] Vitulli, M. A., Weak normality and seminormality, In: Commutative algebra: Noetherian and non-Noetherian perspectives. Springer-Verlag; 2011. p. 441–480.

[77] Vitulli, M. A., Leahy, J. V., The weak subintegral closure of an ideal. J Pure Appl Algebra. 1999;141:185–200.

[78] Vraciu, A. ∗-independence and special tight closure. J Algebra. 2002;249:544–565.

[79] ———, A new version of α-tight closure, Nagoya Math J. 2008;192:1–25.

[80] Zafrullah, M., Putting t-invertibility to use. In: Non-Noetherian commutative ring theory. vol. 520 of Mathematics and its applications. Dordrecht: Kluwer Acad. Publ.; 2000. p. 429–457.

Author Information

Neil Epstein, Institut für Mathematik, Universität Osnabrück, Osnabrück, Germany.
E-mail: nepstein@uni-osnabrueck.de

A Survey of Test Ideals

Karl Schwede and Kevin Tucker

Abstract. Test ideals were first introduced by Mel Hochster and Craig Huneke in their celebrated theory of tight closure, and since their invention have been closely tied to the theory of Frobenius splittings. Subsequently, test ideals have also found application far beyond their original scope to questions arising in complex analytic geometry. In this paper we give a contemporary survey of test ideals, F-singularities, and their wide-ranging applications.

1 Introduction

Test ideals were first introduced by Mel Hochster and Craig Huneke in their celebrated theory of tight closure [70], and since their invention have been closely tied to the theory of Frobenius splittings [109, 121]. Subsequently, test ideals have also found application far beyond their original scope to questions arising in complex analytic geometry. In this paper we give a contemporary survey of test ideals and their wide-ranging applications.

The test ideal has become a fundamental tool in the study of positive characteristic algebraic geometry and commutative algebra. To each ring R of prime characteristic $p > 0$, one can associate a test ideal $\tau(R)$ which reflects properties of the singularities of R. If R is regular, then $\tau(R) = R$; more generally, if the singularities of R are mild, one expects that $\tau(R)$ is close to or equal to R. Conversely, severe singularities give rise to small test ideals.

While the name *test* ideal comes from Hochster and Huneke's original description as the so-called test elements in the theory of tight closure, we initially define them herein more directly without any reference to tight closure. Briefly, our approach makes use of pairs (R, ϕ) where R is an integral domain and $\phi \colon R^{1/p} \to R$ is an R-module homomorphism, a familiar setting to readers comfortable with the theory of Frobenius splittings. This perspective has numerous advantages. In addition to the relative simplicity of the definition of the test ideal, this setting also provides a natural

segue into the connection between the test ideal and the multiplier ideal. Nevertheless, we do however include a short section on the classical definition via tight closure theory. In addition, we also include sections focusing on various related measures of singularities in positive characteristic besides the test ideal, such as F-rationality and Hilbert–Kunz multiplicity.

We have tried to make the sections of this paper modular, attempting to minimize the reliance of each individual section on the previous sections. Following the initial discussion on preliminaries and notation, the main statements throughout the remainder of the document can all be read independently. In addition, we have included numerous exercises scattered throughout the text. It should be noted that while many of the exercises are quite easy, some have been decorated with a * to indicate that they are substantially more difficult.

We hope that this survey will be readable and useful to a wide variety of potential audiences. In particular, we have three different audiences in mind:

(i) Readers working in characteristic $p > 0$ commutative algebra who wish to understand generalizations to "pairs" and connections between test ideals and algebraic geometry. These individuals will probably be most interested in Sections 3, 6, and 7.

(ii) Readers familiar with Frobenius splitting techniques who wish to learn of the language and methods used by their counterparts studying tight closure (Section 5) and connections to the minimal model program (Section 4). These individuals may wish to skim Section 2. They may additionally find Sections 3 and 8 useful.

(iii) Readers with a background in complex analytic and algebraic geometry working on notions related to multiplier ideals or the minimal model program who wish to learn about characteristic $p > 0$ methods. The most useful material for these individuals is likely found in Sections 2, 3, 4 and 6.

This survey is not, however, designed to be an introduction to tight closure, as there are already several excellent surveys and resources on the subject, see [68, 76, 147] and [27, Chapter 10]. In addition, the reader interested in Frobenius splitting and related cohomology vanishing theorems is referred to [25]; we shall not have occasion to discuss global vanishing theorems in this survey.

In the appendices to this paper, we very briefly review the notions of Cohen–Macaulay and Gorenstein rings, as well as several forms of duality which are used minimally throughout the body of the paper. These include local duality, Matlis duality and Grothendieck duality. Also included is a short summary of the formalism of divisors on normal varieties from a very algebraic point of view.

As those experts already familiar with the technical language surrounding the development of test ideas will be quick to notice, the terminology and notation in this paper also differs from that used historically in the following way:

Convention. When referring to the test ideal $\tau(R)$ throughout this paper, we always refer to the *big (or non-finitistic) test ideal*, often denoted by $\widetilde{\tau}(R)$ or $\tau_b(R)$ in the literature. We will call the classical test ideal, i.e. the test ideal originally introduced by Hochster and Huneke, the *finitistic test ideal* and denote it rather by $\tau_{\mathrm{fg}}(R)$.

We make this simplifying convention largely because we believe there is now consensus that the *big test ideal* is the preferable notion to study. Of course, the two notions (finitistic and non-finitistic) are frequently known to coincide and are conjectured to be equivalent in general (Conjecture 5.14).

2 Characteristic p Preliminaries

Setting. Throughout this paper all rings are integral domains essentially of finite type over a field k. In this context, the word "essentially" means that R is obtained from a finitely generated k-algebra by localizing at a multiplicative system. In this section, that field k is always perfect of prime positive characteristic $p > 0$.[1]

2.1 The Frobenius Endomorphism

When working in characteristic $p > 0$, the Frobenius or p-th power endomorphism is a powerful tool which can be thought of in several equivalent ways. First and foremost, it is the ring homomorphism $F\colon R \to R$ given by $r \mapsto r^p$. However, in practice it is often convenient to distinguish between the copies of R serving as the source and target. To that end, consider the set $R^{1/p}$ of all p-th roots of elements of R inside a fixed algebraic closure of the fraction field of R. The set $R^{1/p}$ is closed under addition and multiplication, and it forms a ring abstractly isomorphic to R itself (by taking p-th roots). The inclusion $R \subseteq R^{1/p}$ is naturally identified with the Frobenius endomorphism of R and gives $R^{1/p}$ the structure of an R-module.

More generally, denoting by R^{1/p^e} the set of p^e-th roots of elements of R and iterating the above procedure gives

$$R \subseteq R^{1/p} \subseteq R^{1/p^2} \subseteq \cdots \subseteq R^{1/p^e} \subseteq R^{1/p^{e+1}} \subseteq \cdots$$

where each inclusion is identified with the Frobenius endomorphism of R. Thus, as before R^{1/p^e} is a ring abstractly isomorphic to R, and the inclusion $R \subseteq R^{1/p^e}$ is identified with the e-th iterate $F^e\colon R \to R$ of Frobenius given by $r \mapsto r^{p^e}$. For any ideal $I = \langle z_1, \ldots, z_m \rangle \subseteq R$, we write $I^{1/p^e} = \langle z_1^{1/p^e}, \ldots, z_m^{1/p^e} \rangle_{R^{1/p^e}}$ to denote the ideal (in R^{1/p^e}) of p^e-th roots of elements of I. Again, we have that R^{1/p^e} is an R-module via the inclusion $R \subseteq R^{1/p^e}$.

---

[1] Essentially all of the positive characteristic material in this paper can easily be generalized to the setting of reduced F-finite rings. In addition, large portions of the theory extend to the setting of excellent local rings.

Exercise 2.1. Consider the polynomial ring $S = k[x_1, \ldots, x_d]$. Show that S^{1/p^e} is a free S-module of rank p^{ed} with S-basis $\{x_1^{\lambda_1/p^e} \ldots x_d^{\lambda_d/p^e}\}_{0 \le \lambda_i \le p^e - 1}$.

If M is any R-module, the (geometrically motivated) notation $F_*^e M$ is often used to denote the corresponding R-module coming from restriction of scalars for F^e. Thus, M and $F_*^e M$ agree as both sets and Abelian groups. However, if $F_*^e m$ denotes the element of $F_*^e M$ corresponding to $m \in M$, we have $r \cdot F_*^e m = F_*^e (r^{p^e} \cdot m)$ for $r \in R$ and $m \in M$. It is easy to see that $F_*^e R$ and R^{1/p^e} are isomorphic R-modules by identifying $F_*^e r$ with r^{1/p^e} for each $r \in R$. While we have taken preference to the use of R^{1/p^e} throughout, it can be very helpful to keep both perspectives in mind.

Remark 2.2. We caution the reader that the module $F_*^e M$ is quite different from that which is commonly denoted $F^e(M)$ originating in [120]. This latter notation coincides rather with $M \otimes_R F_*^e R$ considered as an R-$F_*^e R$ bimodule.

Exercise 2.3. Show that $F_*^e(\_)$ is an exact functor on the category of R-modules. Conclude that $F_*^e(R/I)$ and $R^{1/p^e}/I^{1/p^e}$ are isomorphic R-modules (and furthermore as $(F_*^e R = R^{1/p^e})$-modules) for any ideal $I \subseteq R$.

Lemma 2.4. R^{1/p^e} *is a finitely generated R-module.*

Proof. Since R is essentially of finite type over k we write $R = W^{-1}(k[x_1, \ldots, x_n]/I)$ where I is an ideal in $S = k[x_1, \ldots, x_n]$ and W is a multiplicative system in S/I. First notice that $(S/I)^{1/p^e} = S^{1/p^e}/I^{1/p^e}$ is certainly a finite S/I-module by Exercise 2.1. But then we have that $W^{-1}((S/I)^{1/p^e})$ is a finitely generated $W^{-1}(S/I)$-module, and so the result is proven after observing

$$W^{-1}((S/I)^{1/p^e}) = ((W^{p^e})^{-1}(S/I))^{1/p^e} = (W^{-1}(S/I))^{1/p^e}. \qquad \square$$

Test ideals are measures of singularities of rings of characteristic $p > 0$, and will be defined initially through the use of a homomorphism $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$. The following result demonstrates that it is reasonable to use properties of R^{1/p^e} to quantify the singularities of R.

Theorem 2.5 ([97]). *R is regular if and only if R^{1/p^e} is a* locally-*free R-module.*

Proof. The forward direction of the proof follows by reducing to the case of Exercise 2.1, while the converse direction is more involved; see [97] and [102]. $\qquad \square$

2.2 F-purity

Rather than requiring that R^{1/p^e} be a free R-module, one might consider the weaker condition that R is a direct summand of R^{1/p^e}. To that end, recall that an inclusion of rings $A \subseteq B$ is called *split* if there is an A-module homomorphism $s\colon B \to A$ such

that $s|_A = \mathrm{id}_A$ (in which case B is isomorphic as an A-module to $A \oplus \ker(s)$, and s is called a *splitting of $A \subseteq B$*).

Definition 2.6. R is *F-pure*[2] if the inclusions $R \subseteq R^{1/p^e}$ are split.

Exercise 2.7. Suppose that R is F-pure. Show that, for every R-module M and all $e \geq 1$, the natural map $M \to M \otimes_R R^{1/p^e}$ is injective.

In the setting of this paper – where R is essentially of finite type over a perfect field k – the converse statement also holds [67], but may fail in general. For an arbitrary ring, the injectivity of $M \to M \otimes_R R^{1/p^e}$ for all M is taken to be the definition of F-purity.

Exercise 2.8. Show that if $R \subseteq R^{1/p^e}$ is split for some $e \geq 1$, then it is split for all $e \geq 1$.

Exercise 2.9. Suppose that $\mathfrak{q} \in \mathrm{Spec}\, R$ is a point such that $R_\mathfrak{q}$ is F-pure. Show that there exists an open neighborhood $U \subseteq \mathrm{Spec}\, R$ of $\mathfrak{q}$ such that $R_\mathfrak{p}$ is F-pure for every point $\mathfrak{p} \in U$.
Hint. Prove $R \subseteq R^{1/p^e}$ splits if and only if "evaluation at 1" $\mathrm{Hom}_R(R^{1/p^e}, R) \to R$ is surjective.

Exercise 2.10. Suppose that for every maximal ideal $\mathfrak{m} \in \mathrm{Spec}\, R$, $R_\mathfrak{m}$ is F-pure. Show that R is also F-pure.

In Theorem 2.14 below, we exhibit a simple way of determining whether R is F-pure.

Definition 2.11 (Frobenius powers of an ideal). Suppose $I = \langle y_1, \ldots, y_m \rangle \subseteq R$ is an ideal. Then for any integer $e > 0$, we set $I^{[p^e]}$ to be the ideal $\langle y_1^{p^e}, \ldots, y_n^{p^e} \rangle_R$.

Exercise 2.12. Show that $(I^{[p^e]})^{1/p^e} = IR^{1/p^e}$, and conclude $I^{[p^e]}$ is independent of the choice of generators of I.

Exercise 2.13. Suppose that R is a regular local ring and $I \subset R$ is an ideal. If $x \in R$, show that $x \in I^{[p^e]}$ if and only if $\phi(x^{1/p^e}) \in I$ for all $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$.

Theorem 2.14 (Fedder's Criterion, [44, Lemma 1.6]). *Suppose that $S = k[x_1, \ldots, x_n]$ and that $R = S/I$ is a quotient ring. Then for any point $\mathfrak{q} \in \mathrm{Spec}\, R = V(I) \subseteq \mathrm{Spec}\, S$, the local ring $R_\mathfrak{q}$ is F-pure if and only if $(I^{[p]} : I) \not\subseteq \mathfrak{q}^{[p]}$. (Notice we are abusing notation by identifying $\mathfrak{q} \in \mathrm{Spec}\, R$ with its pre-image in $\mathrm{Spec}\, S$).*

---

[2] A splitting of $R \subseteq R^{1/p}$ is referred to as an *F-splitting*. At times, *F*-pure rings are also known as *F-split*, but we caution the reader that (particularly when in a non-affine setting) these terms are not always interchangeable. See also Exercise 2.7.

Proof. We sketch the main ideas of the proof and leave the details to the reader. First observe that every map $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$ is the quotient of a map $\psi \in \mathrm{Hom}_S(S^{1/p^e}, S)$ (use the fact that S^{1/p^e} is a projective S-module). Next prove that $\mathrm{Hom}_S(S^{1/p^e}, S)$ is isomorphic to S^{1/p^e} as an S^{1/p^e}-module. Finally, show that $(I^{[p^e]} : I)^{1/p^e} \cdot \mathrm{Hom}_S(S^{1/p^e}, S)$ corresponds exactly to those elements of $\mathrm{Hom}_S(S^{1/p^e}, S)$ which come from $\mathrm{Hom}_R(R^{1/p^e}, R)$. Once this correspondence is in hand, show that the elements $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$ that are surjective at $R_{\mathfrak{q}}$ are in bijective correspondence with the elements $x \in (I^{[p^e]} : I)$ which are not contained in $\mathfrak{q}^{[p^e]}$. $\qquad\square$

Exercise 2.15 (Coordinate Hyperplanes are F-pure). Suppose that $S = k[x_1, \ldots, x_n]$ and $I = \langle x_1 \cdots x_n \rangle$. Show that S/I is F-pure.

Exercise* 2.16 (Elliptic curves). Show that $R = \mathbb{F}_p[x, y, z]/\langle x^3 + y^3 + z^3 \rangle$ is not F-pure if $p = 2, 3, 5, 11$, but is F-pure if $p = 7, 13$. Generally, show that R is F-pure if and only if $p \equiv 1 \mod 3$, in which case the associated elliptic curve is ordinary (see [61, p. 332]).

Exercise 2.17. Suppose that $S = \mathbb{F}_p[x, y, z]$ and that $f = xy - z^2$ and $g = x^4 + y^4 + z^4$. Show that, for any choice of p, $S/\langle f \rangle$ is always F-pure while $S/\langle g \rangle$ is never F-pure.

Exercise 2.18. [75, Proposition 5.31] A reduced ring R of characteristic $p > 0$ with total quotient ring K is called weakly normal if it satisfies the following property: for every $x \in K$, $x^p \in R$ automatically implies $x \in R$ as well. Prove that any F-pure ring is weakly normal.

Hint. First check that a splitting of $R \subseteq R^{1/p}$ can be extended to a splitting of $K \subseteq K^{1/p}$.

3 The Test Ideal

Setting. In this section as before, all rings are integral domains of essentially finite type over a perfect field of characteristic $p > 0$.

While the test ideal was first described as an auxiliary component of tight closure theory, we give a description of the test ideal without reference to tight closure in this section. This description has roots in [56, 107, 144]; see also [126, Theorem 6.3] for further statements and details.

3.1 Test Ideals of Map-pairs

We begin by introducing test ideals for pairs (R, ϕ), where the addition of a homomorphism $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$ in fact helps to simplify the definition.

Definition 3.1. Fix an integer $e > 0$ and a non-zero R-linear map $\phi: R^{1/p^e} \to R$ (for example, a splitting of $R \subseteq R^{1/p^e}$). We define the *test ideal* $\tau(R, \phi)$ to be the unique smallest non-zero ideal $J \subseteq R$ such that $\phi(J^{1/p^e}) \subseteq J$.

We make two initial observations about this definition:

(i) It is in no way clear that there is such a smallest ideal! (More on this soon.)

(ii) The choice of ϕ can wildly change the test ideal, as in Exercise 3.5 below. In particular, $\tau(R, \phi)$ does not just reflect properties of R, but rather incorporates those of ϕ as well.

Remark 3.2. If $\phi: R^{1/p^e} \to R$ is as above, and $J \subseteq R$ is an ideal such that $\phi(J^{1/p^e}) \subseteq J$, then J is said to be *ϕ-compatible*. Thus $\tau(R, \phi)$ is the unique smallest non-zero ϕ-compatible ideal.

Exercise 3.3 (cf. [14]). With notation as above, show that $\phi(\tau(R, \phi)^{1/p^e}) = \tau(R, \phi)$. *Hint.* Show that $\phi(\tau(R, \phi)^{1/p^e})$ is ϕ-compatible.

Exercise 3.4 ([45, Proposition 2.5; 126, Theorem 7.1; 159, Theorem 3.3]). Suppose that in addition $\phi: R^{1/p^e} \to R$ is surjective (for example, a splitting of $R \subseteq R^{1/p^e}$). Show that $\tau(R, \phi)$ is a radical ideal. Furthermore, prove that $R/\tau(R, \phi)$ is an F-pure ring.

Exercise 3.5. Suppose that $R = \mathbb{F}_2[x, y]$ and recall that $R^{1/2}$ is a free R-module (Exercise 2.1) with basis $1, x^{1/2}, y^{1/2}, (xy)^{1/2}$. Consider the R-linear three maps $\alpha, \beta, \gamma: R^{1/2} \to R$ defined as follows:

$$R^{1/2} \xrightarrow{\alpha} R \qquad R^{1/2} \xrightarrow{\beta} R \qquad R^{1/2} \xrightarrow{\gamma} R$$

$$1 \mapsto 0 \qquad\qquad 1 \mapsto 0 \qquad\qquad 1 \mapsto 1$$

$$x^{1/2} \mapsto 0 \qquad\quad x^{1/2} \mapsto 1 \qquad\quad x^{1/2} \mapsto 0$$

$$y^{1/2} \mapsto 0 \qquad\quad y^{1/2} \mapsto 0 \qquad\quad y^{1/2} \mapsto 0$$

$$(xy)^{1/2} \mapsto 1 \qquad (xy)^{1/2} \mapsto 0 \qquad (xy)^{1/2} \mapsto 0$$

Prove that $\tau(R, \alpha) = R$, $\tau(R, \beta) = \langle y \rangle$ and $\tau(R, \gamma) = \langle xy \rangle$.

Now we turn our attention to the question of existence. We make use of the following somewhat technical lemma, which has its origins in tight closure theory.

Lemma 3.6 ([70, Section 6; 129, Proposition 3.21]). *Suppose that $\phi: R^{1/p^e} \to R$ is a non-zero R-linear map. Then there exists a non-zero $c \in R$ satisfying the following*

property: for every element $0 \neq d \in R$, there exists an integer $n > 0$ such that $c \in \phi^n((dR)^{1/p^{ne}})$. Here ϕ^n is defined to be the composition map

$$R^{1/p^{ne}} \xrightarrow{\phi^{1/p^{(n-1)e}}} R^{1/p^{(n-1)e}} \xrightarrow{\phi^{1/p^{(n-2)e}}} R^{1/p^{(n-2)e}} \to \cdots \to R^{1/p^e} \xrightarrow{\phi} R.$$

Proof. The proof is involved, and so we omit it here and refer the interested reader to [71, Theorem 5.10]. However, let us remark that if $b \in R$ is such that $R_b := R[b^{-1}]$ is regular and also $\mathrm{Hom}_{R_b}(R_b^{1/p^e}, R_b)$ is generated by ϕ_b as an R_b^{1/p^e}-module, then $c = b^l$ will suffice for some $l \gg 0$. In fact, if additionally $b \in \phi(R^{1/p^e})$, then $c = b^3$ will work. $\qquad\square$

Remark 3.7. The element $c \in R$ constructed above in Lemma 3.6 is an example something called a *test element*. Its construction implies that c remains a test element after localization and completion (this condition is also sometimes called being a *completely stable test element*).

Theorem 3.8. *With the notation of Definition* 3.1*, fix any* $c \in R$ *satisfying the condition of Lemma* 3.6*. Then*

$$\tau(R, \phi) = \sum_{n \geq 0} \phi^n((cR)^{1/p^{ne}}).$$

Here ϕ^0 is defined to be the identity map $R \to R$.

Proof. Certainly the sum $\sum_{n \geq 0} \phi^n((cR)^{1/p^{ne}})$ is the smallest ideal $J \subseteq R$ both containing c and such that $\phi(J^{1/p^e}) \subseteq J$. On the other hand, if $I \subseteq R$ is any non-zero ideal such that $\phi(I^{1/p^e}) \subseteq I$, then Lemma 3.6 implies that $c \in I$. This completes the proof. $\qquad\square$

Exercise* 3.9. [124, Proposition 4.8] Prove that $\tau(R, \phi) = \tau(R, \phi^m)$ for any integer $m > 0$.
Hint. The containment $\subseteq$ is easy. For the other containment, use a clever choice of an element from Lemma 3.6.

Exercise 3.10. Suppose that W is a multiplicative system in R. Let $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$ and consider the induced map $(W^{-1}\phi) \in \mathrm{Hom}_{W^{-1}R}((W^{-1}R)^{1/p^e}, W^{-1}R)$. Then show that $W^{-1}\tau(R, \phi) = \tau(W^{-1}R, W^{-1}\phi)$.
Hint. Suppose that $c \in R$ comes from Lemma 3.6. Prove that $c/1 \in W^{-1}R$ also satisfies the condition of Lemma 3.6 for $W^{-1}\phi$.

We conclude with an algorithm for computing the test ideal of a pair (R, ϕ).

Exercise 3.11 ([82]). Choose c satisfying Lemma 3.6 for a non-zero $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$ (finding such a c can be quite easy, as explained in the proof of Lemma 3.6). Consider the following chain of ideals. $J_0 = cR$, $J_1 = J_0 + \phi(J_0^{1/p^e})$, and in general $J_n = J_{n-1} + \phi(J_{n-1}^{1/p^e})$. Show that $J_n = \tau(R, \phi)$ for $n \gg 0$.

3.2 Test Ideals of Rings

As noted above, $\tau(R, \phi)$ is depends heavily on the choice of ϕ. To remove this dependence, one simply considers all possible ϕ simultaneously.

Definition 3.12. We define the *test ideal*[3] $\tau(R)$ to be the unique smallest non-zero ideal $J \subseteq R$ such that $\phi(J^{1/p^e}) \subseteq J$ for all $e > 0$ and all $\phi \in \operatorname{Hom}_R(R^{1/p^e}, R)$.

It follows from the definition that $\tau(R, \phi) \subseteq \tau(R)$ regardless of the choice of $\phi \in \operatorname{Hom}_R(R^{1/p^e}, R)$.

Exercise 3.13 ([70, Theorem 4.4]). Suppose that $S = k[x_1, \ldots, x_n]$. Prove that $\tau(S) = S$.
Hint. Use the fact that S^{1/p^e} is a free S-module to show the following: for any $d \in S$, there exists an integer $e > 0$ and $\phi \in \operatorname{Hom}_S(S^{1/p^e}, S)$ such that $\phi(d^{1/p^e}) = 1$.

Again, it is not clear that $\tau(R)$ exists.

Theorem 3.14 ([56, Lemma 2.1]). *Fix any non-zero* $\phi \in \operatorname{Hom}_R(R^{1/p}, R)$ *and any* $c \in R$ *satisfying the condition of Lemma* 3.6 *for* ϕ. *Then*

$$\tau(R) = \sum_{e \geq 0} \sum_{\psi} \psi((cR)^{1/p^e}).$$

where the inner sum runs over all $\psi \in \operatorname{Hom}_R(R^{1/p^e}, R)$.

Proof. The proof is essentially the same as in Theorem 3.8 and so is left to the reader. □

Exercise 3.15 (cf. [107, Theorem 7.1 (7)]). Prove that for any given multiplicative system W, $W^{-1}\tau(R) = \tau(W^{-1}R)$.
Hint. Mimic the proof of Exercise 3.10.

Remark 3.16. The result of the above exercise holds in much more general settings than we consider here. See [1, 107].

Exercise 3.17 ([45, 126, 159]). Suppose that R is an F-pure ring. Prove that $\tau(R)$ is a radical ideal and that $R/\tau(R)$ is also F-pure.

Exercise* 3.18 ([25, Exercise 1.2.E (4)]). Suppose that R is a reduced (possibly non-normal) ring and R^N is its normalization. The conductor ideal $\mathfrak{c} \subseteq R$ is the largest

---

[3] Strictly speaking, if we follow the literature, $\tau(R)$ is traditionally called the *big test ideal* or the *non-finitistic test ideal* and often denoted by $\tau_b(R)$ or $\widetilde{\tau}(R)$.

ideal of R^{N} which is also simultaneously an ideal of R (it can also be described as $\mathrm{Ann}_R(R^{\mathrm{N}}/R)$). Show that $\tau(R) \subseteq \mathfrak{c}$.

Hint. Show that $\phi(\mathfrak{c}^{1/p^e}) \subseteq \mathfrak{c}$ for all $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$ and all $e \geq 0$.

We conclude this section with a theorem which characterizes when $\tau(R) = R$.

Theorem 3.19. *Suppose R is a domain essentially of finite type over a perfect field k. Then we have $\tau(R) = R$ if and only if for every $0 \neq c \in R$, there exists an $e > 0$ and an R-linear map $\phi \colon R^{1/p^e} \to R$ which sends c^{1/p^e} to 1.*

Proof. We leave it to the reader to reduce to the case where R is a local ring with maximal ideal $\mathfrak{m}$. First suppose that $\tau(R) = R$. Choose a non-zero $c \in R$ and consider the ideal $\sum_{e \geq 0} \sum_{\psi} \psi((cR)^{1/p^e})$ where the inner sum runs over $\psi \in \mathrm{Hom}_R(R^{1/p^e}, R)$. Since $\tau(R) = R$, this sum must equal R as the sum is clearly compatible under all ψ. Therefore, since R is local, there exists an e with $\psi((cR)^{1/p^e}) \not\subseteq \mathfrak{m}$ and so $1 \in \psi((cR)^{1/p^e})$. Thus $1 = \psi((cd)^{1/p^e})$ for some $d \in R$ and so by setting $\phi(\_) = \psi(d^{1/p^e} \cdot \_)$ we have $1 = \phi(c^{1/p^e})$ as desired.

Conversely, suppose that the condition of the theorem is satisfied. It quickly follows that every non-zero ideal J which is ϕ-compatible for all $\phi \colon R^{1/p^e} \to R$ and all $e > 0$, satisfies $1 \in J$. Thus $\tau(R) = R$. $\square$

Definition 3.20. A ring R for which $\tau(R) = R$ is called *strongly F-regular*.

Theorem 3.21 ([69]). *A regular ring R is strongly F-regular.*

Proof. Left as an exercise to the reader (cf. Exercise 3.13). $\square$

Exercise 3.22 ([70, 71]). Prove that a strongly F-regular ring is Cohen–Macaulay.

Hint. Reduce to the case of a local ring $(R, \mathfrak{m})$ and find a non-zero element $c \in R$ which annihilates $H^i_{\mathfrak{m}}(R)$ for all $i < \dim R$. Now apply the functors $H^i_{\mathfrak{m}}(\_)$ to the homomorphism $R \to R^{1/p^e}$ which sends $1 \to c^{1/p^e}$. Next, apply the same functors to a map $\phi \colon R^{1/p^e} \to R$ which sends c^{1/p^e} to 1. Finally, use the criterion for checking whether a ring Cohen–Macaulay found in Appendix A, fact (iv).

Exercise 3.23 ([71]). Suppose that $R \subseteq S$ is a split inclusion of normal domains where S is strongly F-regular (e.g. if S is regular). Show that R is also strongly F-regular and in particular Cohen–Macaulay.

3.3 Test Ideals in Gorenstein Local Rings

Consider now that the ring R has a canonical module ω_R. Applying the functor $\mathrm{Hom}_R(\_, \omega_R)$ to the natural inclusion $R \subseteq R^{1/p^e}$, yields a map

$$\mathrm{Hom}_R(R^{1/p^e}, \omega_R) \to \omega_R.$$

Now, by Theorem A.8, we have $\operatorname{Hom}_R(R^{1/p^e}, \omega_R) \cong \omega_{R^{1/p^e}} = (\omega_R)^{1/p^e}$. Thus the map above may be viewed as a homomorphism

$$\Phi_R^e \colon \omega_R^{1/p^e} \to \omega_R.$$

In a Gorenstein local ring we know that $\omega_R \cong R$, and so we have a *nearly* canonical map $\Phi_R \colon R^{1/p^e} \to R$.

Setting. Throughout the rest of this subsection, we will assume that R is a Gorenstein[4] local domain essentially of finite type over a perfect field k, and the map $\Phi_R^e \colon R^{1/p^e} \to R$ is as described above.

Lemma 3.24 ([124, Lemma 7.1], cf. [107, Example 3.6]). *With notation as above, the R-linear map $\Phi_R^e \colon R^{1/p^e} \to R$ generates $\operatorname{Hom}_R(R^{1/p^e}, R)$ as an R^{1/p^e}-module.*

Proof. Left to the reader.   □

Remark 3.25. When one identifies R with ω_R, there is a choice to be made. In particular, using the above definition, Φ_R^e is *not* canonically determined in an absolute sense. Rather, $\Phi_R^e \in \operatorname{Hom}_R(R^{1/p^e}, R)$ is uniquely determined up to multiplication by a unit in R^{1/p^e}. Using the Cartier operator, however, it is possible to give a more canonical construction of Φ_R^e. See, for example [25], where Φ_R^e is called the *trace*.

Exercise 3.26. Suppose that $S = k[x_1, \ldots, x_n]$ where k is a perfect field and consider the S-linear map $\Psi \colon S^{1/p^e} \to S$ which sends $(x_1 \ldots x_n)^{(p^e-1)/p^e}$ to 1 and all other monomials of the free basis $\{x_1^{\lambda_1/p^e} \ldots x_n^{\lambda_n/p^e}\}_{0 \le \lambda_i \le p^e-1}$ to zero. Show that Ψ generates $\operatorname{Hom}_S(S^{1/p^e}, S)$ as an S-module, and thus that Ψ may be identified with Φ_S^e.

At first glance, writing Φ_R^e might seem in conflict with the exponential notation introduced in Lemma 3.6. However, it is not difficult to verify that – up to multiplication by a unit as in Remark 3.25 – one has $(\Phi_R^1)^e = \Phi_R^e$. See [99, Appendix F] or [124, Lemma 3.9, Corollary 3.10] for further details.

Theorem 3.27. *Suppose that R is Gorenstein and local and that Φ_R^e is as above (for any $e > 0$). Then $\tau(R) = \tau(R, \Phi_R^e)$.*

Proof. Certainly $\tau(R, \Phi_R^e) \subseteq \tau(R)$ since $\tau(R)$ is certainly Φ_R^e-compatible. For the converse inclusion, first note that by Exercise 3.9, $\tau(R, \Phi_R^e) = \tau(R, \Phi_R^d)$ for any

---

[4] Everything in this subsection can be immediately generalized to any ring satisfying $\omega_R \cong R$, a condition sometimes called quasi-Gorenstein, or 1-Gorenstein. It is possible to generalize many of the results in this setting to the $\mathbb{Q}$-Gorenstein setting as well. See Appendix A for additional definitions.

integer $d > 0$. So consider now some $\phi : F_*^d R \to R$. We know we can write $\phi(\_) = \Phi_R^d(c^{1/p^d} \cdot \_)$ for some element $c \in R^{1/p^d}$. Thus

$$\phi(\tau(R, \Phi_R^e)^{1/p^d}) = \Phi_R^d(c^{1/p^d} \tau(R, \Phi_R^d)^{1/p^d})$$

$$\subseteq \Phi_R^d(\tau(R, \Phi_R^d)^{1/p^d})$$

$$\subseteq \tau(R, \Phi_R^d) = \tau(R, \Phi_R^e)$$

and so $\tau(R) \subseteq \tau(R, \Phi_R^e)$ as desired. $\square$

Philosophical Statement 3.28. The previous theorem motivates the study of test ideal pairs $\tau(R, \phi)$. For example, consider the following situation. Suppose that R is a non-normal Gorenstein domain and that R^N is its normalization. By applying Exercise 3.18, it can be shown that every R-linear map $\phi: R^{1/p^e} \to R$ extends (uniquely) to a R^N-linear map $\overline{\phi}: (R^N)^{1/p^e} \to R^N$ (for details, see [25, Exercise 1.2.E(4)]).

In particular, $\Phi_R^e : R^{1/p^e} \to R$ extends to a map $\overline{\Phi_R^e}$ on the normalization as asserted above. However, even in the case where R^N is Gorenstein, $\overline{\Phi_R^e}$ is almost certainly not equal to $\Phi_{R^N}^e$. Nevertheless, it may still be advantageous to work on R^N, and the following exercise shows that $\tau(R)$ can be computed on the normalization.

Exercise* 3.29. Suppose that R is Gorenstein and R^N is its normalization (which is not assumed Gorenstein). Fix $\overline{\Phi_R^e}$ as above, show that $\tau(R^N, \overline{\Phi_R^e}) = \tau(R)$.

4 Connections with Algebraic Geometry

In this section we explain the connection between the test ideal and the multiplier ideal, a construction which first appeared in complex analytic geometry. We assume that the reader already has some familiarity with constructions such as divisors on normal algebraic varieties, a resolution of singularities, and the canonical divisor. Note that we have provided a brief review of divisors in Appendix B aimed at those mainly familiar with algebraic techniques. Further references for this section include [90], [100] or [15] (the latter giving a particularly satisfying introduction to multiplier ideals). Again, we remind the reader that the material in this section is *not* required to understand the sections that follow. See also Section 6.

Setting. Throughout this section, let R_0 be a normal domain of finite type over $\mathbb{C}$, and let $X_0 = \operatorname{Spec} R_0$ denote the corresponding affine algebraic variety.

4.1 Characteristic 0 Preliminaries

Before defining the multiplier ideal, we say a brief word about the type of resolution of singularities we consider.

Definition 4.1. Suppose that Y is a variety defined over $\mathbb{C}$. A proper birational map $\pi : Y' \to Y$ is called a *log resolution of singularities for Y* if π is proper and birational and Y' is smooth and $\text{exc}(\pi)$, the exceptional set of π, is a divisor with simple normal crossings (see Definition B.5 in the appendix). Given a closed subscheme $Z \subseteq Y$, π is called a *log resolution of singularities for $Z \subseteq Y$* if π is a log resolution of singularities for Y and if both $\pi^{-1}(Z)$ and $\pi^{-1}(Z) \cup \text{exc}(\pi)$ are divisors with simple normal crossings.

We first define the multiplier ideal of R_0 in the case that R_0 is Gorenstein. Let $\pi : \widetilde{X}_0 \to X_0$ be a log resolution of singularities, and choose a canonical divisor $K_{\widetilde{X}_0}$ on $\widetilde{X}_0$, in other words, we choose a divisor $K_{\widetilde{X}_0}$ such that $\mathcal{O}_{\widetilde{X}_0}(K_{\widetilde{X}_0}) = \wedge^{\dim \widetilde{X}_0} \Omega_{\widetilde{X}_0/\mathbb{C}}$. We then obtain a *canonical divisor* on X_0 as follows. Set K_{X_0} to be the (unique) divisor on X_0 which agrees with $K_{\widetilde{X}_0}$ wherever π is an isomorphism. We now can define the multiplier ideal of X_0.

Definition 4.2. Consider the module $\Gamma(\widetilde{X}_0, \mathcal{O}_{\widetilde{X}_0}(\lceil K_{\widetilde{X}_0} - \pi^* K_{X_0} \rceil))$. This module is called the *multiplier ideal* and is denoted by $\mathcal{J}(X_0)$. It is independent of the choice of resolution.

Of course, it is natural to ask why this module is an ideal. However, set $U = \widetilde{X}_0 \setminus \text{exc}(\pi)$ which is an open subset of both $\widetilde{X}_0$ and X_0 (in fact, $X_0 \setminus U$ has codimension at least 2). We have the natural inclusion

$$\Gamma(\widetilde{X}_0, \mathcal{O}_{\widetilde{X}_0}(K_{\widetilde{X}_0} - \pi^* K_{X_0})) \subset \Gamma(U, \mathcal{O}_{\widetilde{X}_0}(K_{\widetilde{X}_0} - \pi^* K_{X_0}))$$

But $(K_{\widetilde{X}_0} - \pi^* K_{X_0})|_U$ is zero, so the right side is just $\Gamma(U, \mathcal{O}_{X_0}) = R_0$ because R is S2; see [61, Chapter III, the method of Exercise 3.5] and [63, Proposition 1.11].

The multiplier ideal has been discovered and re-discovered in many contexts. At least as early as [47], it was noted that $\mathcal{J}(X_0)$ is independent of the choice of resolution and might be an interesting object to study. Variants of the multiplier ideals described also appeared throughout the work of Joseph Lipman and others in the 1970's, see for example [103]. However, multiplier ideals have been most useful in the context of pairs (definitions will be provided below) and first appeared independently in the works of Nadel [119], from the analytic perspective, as well as Lipman [104], from the perspective of commutative algebra. However, the fundamental algebro-geometric theory of multiplier ideals was worked out even earlier without the formalism of multiplier ideals by Esnault–Viehweg in relation to Kodaira-vanishing and its generalization, Kawamata–Viehweg vanishing; see [86], [160] and [43].

Remark 4.3. Smooth varieties have multiplier ideal $\mathcal{J}(X_0) = \mathcal{O}_{X_0}$. The easiest way to see this is to simply take π as the identity (in other words, take X_0 as its own resolution). In general, the more severe the singularities of X_0, the smaller the ideal $\mathcal{J}(X_0)$ is.

Example 4.4. Consider the following $X_0 = \operatorname{Spec} \mathbb{C}[x, y, z]/\langle x^3 + y^3 + z^3 \rangle = \operatorname{Spec} R_0$. Because this is a cone over a smooth variety (an elliptic curve), it has a resolution $\widetilde{X}_0 \to X_0$ obtained by blowing up the origin. We embed $X_0 \subseteq \mathbb{C}^3$ in the obvious way and blow up the origin in $\mathbb{C}^3$ to obtain a log resolution $\pi : Y \to \mathbb{C}^3$ of X_0 inside $\mathbb{C}^3$.

$$
\begin{array}{ccc}
E \lhook\joinrel\longrightarrow & \widetilde{X}_0 \lhook\joinrel\longrightarrow & Y \\
\downarrow & \downarrow & \downarrow{\scriptstyle \pi} \\
\{\mathrm{pt}\} \lhook\joinrel\longrightarrow & X_0 \lhook\joinrel\longrightarrow & \mathbb{C}^3.
\end{array}
$$

Here E is the elliptic curve obtained by blowing up the cone point in X_0. We know $K_Y = 2F$ where $F \cong \mathbb{P}^2_{\mathbb{C}}$ is the exceptional divisor of π by [61, Chapter 8.5(b)], thus we set $K_{\mathbb{C}^3} = 0$. It follows that $K_Y + \widetilde{X}_0 = 2F + \widetilde{X}_0$. On the other hand, we know $\pi^* X_0 = \widetilde{X}_0 + 3F$, where the 3 comes from the fact that $x^3 + y^3 + z^3$ vanishes to order 3 at the origin (the point being blown-up). Therefore,

$$ K_Y + \widetilde{X}_0 = 2F + \widetilde{X}_0 = \pi^* X_0 - F. $$

Now, $X_0 \sim 0$ in $\operatorname{Pic}(\mathbb{C}^3) = 0$, so $\pi^* X_0 \sim 0$ also. Thus $K_Y + \widetilde{X}_0 \sim -F$ and so by the adjunction formula (in the form of [61, Chapter II, Ex. 8.20]),

$$ K_{\widetilde{X}_0} \sim (K_Y + \widetilde{X}_0)|_{\widetilde{X}_0} \sim (-F)|_{\widetilde{X}_0} \sim -E. $$

So we set $K_{\widetilde{X}_0} = -E$ and then see that the corresponding $K_{X_0} = 0$ (since that is the divisor that agrees with $\sim -E$ outside of exceptional locus).

Therefore, $\mathcal{O}_{\widetilde{X}_0}(K_{\widetilde{X}_0} - \pi^* K_{X_0}) = \mathcal{O}_{\widetilde{X}_0}(-E)$. This sheaf can be thought of as the sheaf of functions in the fraction field of R_0 which vanish to order 1 along E and have no poles. It is then clear that $\Gamma\left(U, \mathcal{O}_{X_0}\right)$ is just the maximal ideal of the origin in R_0.

Exercise 4.5. Compute the multiplier ideal of $\operatorname{Spec} \mathbb{C}[x, y, z]/\langle x^n + y^n + z^n \rangle$ for arbitrary $n > 1$.

4.2 Reduction to Characteristic $p > 0$ and Multiplier Ideals

We now relate the multiplier ideal and the test ideal. We need to briefly describe *reduction to characteristic p,* a method of translating varieties in characteristic zero to characteristic $p > 0$. We make many simplifying assumptions and so we refer the reader to [147], [73], or [76] for a more detailed description of the reduction to positive characteristic process in this context.

Suppose that $X_0 = \operatorname{Spec} R_0 = \operatorname{Spec} \mathbb{C}[x_1, \dots, x_n]/I \subseteq \mathbb{C}^n$. We write $I = \langle f_1, \dots, f_m \rangle$ where the f_i are polynomials. For simplicity, we assume that all of the coefficients of the f_i are integers. We set $R_{\mathbb{Z}}$ to be the ring $\mathbb{Z}[x_1, \dots, x_n]/\langle f_1, \dots, f_m \rangle$. For each prime integer p, consider the ring $R_p := R_{\mathbb{Z}}/p R_{\mathbb{Z}} \cong (\mathbb{Z}/p\mathbb{Z})[x_1, \dots, x_n]/\langle f_1 \mod p, \dots, f_m \mod p \rangle$ and the associated scheme $X_p = \operatorname{Spec} R_p$. The scheme

X_p is called a characteristic $p > 0$ model for X_0, and for large $p \gg 0$, X_p and X_0 share many properties. For example, R_p is regular for large $p \gg 0$ if and only if R_0 is regular, [73]. Given an ideal $J_0 \subseteq R_0$, we may also reduce it to positive characteristic by viewing a set of defining equations modulo p, to obtain an ideal J_p (of course, J_p might depend on the particular generators of J chosen in small characteristics).

Remark 4.6. If the f_i are not defined over $\mathbb{Z}$, instead of working with $R_{\mathbb{Z}}$, one should work with $R_A = A[x_1, \ldots, x_n]/\langle f_1, \ldots, f_m \rangle$ where A is the $\mathbb{Z}$-algebra generated by the coefficients of the f_i (and the coefficients of any other ideals one wishes to reduce to characteristic $p > 0$). Instead of working modulo prime integers, one should quotient out by maximal ideals of A.

Containments and equality (or non-containments and non-equality) of ideals are preserved after reduction to characteristic $p \gg 0$. By viewing finitely generated R_0-modules as quotients of $R_0^{\oplus n}$, one can likewise reduce finitely generated modules to positive characteristic. Maps between such modules can then be represented as matrices, which themselves can be reduced to characteristic $p > 0$, and properties of those maps, such as injectivity, non-injectivity, surjectivity and non-surjectivity are also be preserved for $p \gg 0$. In particular, if a map of modules is an isomorphism after reduction to characteristic $p \gg 0$, then it is an isomorphism in characteristic zero as well.

Now, if $\pi : \widetilde{X}_0 \to X_0$ is a resolution of the singularities of X_0 obtained by blowing up an ideal J_0, then we may reduce J_0 to J_p, and then blow that up to obtain $\pi_p : \widetilde{X}_p \to X_p$, which is also a resolution of singularities for all $p \gg 0$ (of course, the existence of resolutions of singularities for arbitrary varieties in characteristic $p > 0$ is still an open question [7, 28, 29, 30]). Finally, the multiplier ideal $\mathcal{J}(X)_p$ (the multiplier ideal reduced to characteristic p) coincides with the characteristic $p > 0$ multiplier ideal $\mathcal{J}(X_p) := \Gamma(X_p, \mathcal{O}_{\widetilde{X}_p}(K_{\widetilde{X}_p} - \pi_p^* K_{X_p}))$ for $p \gg 0$. Again, we suggest the reader see [147], [73], or [76] for a much more detailed description of the reduction to characteristic $p > 0$ process.

Theorem 4.7 ([53, 146]). *Suppose that R_0 is a Gorenstein ring in characteristic 0 with $X_0 = \operatorname{Spec} R_0$. Then $\mathcal{J}(X_0)_p = \tau(X_p)$ for all $p \gg 0$.*

Proof. We will only prove the $\supseteq$ containment. As above, we choose $\pi : \widetilde{X}_0 \to X_0$ to be a log resolution of singularities which we reduce to a positive characteristic resolution of singularities $\pi_p : \widetilde{X}_p \to X_p$. We have the following commutative diagram of schemes in characteristic $p > 0$

$$
\begin{array}{ccc}
\widetilde{X}_p & \xrightarrow{\ F\ } & \widetilde{X}_p \\
{\scriptstyle \pi_p} \downarrow & & \downarrow {\scriptstyle \pi_p} \\
X_p & \xrightarrow[\ F\ ]{} & X_p
\end{array}
$$

where the maps labeled F are the Frobenius maps. By duality, see Corollary A.12, we have the following diagram of obtained from canonical modules.

$$
\begin{array}{ccc}
\Gamma(\widetilde{X}_p, \omega_{\widetilde{X}_p}) & \xrightarrow{\Phi_{\widetilde{X}_p}} & \Gamma(\widetilde{X}_p, \pi_* \omega_{\widetilde{X}_p}) \\
\downarrow & & \downarrow \\
\Gamma(X_p, \omega_{X_p}) & \xrightarrow[\Phi_{X_p}]{} & \Gamma(X_p, \omega_{X_p}).
\end{array}
$$

By working on a sufficiently small affine chart, because X_0 and thus X_p is Gorenstein, we may assume that $\Gamma(X_p, \omega_{X_p}) \cong R_p$ and thus assume that Φ_{X_p} is the map Φ_{R_p} discussed in Subsection 3.3.

The image of the vertical maps is the multiplier ideal $\mathcal{J}(X_p)$ and so it follows from the diagram that the multiplier ideal is Φ_R-compatible. Thus $\mathcal{J}(X_p) \supseteq \tau(R_p)$ as long as $\mathcal{J}(X_p) \neq 0$ by Theorem 3.27. But $\mathcal{J}(X_p)$ is non-zero because π is an isomorphism at the generic points of X_p and $\widetilde{X}_p$. $\qquad\square$

Exercise* 4.8. While the result above holds for $p \gg 0$, it does not necessarily hold for small $p > 0$. Consider the ring $R = \mathbb{F}_2[x, y, z]/\langle z^2 + xyz + xy^2 + x^2 y \rangle$. Verify the following:

(i) R is F-pure (use Fedder's criterion).

(ii) R is not strongly F-regular (show that $\tau(R) = \langle x, y, z \rangle$).

(iii) The singularities of R can be resolved in characteristic 2 and furthermore, $\mathcal{J}(R) = R$ (use the method of Example 4.4). This is more involved.

Also see [10] and [132, Example 7.12].

4.3 Multiplier Ideals of Pairs

We have so far only defined the multiplier ideal for a Gorenstein ring. We now consider a more general setting.

Definition 4.9. Suppose that X is a normal variety of any characteristic. Then a $\mathbb{Q}$-divisor Δ is a formal sum of prime Weil divisors with rational coefficients (in other words, a $\mathbb{Q}$-divisor is just a divisor where we allow rational coefficients). A $\mathbb{Q}$-divisor Δ is called *effective* if all its coefficients are positive. Two $\mathbb{Q}$-divisors Δ_1 and Δ_2 are said to be $\mathbb{Q}$-*linearly equivalent*, denoted $\Delta_1 \sim_{\mathbb{Q}} \Delta_2$, if there exists an integer $n > 0$ such that $n\Delta_1$ and $n\Delta_2$ are linearly equivalent Weil divisors. We say that a $\mathbb{Q}$-divisor Γ is $\mathbb{Q}$-*Cartier* if there exists an integer n such that $n\Gamma$ is an integral Cartier divisor. In that case, the *index of* Γ is the smallest positive integer n such that $n\Gamma$ is an integral Cartier divisor. See Appendix B for a more detailed discussion from an algebraic perspective.

Instead of working with an arbitrary variety, one often works with a pair.

Definition 4.10. A *log $\mathbb{Q}$-Gorenstein pair* (or simply a *pair* if the context is understood) is the data of a normal variety X of any characteristic and an effective $\mathbb{Q}$-divisor Δ such that $K_X + \Delta$ is $\mathbb{Q}$-Cartier. A pair is denoted by (X, Δ). The *index of* (X, Δ) is defined to be the index of $K_X + \Delta$.

Remark 4.11. There are many reasons why one should consider pairs. Of course, you might be interested in a divisor inside an ambient variety, and pairs are natural in that context. Also, not all varieties are Gorenstein, and log $\mathbb{Q}$-Gorenstein pairs have associated multiplier ideals (as we'll see shortly). Another reason that pairs occur is if one changes the variety. In particular, suppose that $Y \to X$ is a morphism of varieties; for example, a closed immersion, a blow-up, a finite map, or a fibration. Then in many cases properties of X (respectively Y) can be detected by studying an appropriate pair (X, Δ) (respectively (Y, Δ)), see for example [85] or [87]. However, many of the deepest applications of multiplier ideals of pairs are revealed by observing the behavior of the multiplier ideal as the coefficients of Δ vary. This is not a topic we will explore in this article. We invite the reader to see [33, 35, 100, 140, 141] for more background.

Before we define the multiplier ideal, we first we state how to pull-back $\mathbb{Q}$-Cartier divisors. Suppose that Γ is a $\mathbb{Q}$-Cartier divisor on X and $\pi : Y \to X$ is a birational map from a normal variety Y. Choose n such that $n\Gamma$ is Cartier and define $\pi^*\Gamma$ to be $\frac{1}{n}\pi^*(n\Gamma)$.

Definition 4.12. Suppose that (X_0, Δ_0) is a log $\mathbb{Q}$-Gorenstein pair in characteristic zero. Set $\pi : \widetilde{X}_0 \to X_0$ to be a log resolution of singularities of a pair (X_0, Δ_0) (in other words, we also assume that $\mathrm{Supp}(\pi^{-1}\Delta_0) \cup \mathrm{exc}(\pi)$ is a simple normal crossings divisor). Consider the module $\Gamma(\widetilde{X}_0, \mathcal{O}_{\widetilde{X}_0}(K_{\widetilde{X}_0} - \pi^*(K_{X_0} + \Delta_0)))$. This module is called the *multiplier ideal* and is denoted by $\mathcal{J}(X_0, \Delta_0)$. It is independent of the choice of log resolution.

We say that (X_0, Δ_0) has *log terminal singularities* if $\mathcal{J}(X_0, \Delta_0) = \mathcal{O}_{X_0}$. For more about log terminal singularities, see [90] and [92].

Exercise 4.13. Suppose that (X_0, Δ_0) is a pair where X is smooth and Δ_0 has simple normal crossings support. Show that $\mathcal{J}(X_0, \Delta_0) = \mathcal{O}_{X_0}(-\lfloor \Delta_0 \rfloor)$.

Exercise 4.14. Suppose that X_0 is smooth and that D is an effective Cartier divisor on X_0. Prove that $\mathcal{J}(X_0, D) = \mathcal{O}_{X_0}(-D)$.

Hint. Use the projection formula, [61, Chapter II, Exercise 5.1(d)]

4.4 Multiplier Ideals vs. Test Ideals of Divisor Pairs

Previously we considered test ideals of pairs (R, ϕ) where R is a ring of characteristic p and $\phi : R^{1/p^e} \to R$ is an R-linear map. We will see that this pair is essentially the same data as a log $\mathbb{Q}$-Gorenstein pair (X, Δ).

Setting. Throughout this subsection, R is used to denote a *normal* ring essentially of finite type over a perfect field of characteristic $p > 0$. Furthermore, $X = \operatorname{Spec} R$.

Suppose we are given a $\phi \in \operatorname{Hom}_R(R^{1/p^e}, R)$. The module $\operatorname{Hom}_R(R^{1/p^e}, R)$ is S2 both as an R-module and as an R^{1/p^e}-module. Therefore it is determined by its localizations outside a set $Z \subseteq X$ of codimension 2 (the singular locus), see [62, Theorem 1.12]. We set U to be the smooth locus of X and consider the sheaf $\mathscr{H}\mathrm{om}_{\mathcal{O}_U}(\mathcal{O}_U^{1/p^e}, \mathcal{O}_U)$. Tensoring with $\omega_U = \mathcal{O}_U(K_U)$ and using the projection formula, we see that this module is isomorphic to

$$
\begin{aligned}
\mathscr{H}\mathrm{om}_{\mathcal{O}_U}&(\mathcal{O}_U^{1/p^e} \otimes_{\mathcal{O}_U} \mathcal{O}_U(K_U), \mathcal{O}_U(K_U)) \\
&\cong \mathscr{H}\mathrm{om}_{\mathcal{O}_U}((\mathcal{O}_U(p^e K_U))^{1/p^e}, \mathcal{O}_U(K_U)) \\
&\cong (\mathscr{H}\mathrm{om}_{\mathcal{O}_U}(\mathcal{O}_U(p^e K_U), \mathcal{O}_U(K_U)))^{1/p^e} \\
&\cong (\mathcal{O}_U((1 - p^e)K_U))^{1/p^e}.
\end{aligned}
$$

Here the first isomorphism is due to the projection formula and the fact that $(F^e)^* \mathscr{L} = \mathscr{L}^{p^e}$ for any line bundle $\mathscr{L}$. The second isomorphism is Theorem A.8 from the Appendix. The last isomorphism is just [61, Chapter II, Exercise 5.1(b)].

Because $\operatorname{Hom}_R(R^{1/p^e}, R)$ is S2, it is determined on U, see [62, Theorem 1.12]. Therefore,

$$
\begin{aligned}
\operatorname{Hom}_R(R^{1/p^e}, R) &\cong \operatorname{Hom}_{\mathcal{O}_U}(\mathcal{O}_U^{1/p^e}, \mathcal{O}_U) \\
&\cong \Gamma(U, (\mathcal{O}_U((1 - p^e)K_U))^{1/p^e}) \\
&\cong \Gamma(X, (\mathcal{O}_X((1 - p^e)K_X))^{1/p^e}).
\end{aligned}
$$

Of course, $(\mathcal{O}_X((1 - p^e)K_X))^{1/p^e}$ is abstractly isomorphic to $\mathcal{O}_X((1 - p^e)K_X)^{1/p^e}$. Therefore, ϕ may be viewed as a global section of $\mathcal{O}_X((1 - p^e)K_X)$. In particular, by [61, Proposition 7.7] which also works for reflexive rank-1 sheaves on normal varieties, ϕ determines an effective divisor D_ϕ linearly equivalent to $(1 - p^e)K_X$. Set

$$
\Delta_\phi := \frac{1}{p^e - 1} D_\phi.
$$

Exercise 4.15. If $R = \mathbb{F}_p[x, y]$, find ϕ such that Δ_ϕ is the sum of the two coordinate axes (in other words, that $\Delta_\phi = \operatorname{div}(xy)$). Find a ϕ such that $\Delta_\phi = 0$.

It is straightforward check that there is a bijection between the following two sets, see [124, Theorems 3.11, 3.13].

$$\left\{ \begin{array}{c} \text{Non-zero } R\text{-linear maps} \\ \phi : F_*^e R \to R \text{ up to} \\ \text{pre-multiplication by units.} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Effective } \mathbb{Q}\text{-divisors } \Delta \\ \text{on } X = \operatorname{Spec} R \text{ such that} \\ (1 - p^e)(K_X + \Delta) \sim 0. \end{array} \right\} . \quad (4.15.1)$$

Exercise* 4.16 ([126, Proof of Theorem 6.7], cf. [57, Proof of the main theorem]). Suppose that $\phi : R^{1/p^e} \to R$ is a non-zero R-linear map and that $\pi : \widetilde{X} \to X = \operatorname{Spec} R$ is a birational map where $\widetilde{X}$ is normal. Prove that ϕ induces a map

$$(\mathcal{O}_{\widetilde{X}}(\lceil K_{\widetilde{X}} - \pi^*(K_X + \Delta_\phi) \rceil))^{1/p^e} \to \mathcal{O}_{\widetilde{X}}(\lceil K_{\widetilde{X}} - \pi^*(K_X + \Delta_\phi) \rceil)$$

which agrees with ϕ wherever π is an isomorphism.

Theorem 4.17 ([151, Theorem 3.2]). *Suppose that $X_0 = \operatorname{Spec} R_0$ is a variety of finite type over $\mathbb{C}$ and that (X_0, Δ_0) is a log $\mathbb{Q}$-Gorenstein pair. Then, after reduction to characteristic $p \gg 0$, $(\mathcal{J}(X_0, \Delta_0))_p = \tau(X_p, \phi_{\Delta_p})$ where ϕ_{Δ_p} is a map corresponding to Δ_p as in (4.15.1) above.*

Proof. We only briefly sketch the proof. By working on a smaller affine chart if necessary, we may assume that $n(K_{X_0} + \Delta_0) \sim 0$ for some integer n. We reduce both X_0 and Δ_0 (and a log resolution) to characteristic p and notice that if $n(K_{X_0} + \Delta_0) \sim 0$, then that property is preserved after reduction to characteristic $p \gg 0$. Thus we may always assume that there exists an $e > 0$ such that $(1 - p^e)(K_{X_p} + \Delta_p)$ is Cartier. We set ϕ_{Δ_p} to be a map corresponding to Δ_p via (4.15.1) above.

Now use the exercise 4.16 above to show that $\mathcal{J}(X_0, \Delta_0)_p = \mathcal{J}(X_p, \Delta_p)$ is ϕ-compatible. Thus the inclusion $\supseteq$ is rather straightforward. The converse inclusion requires additional techniques that we will not cover here. $\square$

Remark 4.18. While multiplier ideals are quite closely to test ideals, many basic properties which hold for multiplier ideals fail spectacularly for test ideals. For example, it follows immediately from the definition that every multiplier ideal is integrally closed (we suggest the reader prove this as an exercise). However, not every test ideal is integrally closed [108] and furthermore, every ideal in a regular ring is the test ideal of an appropriate pair $\tau(R, \langle f \rangle^t)$, see [118] (here $(R, \langle f \rangle^t)$ is a pair as discussed in Section 6 below).

5 Tight Closure and Applications of Test Ideals

In this section we survey the test ideal's historic connections with tight closure theory. It is not necessary to read this section in order to understand later sections. We should also mention that as a survey of tight closure, this section is completely inadequate.

Some important aspects of tight closure theory are completely missing (for example, phantom homology). Again, we refer the reader to the book [76] or [27, Chapter 10] for a more complete account.

Setting. In this section, all rings are assumed to be integral domains essentially of finite type over a perfect field of characteristic $p > 0$.

Suppose that $R \subseteq S$ is an extension of rings. Consider an ideal $I \subseteq R$ and its extension IS. We always have that $(IS) \cap R \supseteq I$, however:

Lemma 5.1. *With $R \subseteq S$ as above and further suppose the extension splits as a map of R-modules. Then*
$$(IS) \cap R = I.$$

Proof. Fix $\phi : S \to R$ to be the splitting given by hypothesis. Suppose that $z \in (IS) \cap R$, in other words, $z \in IS$ and $z \in R$. Write $I = \langle x_1, \ldots, x_n \rangle$, we know that there exists $s_i \in S$ such that $z = \sum s_i x_i$. Now, $z = \phi(z) = \phi\left(\sum s_i x_i\right) = \sum x_i \phi(s_i) \in I$ as desired. $\square$

A converse result holds too.

Theorem 5.2 ([67]). *Suppose that $R \subseteq S$ is a finite extension of approximately Gorenstein[5] rings, a condition which every ring in this section automatically satisfies. If for every ideal $I \subseteq R$, we have $IS \cap R = S$, then $R \subseteq S$ splits as a map of R-modules.*

Proof. See [67] $\square$

Consider now what happens if the extension $R \subseteq S$ is the Frobenius map. Recall from Definition 2.11 that if $I = \langle x_1, \ldots, x_m \rangle$, then $I^{[p^e]} = \langle x_1^{p^e}, \ldots, x_m^{p^e} \rangle$. It is an easy exercise to verify that this is independent of the choice of generators x_i.

Exercise 5.3. Notice that R is abstractly isomorphic to R^{1/p^e} as a ring. Show that under this isomorphism, $I^{[p^e]}$ corresponds to the extended ideal $I(R^{1/p^e})$ coming from $R \subseteq R^{1/p^e}$.

Definition 5.4. Given an ideal $I \subseteq R$, the *Frobenius closure of I* (denoted I^F) is the set of all elements $z \in R$ such that $z^{p^e} \in I^{[p^e]}$ for some $e > 0$. Equivalently, it is equal to the set of all elements $z \in R$ such that $z \in (IR^{1/p^e})$ for some $e > 0$.

Remark 5.5. The set I^F is an ideal. Explicitly, if $z_1, z_2 \in I^F$, then $z_1^{p^a} \in I^{[p^a]}$ and $z_2^{p^b} \in I^{[p^b]}$. Notice that we may assume that $a = b$. Thus $z_1 + z_2 \in I^F$. On the other hand, clearly $hz_1 \in I^F$ for any $h \in R$.

---

[5] Nearly all rings in geometry satisfy this condition. Explicitly, a local ring $(R, \mathfrak{m})$ is called approximately Gorenstein if for every integer $N > 0$, there exists $I \subseteq \mathfrak{m}^N$ such that R/I is Gorenstein.

We point out a several basic facts about I^F mostly for comparison with tight closure (defined below).

Proposition 5.6. *Fix R to be a domain and $\langle x_1, \ldots, x_n \rangle = I \subseteq R$ an ideal.*

  (i) $(I^F)^F = I^F$.

 (ii) *For any multiplicative set W, $(W^{-1}I)^F = W^{-1}(I^F)$.*

(iii) *R is F-split if and only if $I = I^F$ for all ideals $I \subseteq R$.*

Proof. The proof of property (i) is left to the reader. For (ii), we note that ($\supseteq$) is obvious. Conversely, suppose that $z \in (W^{-1}I)^F$, thus $z^{p^e} \in (W^{-1}I)^{[p^e]} = W^{-1}(I^{[p^e]})$. Therefore, for some $w \in W$, $wz^{p^e} \in I^{[p^e]}$, which implies that $(wz)^{p^e} \in I^{[p^e]}$ and the converse inclusion holds. Part (iii) is obvious by Theorem 5.2. $\qquad\square$

Now we define tight closure.

Definition 5.7 ([70]). Suppose that R is an F-finite domain and I is an ideal of R, then the *tight closure of I* (denoted I^*) is defined to be the set

$$\{z \in R \mid \exists\, 0 \neq c \in R \text{ such that } cz^{p^e} \in I^{[p^e]} \text{ for all } e \geq 0\}.$$

It should be noted that tight closure is notoriously difficult to compute. For a survey on computations of tight closure (using highly geometric methods) we suggest reading [23]. Also see [20, 21, 81, 136].

Proposition 5.8. *Suppose we have an ideal $\langle x_1, \ldots, x_n \rangle = I \subseteq R$ where R is an F-finite domain.*

  (i) *I^* is an ideal containing I, [70, Proposition 4.1(a)].*

 (ii) *$(I^*)^* = I^*$, [70, Proposition 4.1(e)].*

(iii) *It is known that the formation of I^* does NOT commute with localization, [24].*

(iii′) *If I is generated by a system of parameters, then the formation of I^* does commute with localization, [4, 142].*

(iv) *If $\tau(R) = R$, then $I^* = I$ for all ideals I, [69, Theorem 3.1(d)].*

 (v) *We always have the containment $I^* \subseteq \overline{I}$ where $\overline{I}$ is the integral closure of I, [70, Theorem 5.2].*

Proof. For (i), suppose that $cz^{p^e} \in I^{[p^e]}$ and $dy^{p^e} \in I^{[p^e]}$ for all $e \geq 0$ for certain $c, d \in R \setminus \{0\}$. Then $cd(z+y)^{p^e} \in I^{[p^e]}$ for all $e \geq 0$. Of course, clearly I^* contains I (choose $c = 1$). Property (ii) is left to the reader. The proof of (iii) is beyond the scope of this survey, see [24]. The proof of (iii′) can be found in [142] where it is actually shown that tight closure coincides with plus-closure.

For (iv), suppose that $z \in I^*$ and $\tau(R) = R$. Choose $c \neq 0$ such that $cz^{p^e} \in I^{[p^e]}$ for all $e \geq 0$. We know that there exists an $e > 0$ and $\phi : R^{1/p^e} \to R$ which sends c

to 1. Write $cz^{p^e} = \sum a_i x_i^{p^e}$. Then $z = \phi(cz^{p^e}) = \sum x_i \phi(a_i) \in I$. For (v) we give a hint in the form of a characterization of $\overline{I}$. One has $x \in \overline{I}$ if and only if there exists $0 \neq c \in R$ such that $cx^n \in I^n$ for all $n > 0$. □

We now state some important additional more subtle properties of tight closure.

Theorem 5.9 ([27, Chapter 10; 76; 147, Section 1.3]).

- *(Persistence) Given any map of rings $R \to S$, $I^*S \subseteq (IS)^*$.*

- *(Finite extensions) If $R \subseteq S$ is a finite extension of rings, then $(IS) \cap R \subseteq I^*$ for all ideals $I \subseteq R$. Also see [142].*

- *(Colon Capturing) If R is local and $x_1, \ldots, x_d$ is a system of parameters for R, then we have $(x_1, \ldots, x_i) :_R x_{i+1} \subseteq (x_1, \ldots, x_i)^*$.*

Perhaps the most important open problem in tight closure theory is the following.

Conjecture 5.10. R is strongly F-regular if and only if $I^* = I$ for all ideals I.

Remark 5.11. A number of special cases of this conjecture are known; see [76, Theorem 12.2], [106], [107], [6] and [149]. One should note that the method of Lemma 5.1 immediately yields the ($\Rightarrow$) implication.

In fact, one can also simply use tight closure of ideals to define a slightly different variant of test ideals.

Definition 5.12. Suppose that R is a domain essentially of finite type over a perfect field. Define $\tau_{\mathrm{fg}}(R)$ to be $\bigcap_{I \subseteq R}(I :_R I^*)$. This ideal is called the *finitistic test ideal* or sometimes the *classical test ideal*.

Remark 5.13. The definition of the test ideal in this article is non-standard. Normally $\tau_{\mathrm{fg}}(R)$ is called the *test ideal*, while the ideal we denoted by $\tau(R)$ is called the *non-finitistic test ideal*, or sometimes the *big test ideal* and is commonly denoted by $\widetilde{\tau}(R)$ or $\tau_b(R)$. It is hoped that these two potentially different ideals always coincide, see the conjecture below. However, even if they do not, there now seems to be consensus that the *non-finitistic test ideal* is the better notion.

Conjecture 5.14. The ideals $\tau_{\mathrm{fg}}(R)$ and $\tau(R)$ coincide.

Exercise 5.15 (cf. [107, Theorem 7.1(4)]). Prove that $\tau(R) \subseteq \tau_{\mathrm{fg}}(R)$.

Exercise 5.16 ([45, Proposition 2.5]). Suppose that R is F-pure, show that $\tau_{\mathrm{fg}}(R)$ is a radical ideal.

5.1 The Briançon–Skoda Theorem

Now we move on to one of the classical applications of tight closure theory, a very simple proof of the Briançon–Skoda theorem.

Theorem 5.17 ([70, Theorem 5.4]). *Let R be an F-finite domain, and $(u_1, \ldots, u_n) = I \subseteq R$ an ideal. Then for every natural number m,*

$$\overline{I^{m+n}} \subseteq \overline{I^{m+n-1}} \subseteq (I^m)^*$$

and so

$$\tau(R)\overline{I^{m+n}} \subseteq \tau_{\mathrm{fg}}(R)\overline{I^{m+n}} \subseteq I^m.$$

This gives a particularly nice statement in the case that R is strongly F-regular (because $\tau(R) = R$).

Proof from [68]. For any $y \in \overline{I^{m+n-1}}$, we know that there exists $0 \neq c \in R$ such that $cy^l \in (I^{m+n-1})^l$ for all $l \geq 0$, see [79, Exercise 1.5]. Consider a monomial $u_1^{a_1} \ldots u_n^{a_n}$ where $a_1 + \cdots + a_n = l(m + n - 1)l$. Write each $a_i = b_i l + r_i$ where $0 \leq r_i \leq l - 1$. We claim that the sum of the b_i is at least m, which will imply that the monomial is contained in $(I^m)^{[l]}$ for all l such that $l = p^e$. However, if the sum $b_1 + \cdots + b_m \leq m - 1$, then $l(m + n - 1) = \sum a_i \leq l(m - 1) + n(l - 1) = l(m + n - 1) - n < l(m + n - 1)$, which implies the claim.
   Thus $cy^{p^e} \in I^{[p^e]}$ and so $y \in (I^m)^*$ as desired.   □

Exercise 5.18. Following the method in the above proof, if $\mathfrak{a}$ is an ideal generated by r elements, show that $\mathfrak{a}^{rp^e} \subseteq \mathfrak{a}^{[p^e]}\mathfrak{a}^{(r-1)p^e}$ for all $e \geq 0$.

5.2 Tight Closure for Modules and Test Elements

Definition 5.19. Suppose that R is a domain and that M is an R-module. We define the *tight closure of 0 in M*, denoted 0_M^* as follows.

$$0_M^* = \{m \in M \mid \exists 0 \neq c \in R, \text{ such that } 0 = m \otimes c^{1/p^e} \in M \otimes_R R^{1/p^e} \text{ for all } e \geq 0.\}$$

If $0_M^* = 0$, then we say that 0 *is tightly closed in M*.

Remark 5.20. More generally, given a submodule $N \subseteq M$, one can define $N_M^* \subseteq M$, the *tight closure of N in M*. However, this submodule is just the pre-image of $0_{M/N}^* \subseteq M/N$ under the natural surjection $M \to M/N$, see [70, Remark 8.4].

   It is known that a ring is strongly F-regular if and only if 0 is tightly closed in every module, [68]. By Remark 5.20, note that $I^* = I$, if and only if $0_{R/I}^* = 0$.
   We conclude with one more definition.

Definition 5.21. An element $0 \neq c \in R$ is called a *finitistic test element* if for every ideal $I \subseteq R$ and every $z \in I^*$, we have

$$cz^{p^e} \in I^{[p^e]}.$$

An element $0 \neq c \in R$ is called a *(big) test element* if for every R-module M and every $z \in 0_M^*$, we have

$$0 = z \otimes c^{1/p^e} \in M \otimes_R R^{1/p^e}.$$

Theorem 5.22. *Suppose that $c \in R$ is chosen as in Lemma 3.6 for some non-zero R-linear map $\phi : R^{1/p^e} \to R$. Then c is a finitistic test element and a big test element.*

Proof. First consider the finitistic case.

Suppose that $z \in I^*$. Then there exists a $0 \neq d \in R$ such that $dz^{p^e} \in I^{[p^e]}$ for all $e \geq 0$. Fix $\phi : R^{1/p} \to R$. It follows from Lemma 3.6 that there exists an integer $e_0 > 0$ such that $\phi^{e_0}(d^{1/p^{e_0}}) = c$. Applying ϕ^{e_0} to the equation $dz^{p^e} \in I^{[p^e]}$ for $e \geq e_0$ yields

$$cz^{p^{e-e_0}} \in \phi^{e_0}(I^{[p^e]}) \subseteq I^{[p^{e-e_0}]}.$$

Since this holds for all $e \geq e_0$, we see that c is indeed a finitistic test element.

We leave the non-finitistic case to the reader. It is essentially the same argument but instead one considers the map $E \otimes_R R^{1/p^e} \to E \otimes_R R = E$ which defined by $z \otimes d^{1/p^e} \mapsto z \otimes \phi(d^{1/p^e}) = \phi(d^{1/p^e})z$ where $\phi : R^{1/p^e} \to R$ is the map given in the hypothesis. $\square$

Exercise* 5.23 ([68, 70]). Show that $\tau_{\mathrm{fg}}(R)$ is generated by the set of finitistic test elements. Even more,

$$\tau_{\mathrm{fg}}(R) = \{ \text{ the set of all of the finitistic test elements of } R\} \cup \{0\}.$$

Furthermore, show that $\tau(R)$ is likewise generated by the big test elements of R.
Hint. Suppose that $z \in I^*$, show that for every $e > 0$, $z^{p^e} \in (I^{[p^e]})^*$.

Remark 5.24. Test ideals are made up of test elements, or those elements which can be used to *test* tight closure containments. This is the etymology of the name "test ideals".

Exercise 5.25. Suppose that $(R, \mathfrak{m})$ is a local domain and E is the injective hull of the residue field $R/\mathfrak{m}$. Show that 0_E^* is the Matlis dual of $R/\tau(R)$.
Hint. Choose an element $0 \neq c \in R$ satisfying the conclusion of Lemma 3.6. Show that

$$0_E^* = \bigcap_{e \geq 0} \ker(E \to E \otimes R^{1/p^e})$$

where the maps in the intersection send $z \mapsto z \otimes c^{1/p^e}$. Show that this intersection is the Matlis dual of the construction of the test ideal found in Theorem 3.14. See Appendix A for Matlis Duality.

6 Test Ideals for Pairs (R, α^t) and Applications

As mentioned before, many of the most important applications of multiplier ideals in characteristic zero were for multiplier ideals of pairs. Another variant of pairs not discussed thus-far in this survey is the pair (R_0, α_0^t) where R_0 is a normal $\mathbb{Q}$-Gorenstein domain of finite type over $\mathbb{C}$, α_0 is a non-zero ideal and $t \geq 0$ is a real number. The associated multiplier ideals $\mathcal{J}(\operatorname{Spec} R_0, \alpha_0^t)$ are important in many applications and have themselves become objects of independent interest, see for example [100] and [101]. Inspired by this relation, N. Hara and K.-i. Yoshida defined test ideals for such pairs. They also proved the analog of Theorem 4.17 showing that the multiplier ideal coincides with the test ideal after reduction to characteristic $p \gg 0$.

Setting. In this section, unless otherwise specified, all rings are assumed to be integral domains essentially of finite type over a perfect field of characteristic $p > 0$.

6.1 Initial Definitions of α^t-test Ideals

We now show how to incorporate an ideal α and coefficient $t \in \mathbb{Q}_{\geq 0}$ into the test ideal. An important motivating case is when R is in fact regular; in this situation, one should think of this addition as roughly measuring the singularities of (a multiple of) the closed subscheme of $\operatorname{Spec}(R)$ defined by α.

Definition 6.1 ([58, 123]). Suppose that R is a ring, let $\alpha \subseteq R$ be a non-zero ideal, and $t \in \mathbb{Q}_{\geq 0}$. The *test ideal* $\tau(R, \alpha^t)$ (or simply $\tau(\alpha^t)$ when confusion is unlikely to arise) is defined to be the unique smallest non-zero ideal $J \subseteq R$ such that we have $\phi((\alpha^{\lceil t(p^e-1)\rceil} J)^{1/p^e}) \subseteq J$ for all $e > 0$ and all $\phi \in \operatorname{Hom}_R(R^{1/p^e}, R)$.

Remark 6.2. In other words, $\tau(R, \alpha^t)$ is in fact the unique smallest non-zero ideal which is ϕ-compatible for all $\phi \in (\alpha^{\lceil t(p^e-1)\rceil})^{1/p^e} \cdot \operatorname{Hom}_R(R^{1/p^e}, R)$ and all $e \geq 0$. Again, it is unclear that a smallest such non-zero ideal exists.

Remark 6.3. As in previous sections, N. Hara and K.-i. Yoshida's original definition was the *finitistic test ideal* of a pair. In particular, they defined $\tau_{\mathrm{fg}}(R, \alpha^t)$ to be $\bigcap_{I \subseteq R}(I : I^{*\alpha^t})$ where $I^{*\alpha^t}$ is the α^t-tight closure of I, see Definition 6.13 below. These two ideals are known to coincide in many cases including the case that R is $\mathbb{Q}$-Gorenstein.

Theorem 6.4 ([56]). *Suppose that R is a ring, $\alpha \subseteq R$ is a non-zero ideal, and $t \in \mathbb{Q}_{\geq 0}$. Then, for any non-zero $c \in \tau(R, \alpha^t)$, we have*

$$\tau(R, \alpha^t) = \sum_{e \geq 0} \sum_{\phi} \phi((c\alpha^{\lceil t(p^e-1)\rceil})^{1/p^e})$$

where the inner sum runs over $\phi \in \operatorname{Hom}_R(R^{1/p^e}, R)$. More generally, the above equality remains true if c is replaced by any non-zero element of $\tau(R, \alpha^t)$.

Proof. This is left as an exercise to the reader. For a hint, reduce to the case of Lemma 3.6. □

Exercise 6.5 ([58, Remark 6.6]). Suppose that R is a ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_k \subseteq R$ are non-zero ideals, and $t_1, \ldots, t_k \in \mathbb{Q}_{\geq 0}$. Imitating the above result and its proof, show that one can define a test ideal $\tau(\mathfrak{a}_1^{t_1} \mathfrak{a}_2^{t_2} \cdots \mathfrak{a}_k^{t_k})$ as the unique smallest non-zero ideal $J \subseteq R$ such that

$$\phi\left(\left(J \cdot b \prod_{i=1}^{k} \mathfrak{a}_i^{\lceil t_i(p^e-1)) \rceil}\right)^{1/p^e}\right) \subseteq J$$

for all $e > 0$ and all $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$.

The following property of test ideals was inspired by analogous statement for multiplier ideals.

Theorem 6.6 ([16, Corollary 2.16; 18, Lemma 3.23; 117, Remark 2.12]). *Suppose that R is a ring, $\mathfrak{a} \subseteq R$ is a non-zero ideal, and $s, t \in \mathbb{Q}_{\geq 0}$. If $s \geq t$, then $\tau(\mathfrak{a}^s) \subseteq \tau(\mathfrak{a}^t)$. Furthermore, there exists $\epsilon > 0$ such that $\tau(\mathfrak{a}^s) = \tau(\mathfrak{a}^t)$ for all $s \in [t, t + \epsilon]$.*

Proof. If $s \geq t$, then $(\mathfrak{a}^{\lceil s(p^e-1)\rceil})^{1/p^e} \subseteq (\mathfrak{a}^{\lceil t(p^e-1)\rceil})^{1/p^e}$ and the first statement is left as an exercise to for the reader. For the second statement, choose non-zero elements $c \in \tau(R, \mathfrak{a}^{t+1})$ and $x \in \mathfrak{a}$. Using the Noetherian property of R with Theorem 6.4 above, there exists an $N \geq 0$ such that

$$\tau(R, \mathfrak{a}^t) = \sum_{e=0}^{N} \sum_{\phi} \phi((cx\mathfrak{a}^{\lceil t(p^e-1)\rceil})^{1/p^e})$$

where the inner sum runs over all $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$. Let $\epsilon = \frac{1}{p^N-1}$, so that $x\mathfrak{a}^{\lceil t(p^e-1)\rceil} \subseteq \mathfrak{a}^{\lceil(t+\epsilon)(p^e-1)\rceil}$ for all $0 \leq e \leq N$. Thus, we have

$$\tau(R, \mathfrak{a}^t) \subseteq \sum_{e \geq 0} \sum_{\phi} \phi((c\mathfrak{a}^{\lceil(t+\epsilon)(p^e-1)\rceil})^{1/p^e}) = \tau(R, \mathfrak{a}^{t+\epsilon})$$

as desired. □

Definition 6.7 ([16, 117, 156]). A positive real number ξ is called an *F-jumping number* of the ideal $\mathfrak{a}$ if $\tau(\mathfrak{a}^\xi) \neq \tau(\mathfrak{a}^{\xi-\epsilon})$ for all $\epsilon > 0$. If R is strongly F-regular, then the smallest F-jumping number of $\mathfrak{a}$ is called the *F-pure threshold* of $\mathfrak{a}$.

Remark 6.8. The F-jumping numbers were introduced as characteristic $p > 0$ analogs of jumping numbers of multiplier ideals in characteristic zero, [35]. We point out that a great interest in F-jumping numbers has revolved around proving that the set of F-jumping numbers form a discrete set of rational numbers. See [16, 17, 18, 54, 84, 128, 131, 155].

Theorem 6.9 ([58]). *Suppose that R is a ring, $\mathfrak{a}, \mathfrak{b} \subseteq R$ are non-zero ideals, and $s, t \in \mathbb{Q}_{\geq 0}$.*

(i) *If $\mathfrak{a} \subseteq b$, then $\tau(\mathfrak{a}^t) \subseteq \tau(\mathfrak{b}^t)$. Furthermore, if $\mathfrak{a}$ is a reduction of $\mathfrak{b}$ (i.e. $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$), then $\tau(\mathfrak{a}^t) = \tau(\mathfrak{b}^t)$.*

(ii) *We have $\mathfrak{a}\, \tau(\mathfrak{b}^s) \subseteq \tau(\mathfrak{a}\mathfrak{b}^s)$ with equality if $\mathfrak{a}$ is principal. In particular, if R is strongly F-regular, then $\mathfrak{a} \subseteq \tau(\mathfrak{a})$.*

(iii) *(Skoda) If $\mathfrak{a}$ is generated by r elements, then $\tau(\mathfrak{a}^r \mathfrak{b}^s) = \mathfrak{a}\, \tau(\mathfrak{a}^{r-1} \mathfrak{b}^s)$.*

Proof. The proof is left as an exercise to the reader. As a hint for (iii), using Exercise 5.18, we have

$$c\mathfrak{a}^r \mathfrak{a}^{r(p^e-1)} = c\mathfrak{a}^{rp^e} = c\mathfrak{a}^{[p^e]}\mathfrak{a}^{(r-1)p^e} = \mathfrak{a}^{[p^e]}c\mathfrak{a}^{r-1}\mathfrak{a}^{(r-1)(p^e-1)}.$$

Then manipulate

$$\tau(\mathfrak{a}^r \mathfrak{b}^s) = \sum_{e \geq 0} \sum_{\phi} \phi((c\mathfrak{a}^r \mathfrak{a}^{r(p^e-1)} \mathfrak{b}^{\lceil t(p^e-1)\rceil})^{1/p^e}). \qquad \square$$

Exercise* 6.10 ([56, Theorem 4.1; 58, Theorem 2.1]). If $\mathfrak{a}$ has a reduction generated by at most r elements, show that $\tau(\mathfrak{a}^t) = \mathfrak{a}\, \tau(\mathfrak{a}^{t-1})$ for any $t \geq r$. In particular, $\tau(\mathfrak{a}^h) = \mathfrak{a}^{h-r+1}\, \tau(\mathfrak{a}^{r-1}) \subseteq \mathfrak{a}^{h-r+1} \subseteq \mathfrak{a}$ for any integer $h \geq r$.

Exercise 6.11 ([56, Proposition 3.1], cf. [126]). For any multiplicative system W, prove that $W^{-1}\tau(R, \mathfrak{a}^t) = \tau(W^{-1}R, (W^{-1}\mathfrak{a})^t)$.

Remark 6.12. While the above exercise was first stated as Proposition 3.1 in [56], the proof provided therein is not sufficient. In particular, one needs the existence of a "test element" that remains a test element after localization. See Remark 3.7. However, once one uses Lemma 3.6 to construct such a test element, the proof in [56] goes through without substantial change.

6.2 $\mathfrak{a}^t$-tight Closure

Definition 6.13. Suppose that R is a ring $\mathfrak{a} \subseteq R$ is an ideal and $t \in \mathbb{Q}_{\geq 0}$. For any ideal I of R, the $\mathfrak{a}^t$-*tight closure of I* (denoted $I^{*\mathfrak{a}^t}$) is defined to be the set

$$\{z \in R \mid \exists\, 0 \neq c \in R \text{ such that } c\mathfrak{a}^{\lceil t(p^e-1)\rceil}z^{p^e} \in I^{[p^e]} \text{ for all } e \geq 0\}.$$

See Definition 2.11 for the definition of $I^{[p^e]}$.

Exercise 6.14 ([58]). Show that $I^{*\mathfrak{a}^t}$ is an ideal containing I, and that $\tau(R, \mathfrak{a}^t)\, I^{*\mathfrak{a}^t} \subseteq I$ for all I.

Exercise 6.15 ([58, Proposition 1.3(4)]). If $\mathfrak{a}$ is a reduction[6] of $\mathfrak{b}$, prove $I^{*\mathfrak{a}^t} = I^{*\mathfrak{b}^t}$ for all $t \in \mathbb{Q}_{\geq 0}$.

Exercise 6.16. In the definition of $I^{*\mathfrak{a}^t}$-tight closure, demonstrate that the containment $c\mathfrak{a}^{\lceil t(p^e-1)\rceil}z^{p^e} \in I^{[p^e]}$ may be replaced by the containment $c\mathfrak{a}^{\lceil tp^e\rceil}z^{p^e} \in I^{[p^e]}$ or the containment $c\mathfrak{a}^{\lfloor t(p^e-1)\rfloor}z^{p^e} \in I^{[p^e]}$ without change to $I^{*\mathfrak{a}^t}$. In fact, the original definition of $I^{*\mathfrak{a}^t}$ was the former of these, see [58].

Exercise 6.17 ([123]). Show that $\tau_{\mathrm{fg}}(\mathfrak{a}^t) := \bigcap_{I \subseteq R}(I^{*\mathfrak{a}^t} : I)$ coincides with the set of $c \in R$ satisfying the following condition: whenever $z \in I^{*\mathfrak{a}^t}$, then $c\mathfrak{a}^{\lceil t(p^e-1)\rceil}z^{p^e} \subseteq I^{[p^e]}$ for all $e \geq 0$.
Hint. Show that if $z \in I^{*\mathfrak{a}^t}$, then for every $e \geq 0$, $\mathfrak{a}^{\lceil t(p^e-1)\rceil}z^{p^e} \subseteq (I^{[p^e]})^{*\mathfrak{a}^t}$.

Remark 6.18. Note when $\mathfrak{a} = R$, we recover the original definition of tight closure. In general, while there are many similarities between tight closure and $\mathfrak{a}^t$-tight closure, there are some very important differences as well. In fact, $\mathfrak{a}^t$-tight closure fails to be a closure operation at all: in many cases $(I^{*\mathfrak{a}^t})^{*\mathfrak{a}^t}$ is strictly larger than $I^{*\mathfrak{a}^t}$ (in other words, the operation is not idempotent). However, if $\mathfrak{a}$ is primary to a maximal ideal, A. Vraciu has developed an alternate version of $\mathfrak{a}^t$-tight closure which shares many aspects of the same theory but which is idempotent, see [162].

Exercise 6.19. If R is strongly F-regular and $\mathfrak{a}$ is a non-zero principal ideal, show that $I^{*\mathfrak{a}} = I : \mathfrak{a}$ for all ideals I. Use this to produce an example where $(I^{*\mathfrak{a}^t})^{*\mathfrak{a}^t}$ is strictly larger than $I^{*\mathfrak{a}^t}$.

6.3 Applications

The test ideal $\tau(\mathfrak{a}^t)$ of a pair was introduced because of the connection between $\tau(R)$ and $\mathcal{J}(X_0 = \mathrm{Spec}\, R_0)$ discussed in Section 4. In particular, working in characteristic zero, many of the primary applications of multiplier ideals involved pairs of the form $(X_0, \mathfrak{a}_0^t)$, or more generally $(X_0, \mathfrak{a}_0^t \mathfrak{b}_0^s)$. One such formula is the subadditivity formula, see [32, 114]. In [152], S. Takagi proved analogous results for the test ideal. In fact, Takagi was able to prove a subadditivity formula on singular varieties (for simplicity, we only handle the smooth case below). Using reduction to characteristic $p > 0$, one can then obtain the same formula for multiplier ideals, thus obtaining a new result in characteristic-zero algebraic geometry. Recently, E. Eisenstein has obtained a geometric proof in characteristic-zero of the results for singular varieties [37].

Exercise* 6.20 ([152, Proposition 2.1]). Given ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$ and numbers $s, t \in \mathbb{R}_{\geq 0}$, prove that $I^{*\mathfrak{a}^t}\tau(\mathfrak{a}^t\mathfrak{b}^s) \subseteq I\,\tau(\mathfrak{b}^s)$ for any ideal $I \subseteq R$.

---

[6] Again, an ideal $\mathfrak{a} \subseteq \mathfrak{b}$ such that $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

Theorem 6.21 (Subadditivity, [152, Theorem 2.7]). *Suppose R is a regular local ring, and $\mathfrak{a}, \mathfrak{b}$ are ideals in R. For any $s, t \in \mathbb{Q}_{\geq 0}$, we have*

$$\tau(\mathfrak{a}^t \mathfrak{b}^s) \subseteq \tau(\mathfrak{a}^t)\tau(\mathfrak{b}^s).$$

If instead R is of finite type over a perfect field k but is not assumed to be regular, then still:

$$\mathfrak{J}(R/k)\tau(\mathfrak{a}^t \mathfrak{b}^s) \subseteq \tau(\mathfrak{a}^t)\tau(\mathfrak{b}^s),$$

where $\mathfrak{J}(R/k)$ is the Jacobian ideal of R over k, see [36, Section 16.6].

Proof. We only prove the first statement. Fix $0 \neq c \in \tau(\mathfrak{a}^t \mathfrak{b}^s) \subseteq \tau(\mathfrak{a}^t) \cap \tau(\mathfrak{b}^s)$. From Exercise 6.20, we have $\tau(\mathfrak{a}^t)^{*\mathfrak{a}^t}\tau(\mathfrak{a}^t \mathfrak{b}^s) \subseteq \tau(\mathfrak{a}^t)\tau(\mathfrak{b}^s)$. To finish the proof, it suffices to show that $\tau(\mathfrak{a}^t)^{*\mathfrak{a}^t} = R$. For all $\psi \in \operatorname{Hom}_R(R^{1/p^e}, R)$, we know $\psi((c\mathfrak{a}^{\lceil t(p^e-1)\rceil})^{1/p^e}) \subseteq \tau(\mathfrak{a}^t)$. Thus, using Exercise 2.13, we see $c\mathfrak{a}^{\lceil t(p^e-1)\rceil} \subseteq \tau(\mathfrak{a}^t)^{[p^e]}$ for all $e \geq 0$. In particular, this shows $1 \in \tau(\mathfrak{a}^t)^{*\mathfrak{a}^t}$ as desired. $\square$

Corollary 6.22 ([152, Theorem 0.1]). *Let $X_0 = \operatorname{Spec} R_0$ be a normal $\mathbb{Q}$-Gorenstein variety over $\mathbb{C}$ and let $\mathfrak{J}(R_0/\mathbb{C})$ be the Jacobian ideal sheaf of X over $\mathbb{C}$. Let $\mathfrak{a}_0, \mathfrak{b}_0 \in \mathcal{O}_{X_0}$ be two non-zero ideal sheaves and fix real numbers $s, t \geq 0$. Then*

$$\mathfrak{J}(R_0/\mathbb{C})\mathcal{J}(X_0, \mathfrak{a}_0^t \mathfrak{b}_0^s) \subseteq \mathcal{J}(X_0, \mathfrak{a}_0^t)\mathcal{J}(X_0, \mathfrak{b}_0^s).$$

Proof. This follows via reduction to characteristic $p > 0$, see Subsection 4.2. Apply Theorem 6.21 and an analog of Theorem 4.17 which can be found in [58, Theorem 6.8]. $\square$

We now discuss another application of the subadditivity formula for test ideals: the growth of symbolic and ordinary powers of an ideal. Recall that the n-th symbolic power of an ideal $\mathfrak{a} \subseteq R$ is given by $\mathfrak{a}^{(n)} = (\mathfrak{a}^n W^{-1} R) \cap R$, where $W \subseteq R$ is the compliment of the union of the associated primes of $\mathfrak{a}$. In the case that $\mathfrak{a}$ is a prime ideal, $\mathfrak{a}^{(n)}$ coincides with the $\mathfrak{a}$-primary component of $\mathfrak{a}^n$.

Theorem 6.23 ([72], cf. [34, 74, 157]). *Let $(R, \mathfrak{m})$ be a regular local ring with infinite residue field $R/\mathfrak{m}$. Let $\mathfrak{a}$ be any non-zero ideal of R and let h be the maximal height of any associated prime ideal of $\mathfrak{a}$. Then $\mathfrak{a}^{(hn)} \subseteq \mathfrak{a}^n$ for all integers $n \geq 1$.*

Proof. Since R is regular (and hence also strongly F-regular), using subadditivity (and Theorem 6.9 (iii)) we have

$$\mathfrak{a}^{(hn)} \subseteq \tau(\mathfrak{a}^{(hn)}) \subseteq (\tau((\mathfrak{a}^{(hn)})^{1/n}))^n$$

for all integers $n \geq 0$. Thus, it suffices to check that $\tau((\mathfrak{a}^{(hn)})^{1/n}) \subseteq \mathfrak{a}^{(1)} = \mathfrak{a}$, which may be done after localizing at each associated prime $\mathfrak{p}$ of $\mathfrak{a}$. Since $R_\mathfrak{p}$ has dimension

at most h and infinite residue field, every non-zero ideal of $R_{\mathfrak{p}}$ has a reduction generated by no more than h elements, [79, Proposition 8.3.7, Corollary 8.3.9]. Thus, since $\mathfrak{a}^{(hn)} R_{\mathfrak{p}} = \mathfrak{a}^{hn} R_{\mathfrak{p}}$, we have (using Exercises 6.10 and 6.11)

$$\tau(R, (\mathfrak{a}^{(hn)})^{1/n}) R_{\mathfrak{p}} = \tau(R_{\mathfrak{p}}, (\mathfrak{a}^{hn} R_{\mathfrak{p}})^{1/n}) = \tau(R_{\mathfrak{p}}, \mathfrak{a}^h R_{\mathfrak{p}}) \subseteq \mathfrak{a} R_{\mathfrak{p}}$$

and we conclude that $\mathfrak{a}^{(hn)} \subseteq \mathfrak{a}^n$ for all $n \geq 0$. $\qquad\square$

Exercise* 6.24. Modify the proof of Theorem 6.23 to show the stronger statement $\mathfrak{a}^{(kn)} \subseteq (\mathfrak{a}^{(k-h+1)})^n$ for all $k \geq n$.

7 Generalizations of Pairs: Algebras of Maps

In this short section we discuss a common generalization of the pairs (R, ϕ) and $(R, \mathfrak{a}^t)$ previously introduced. In fact this generalization encompasses all studied types of pairs, triples, etc. This idea has also been generalized to modules in [12], although we will not work in that generality.

Setting. In this section, unless otherwise specified, all rings are assumed to be integral domains essentially of finite type over a perfect field of characteristic $p > 0$.

Fix a ring[7] R and set $\mathscr{C}_e = \operatorname{Hom}_R(R^{1/p^e}, R)$. The test ideals and related notions such as F-purity and F-regularity are detected by looking for Frobenius splittings and similar special elements of $\mathscr{C}_e$ for various $e \geq 0$. Fundamentally, all pairs we have previously considered restrict the potential elements of $\mathscr{C}_e$ (e.g. only multiples of a fixed homomorphism $\phi: R^{1/p^e} \to R$). We abstract the idea of restricting potential elements of $\mathscr{C}_e$ as follows.

Consider now the Abelian group

$$\mathscr{C} = \bigoplus_{e \geq 0} \mathscr{C}_e = \bigoplus_{e \geq 0} \operatorname{Hom}_R(R^{1/p^e}, R).$$

We can turn this into a non-commutative $\mathbb{N}$-graded ring by the following multiplication rule. For $\alpha \in \mathscr{C}_e$ and $\beta \in \mathscr{C}_d$ we define

$$\alpha \cdot \beta := (\alpha \circ \beta^{1/p^e} : R^{1/p^{d+e}} \to R) \in \mathscr{C}_{d+e}.$$

Explicitly, β^{1/p^e} is the R^{1/p^e}-linear map $R^{1/p^{d+e}} \to R^{1/p^e}$ defined by the rule

$$\beta^{1/p^e}(x^{1/p^{d+e}}) = (\beta(x^{1/p^d}))^{1/p^e}.$$

We then compose with a map $\alpha : R^{1/p^e} \to R$ to obtain $\alpha \cdot \beta$.

---

[7] In fact, M. Blickle has shown that the theory below can be extended F-finite rings which are not necessarily reduced [12].

We call $\mathscr{C}$ the *complete algebra of maps on R*. Notice that $\mathscr{C}$ is not commutative (and $\mathscr{C}_0 = R$ is not even central). Even more, this ring is not generally finitely generated over $\mathscr{C}_0 = R$ [83].

Remark 7.1. Suppose for simplicity that $(R, \mathfrak{m})$ is local. The algebra $\mathscr{C}$ is, up to some choices of isomorphism, Matlis dual to $\mathscr{F}(E)$, the algebra of (iterated-)Frobenius actions on E, the injective hull of the residue field $R/\mathfrak{m}$. See [107].

Definition 7.2 ([129, Section 3]). An (algebra-)pair $(R, \mathscr{D})$ is the combined information of R and a graded-subring $\mathscr{D} \subseteq \mathscr{C}$ such that $\mathscr{D}_0 = \mathscr{C}_0 = \mathrm{Hom}_R(R, R) \cong R$ and $\mathscr{D}_e \neq 0$ for some $e > 0$.

Example 7.3. Suppose R is a ring and $\mathfrak{a} \subseteq R$ is an ideal. Then for any real number $t \geq 0$, we can construct the submodule

$$\mathscr{D}_e := (\mathfrak{a}^{\lceil t(p^e-1)\rceil})^{1/p^e} \cdot \mathscr{C}_e = \bigoplus_{e \geq 0}((\mathfrak{a}^{\lceil t(p^e-1)\rceil})^{1/p^e} \cdot \mathrm{Hom}_R(R^{1/p^e}, R)).$$

One can verify that $\bigoplus_{e \geq 0} \mathscr{D}_e$ forms a graded subalgebra which we denote by $\mathscr{C}^{\mathfrak{a}^t}$.

Exercise 7.4 (Different roundings and algebras). Prove that $\mathscr{C}^{\mathfrak{a}^t}$ is indeed a graded subalgebra of $\mathscr{C}$. Give an example to show that $\bigoplus_{e \geq 0}(\mathfrak{a}^{\lfloor t(p^e-1)\rfloor})^{1/p^e} \cdot \mathscr{C}_e$ is not a graded subalgebra but $\bigoplus_{e \geq 0}(\mathfrak{a}^{\lceil tp^e\rceil})^{1/p^e} \cdot \mathscr{C}_e$ is (although its first graded piece is not necessarily isomorphic to R).

Example 7.5. If one fixes a homogeneous element $\phi \in \mathscr{C}_e$ for $e > 0$, then one can form the algebra $\langle \phi \rangle = \bigoplus_{n \geq 0} \phi^n R^{1/p^{ne}} \subseteq \mathscr{C}$ which is just the subalgebra generated by $\mathscr{C}_0$ and ϕ.

Definition 7.6. Given a pair $(R, \mathscr{D})$, an ideal $I \subseteq R$ is called $\mathscr{D}$-compatible if $\phi(I^{1/p^e}) \subseteq I$ for all $\phi \in \mathscr{D}_e$ and all $e \geq 0$.

Definition 7.7 ([129, Definition 3.16]). The big test ideal $\tau(R, \mathscr{D})$ of a pair $(R, \mathscr{D})$, if it exists, is the unique smallest ideal J that satisfies two conditions:

(i) J is $\mathscr{D}$-compatible, and

(ii) $J \neq \{0\}$.

Exercise 7.8 ([129]). Suppose that $\mathscr{D}$ has a non-zero homogeneous element $\phi \in \mathscr{D}_e$, $e > 0$. Prove that $\tau(R, \mathscr{D})$ exists by using Lemma 3.6.

Exercise 7.9 ([129]). Suppose that $(R, \mathfrak{a}^t)$ is a pair as in Section 6. Prove that $\tau(R, \mathscr{C}^{\mathfrak{a}^t}) = \tau(R, \mathfrak{a}^t)$. Further show that if $\phi \in \mathscr{C}_e$ is non-zero, then $\tau(R, \langle \phi \rangle) = \tau(R, \phi)$.

Algebras of maps appear very naturally. For example, suppose that R is a ring and $\mathscr{C}_R$ is the complete algebra of maps on R. Suppose that $I \subseteq R$ is a $\mathscr{C}_R$-compatible ideal (such as the test ideal $\tau(R)$ or the splitting prime[8] $\mathscr{P}$ of [2].). One can then restrict each element of $\mathscr{C}_R$ to R/I. This yields an algebra of maps $\mathscr{D}_{R/I} = \mathscr{C}_R|_{R/I}$ which may or may not be equal to $\mathscr{C}_{R/I}$.

Exercise 7.10 ([124]). With the notation above, suppose that R is Gorenstein and local. Prove that the algebra $\mathscr{D}_{R/I}$ is equal to $\langle \phi \rangle$ for some $\phi \in \mathscr{C}_{R/I}$.

One can define F-purity for algebras as well.

Definition 7.11. Suppose that $(R, \mathscr{D})$ is a pair. Then the pair is called *sharply F-pure* (or sometimes just *F-pure*) if there exists a homogenous element $\phi \in \mathscr{D}_e$, $e > 0$ such that $\phi(R^{1/p^e}) = R$, i.e. ϕ is surjective.

Exercise 7.12 ([129], cf. [12, 13]). Prove that for a sharply F-pure pair $(R, \mathscr{D})$, $\tau(R, \mathscr{D})$ defines an F-pure subscheme and so in particular is a radical ideal.

The following theorem is an application of this approach of algebras of pairs.

Theorem 7.13 ([129], cf. [31, 130]). *Suppose that $(R, \mathscr{D})$ is a pair (i.e. $\mathscr{D} = \mathscr{C}$). Then*

$$\tau(R, \mathscr{D}) = \sum_{e>0} \sum_{\phi \in \mathscr{D}_e} \tau(R, \phi).$$

If R is additionally normal, then this also equals $\sum_{e>0} \sum_{\phi \in \mathscr{D}_e} \tau(R, \Delta_\phi)$.

For non-$\mathbb{Q}$-Gorenstein normal varieties X_0 over $\mathbb{C}$, de Fernex and Hacon have defined a multiplier ideal $\mathcal{J}(X_0)$ [31]. Furthermore,

$$\mathcal{J}(X_0) = \sum_{\substack{K_{X_0} + \Delta_0 \\ \text{is } \mathbb{Q}\text{-Cartier}}} \mathcal{J}(X_0, \Delta_0).$$

It is therefore natural to conjecture following.

Conjecture 7.14. Given a variety $X_0 = \operatorname{Spec} R_0$ in characteristic zero, we have $\tau(R_p) = \mathcal{J}(X_0)_p$ for all $p \gg 0$ (here the subscript p denotes reduction to characteristic $p > 0$ as in Subsection 4.2).

Work of M. Blickle implies that this conjecture holds for toric rings [11].

Remark 7.15. For other applications, it is likely important that one has a good measure of the finiteness properties of the given algebra $\mathscr{D}$. One very useful such property is the *Gauge-Bounded* property introduced in [12] (cf. [9]). This property is quite useful for proving questions related to the discreteness of F-jumping numbers, see Definition 6.7.

---

[8] In an F-pure local ring, the splitting prime is the unique largest $\mathscr{C}_R$-compatible ideal not equal to the whole ring.

8 Other Measures of Singularities in Characteristic p

So far we have talked about test ideals, F-regularity and F-purity. In this section we introduce several other ways to measure singularities in positive characteristic. For a more complete list, please see the appendix.

First we introduce two other classes of singularities. F-rationality and F-injectivity.

8.1 F-rationality

Setting. In this subsection, unless otherwise specified, all rings are assumed to be integral domains essentially of finite type over a perfect field of characteristic $p > 0$.

Definition 8.1. Suppose that R is a normal Cohen–Macaulay ring and that Φ_R: $\omega_{R^{1/p}} = F_*\omega_R \to \omega_R$ is the canonical dual of Frobenius, see Theorem A.8. We say that R has *F-rational singularities* if there are no non-zero proper submodules $M \subseteq \omega_R$ such that $\Phi_R(F_*M) \subseteq M$.

Exercise* 8.2. Prove that the hypothesis that R is normal above is redundant.

Exercise 8.3 ([45]). Prove that a strongly F-regular ring is F-rational and that a Gorenstein F-rational ring is strongly F-regular.
Hint. For the first part, use Theorem 3.19 and apply the functor $\mathrm{Hom}_R(\_, \omega_R)$.

Exercise* 8.4 ([144]). Recall that an integral domain R_0 of finite type over $\mathbb{C}$ is said to have *rational singularities* if for a resolution of singularities $\pi : \widetilde{X}_0 \to X_0 = \mathrm{Spec}\, R_0$, $\pi_*\omega_{\widetilde{X}_0} = \omega_{X_0}$ and X_0 is Cohen–Macaulay[9]. Now suppose we are given an integral domain R_0 of finite type over $\mathbb{C}$. Show that if R_p has F-rational singularities after reduction to characteristic $p \gg 0$ (see Subsection 4.2), then R_0 has rational singularities in characteristic zero.

Remark 8.5. The converse of the above exercise also holds, but the proof is more involved. See [51] and [110].

We briefly mention the original definition of F-rationality.

Theorem 8.6. *A local ring $(R, \mathfrak{m})$ has F-rational singularities if and only if some ideal $I = (x_1, \ldots, x_n)$ generated by a full system of parameters satisfies $I = I^*$ (here I^* denotes the tight closure of I, see Section 5).*

Proof. See [45] or [27, Chapter 10]. □

---

[9] This is not normally the definition of rational singularities, but is instead a criterion often attributed to Kempf, [89, p. 50].

8.2 *F*-injectivity

Setting. In this subsection, unless otherwise specified, all rings are assumed to be reduced and essentially of finite type over a perfect field of characteristic $p > 0$.

Definition 8.7. A local ring $(R, \mathfrak{m})$ is called *F-injective* if for every integer $i > 0$, the natural map $H^i_{\mathfrak{m}}(R) \to H^i_{\mathfrak{m}}(R^{1/p})$ is injective. An arbitrary ring R is called *F*-injective if all of its localizations at prime ideals are *F*-injective.

Exercise 8.8. Suppose that R is Cohen–Macaulay and local. Prove that R is *F*-injective if and only if the canonical dual to Frobenius $F_* \omega_R \to \omega_R$ is surjective.

Exercise 8.9 ([44]). Prove that a Gorenstein ring is *F*-injective if and only if it is *F*-pure and that an *F*-pure ring is always *F*-injective.

Exercise 8.10 ([45]). Suppose that $(R, \mathfrak{m})$ is a Cohen–Macaulay local ring and $f \in R$ is a regular element. Prove that if R/f is *F*-injective, then R is *F*-injective.

Hint. Using the criterion in Exercise 8.8, consider the diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & F_* \omega_R & \xrightarrow{\ \times F_* f^p\ } & F_* \omega_R & \longrightarrow & F_* \omega_{R/f^p} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \ \downarrow{\scriptstyle \beta} & & \\
0 & \longrightarrow & \omega_R & \xrightarrow{\ \times f\ } & \omega_R & \longrightarrow & F_* \omega_{R/f} & \longrightarrow & 0
\end{array}
$$

Show that β surjects, by considering the map $F_* \omega_{R/f} \to F_* \omega_{R/f^p}$. Now take the cokernels of the left and middle vertical maps and use Nakayama's lemma.

Remark 8.11. It is an open question whether Exercise 8.10 holds without the Cohen–Macaulay assumption. It is however known that the analog of Exercise 8.10 does not hold for *F*-pure rings in general, see [44] and also [137]. One can ask the same question for strongly *F*-regular and *F*-rational singularities, and the answers are no and yes respectively; see [45] and [138].

Exercise* 8.12. [94, 95, 126] A normal Cohen–Macaulay ring R_0 of finite type over $\mathbb{C}$ is called Du Bois if for some (equivalently any) log resolution of singularities $\pi : \widetilde{X}_0 \to X_0 = \operatorname{Spec} R_0$ with simple normal crossings exceptional divisor E_0, $\pi_* \omega_{\widetilde{X}_0}(E_0) \cong \omega_{X_0}$. Prove that if X_p has *F*-injective singularities after reduction to characteristic $p \gg 0$, then X_0 has Du Bois singularities in characteristic zero.

Hint. Consider the diagram

$$
\begin{array}{ccc}
(\pi_*\omega_{\widetilde{X_p}}(p^e E_p))^{1/p^e} & \longrightarrow & \pi_*\omega_{\widetilde{X_p}}(E_p) \\
\rho \downarrow & & \downarrow \beta \\
\omega_{X_p}^{1/p^e} & \xrightarrow{\quad\Phi\quad} & \omega_{X_p}
\end{array}
$$

where the horizontal arrows are the dual of the Frobenius map (see Subsection 3.3).

Remark 8.13. The converse implication of the above exercise is false as stated, in fact that singularity $\mathbb{F}_p[x, y, z]/\langle x^3 + y^3 + z^3 \rangle$ is F-injective if and only if $p = 1 \mod 3$. However, it is an important open question whether a Du Bois singularity is F-injective after reduction to characteristic $p > 0$ for infinitely many primes p (technically, a Zariski-dense set of primes), this condition is called *dense F-injective type* whereas the original condition is called *open F-injective type*. Likewise, it is an open question whether a log canonical singularity is F-pure after reduction to characteristic $p > 0$ for infinitely many primes p.

Exercise* 8.14 ([57]). A log $\mathbb{Q}$-Gorenstein pair (X, Δ) of any characteristic is called *log canonical* if for every proper birational map $\pi : \widetilde{X} \to X$ with $\widetilde{X}$ normal, all the coefficients of $K_{\widetilde{X}} - \pi^*(K_X + \Delta)$ are ≥ -1. This can be checked on a single log resolution of (X, Δ), if it exists (it does in characteristic zero). For more about log canonical singularities, see [90] and [92].

Use the method of the above exercise to show the following. If $X = \operatorname{Spec} R$ is a ring of characteristic p and $\phi : R^{1/p^e} \to R$ is a divisor corresponding to Δ as in (4.15.1), then if ϕ is surjective (i.e. if (R, ϕ) is F-pure) show that (X, Δ) is log canonical. Conclude by showing that log $\mathbb{Q}$-Gorenstein pairs (X_0, Δ_0) over $\mathbb{C}$ of dense F-pure type (i.e. such that ϕ_{Δ_p} is surjective for infinitely many $p \gg 0$) are always log canonical.

8.3 *F*-signature and *F*-splitting Ratio

Recall that a ring R was said to be F-pure if the all of Frobenius inclusions $R \to R^{1/p^e}$ split as a maps of R-modules. In this section, we consider local numerical invariants – the F-signature and F-splitting ratio – which characterize the asymptotic growth of the number of splittings of the iterates of Frobenius.

Setting. In this subsection, unless otherwise specified, all rings are assumed to be *local* integral domains essentially of finite type over a perfect field of characteristic $p > 0$.

Definition 8.15. Let $(R, \mathfrak{m}, k)$ be a local ring. For each $e \in \mathbb{N}$, the *e-th Frobenius splitting (F-splitting) number of R* is the maximal rank $a_e = a_e(R)$ of a free R-module appearing in a direct sum decomposition of R^{1/p^e}. In other words, we may write $R^{1/p^e} = R^{\oplus a_e} \oplus M_e$ where M_e has no free direct summands.

Exercise 8.16. Show that R is F-pure if and only if $a_e > 0$ for some $e \in \mathbb{N}$, in which case $a_e > 0$ for all $e \in \mathbb{N}$.

Exercise 8.17 ([5]). For any prime ideal $\mathfrak{p}$ in R, show that $a_e(R_\mathfrak{p}) \geq a_e(R)$.

Using the following proposition, it is easy to see that the F-splitting numbers are independent of the chosen direct sum decomposition of R^{1/p^e}.

Proposition 8.18 ([2]). *Assume that* $k = k^p$ *is perfect. Consider the sets*

$$I_e := \{r \in R \mid \phi(r^{1/p^e}) \in \mathfrak{m} \text{ for all } \phi \in \operatorname{Hom}_R(R^{1/p^e}, R)\}.$$

Then I_e *is an ideal in R with* $\ell_R(R/I_e) = a_e$.

Exercise* 8.19 ([2]). Check that I_e is, in fact, an ideal. Then prove the proposition.

Theorem 8.20 ([158]). *Let* $(R, \mathfrak{m}, k)$ *be a local ring of dimension* d. *Assume* $k = k^p$ *is perfect. Then the limit*

$$s(R) := \lim_{e \to \infty} \frac{a_e}{p^{ed}}$$

exists and is called the F-signature of R.

The F-signature was first explicitly[10] defined by C. Huneke and G. Leuschke [78] and captures delicate information about the singularities of R. For example, the F-signature of the two-dimensional rational double-points[11] $(A_n), (D_n), (E_6), (E_7), (E_8)$ is the reciprocal of the order of the group defining the quotient singularity [78, Example 18]. However, a positive answer to a conjecture of Monsky implies the existence of local rings with irrational F-signature, see [112].

The heart of the proof of Theorem 8.20 lies in the following technical lemma.

Lemma 8.21 ([158]). *Let* $(R, \mathfrak{m}, k)$ *be a local ring of dimension* d. *If* $\{J_e\}_{e \in \mathbb{N}}$ *is any sequence of* $\mathfrak{m}$-*primary ideals such that* $J_e^{[p]} \subseteq J_{e+1}$ *and* $\mathfrak{m}^{[p^e]} \subseteq J_e$ *for all* e, *then* $\lim_{e \to \infty} \frac{1}{p^{ed}} \ell_R(R/J_e)$ *exists.*

Exercise 8.22 ([158]). Show that the ideals I_e from Proposition 8.18 satisfy $I_e^{[p]} \subseteq I_{e+1}$ and $\mathfrak{m}^{[p^e]} \subseteq I_e$, and use the previous lemma to conclude the existence of the F-signature limit.

---

[10] Implicitly, the F-signature first appeared in [148].

[11] Here it is necessary to assume that $p \geq 7$ to avoid pathologies in low characteristic.

It is quite natural to expect the F-signature to measure the singularities of R. Indeed, when R is regular, R^{1/p^e} itself is a free R-module of rank p^{ed}. Thus, for general R, the F-signature asymptotically compares the number of direct summands of R^{1/p^e} isomorphic to R with the number of such summands one would expect from a regular local ring of the same dimension.

Theorem 8.23 ([5, Theorem 0.2]). *Let $(R, \mathfrak{m}, k)$ be a local ring of dimension d. Assume $k = k^p$ is perfect. Then $s(R) > 0$ if and only if R is strongly F-regular.*

Definition 8.24 ([2]). Suppose R is F-pure. If I_e is as in Proposition 8.18, the ideal $P = \cap_{e \in \mathbb{N}} I_e$ is called the *F-splitting prime* of R.

Exercise* 8.25 ([2, 126]). Check that P is a prime ideal, and that $\phi(P^{1/p^e}) \subseteq P$ for all $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$. In particular, conclude that $\tau(R) \subseteq P$. Show that $P = \langle 0 \rangle$ if and only if R is strongly F-regular. More generally, show that R/P is strongly F-regular.

Theorem 8.26 ([19, 158]). *Let $(R, \mathfrak{m}, k)$ be an F-pure local of dimension d. Assume $k = k^p$ is perfect. Let P be the F-splitting prime of R. Then the limit*

$$r_F(R) := \lim_{e \to \infty} \frac{a_e}{p^{e \dim(R/P)}}$$

exists and is called the F-splitting ratio of R. Furthermore, we have $r_F(R) > 0$.

8.4 Hilbert–Kunz(–Monsky) Multiplicity

Our goal in this section is to explore a variant, introduced by E. Kunz and P. Monsky, of the Hilbert–Samuel multiplicity of a ring. Recall that the Hilbert–Samuel multiplicity of a local ring $(R, \mathfrak{m}, k)$ along an $\mathfrak{m}$-primary ideal I is simply

$$e(I) := \lim_{n \to \infty} \frac{d!}{n^d} \ell_R(R/I^n) \ .$$

The existence of the above limit follows easily from the fact that, for sufficiently large n, $\ell_R(R/I^n)$ agrees with a polynomial in n of degree d. Since this polynomial maps $\mathbb{Z} \to \mathbb{Z}$, it is easy to see that $e(I) \in \mathbb{Z}$. When $I = \mathfrak{m}$, $e(R) := e(\mathfrak{m})$ is called the Hilbert–Samuel multiplicity of R.

Roughly speaking, the idea behind Hilbert–Kunz multiplicity is to use the Frobenius powers $I^{[p^e]}$ of an ideal I, see Definition 2.11, in place of the ordinary powers I^n in the definition of multiplicity. For a somewhat different introduction to the Hilbert–Kunz multiplicity, see [76, Chapter 6].

Setting. In this subsection, unless otherwise specified, all rings are assumed to be *local integral domains essentially of finite type over a perfect field of characteristic $p > 0$.*

Theorem 8.27 ([98, 111]). *Suppose $(R, \mathfrak{m}, k)$ is a local ring of dimension d and characteristic $p > 0$. If I is any $\mathfrak{m}$-primary ideal, then the limit*

$$e_{\mathrm{HK}}(I) := \lim_{e \to \infty} \frac{1}{p^{ed}} \, \ell_R(R/I^{[p^e]})$$

exists and is called the Hilbert–Kunz multiplicity *of R along I. When $I = \mathfrak{m}$, we write $e_{\mathrm{HK}}(R) := e_{\mathrm{HK}}(\mathfrak{m})$ and we refer to this number as the* Hilbert–Kunz multiplicity *of R.*

Many basic properties of Hilbert–Kunz multiplicity (see [111] or [76]) mirror those for Hilbert–Samuel multiplicity, such as the following:

- If $I \subseteq J$ are $\mathfrak{m}$-primary ideals, then $e_{\mathrm{HK}}(I) \geq e_{\mathrm{HK}}(J)$.
- We always have $e_{\mathrm{HK}}(R) \geq 1$ with equality when R is regular.
- $e_{\mathrm{HK}}(R) = \sum_{\mathfrak{p} \in \mathrm{Assh}(R)} e_{\mathrm{HK}}(R/\mathfrak{p})$ where $\mathrm{Assh}(R)$ denotes the set of prime ideals $\mathfrak{p}$ of R with $\dim(R/\mathfrak{p}) = \dim(R)$.
- [80, 163] If R is equidimensional, then $e_{\mathrm{HK}}(R) = 1$ if and only if R is regular.
- If I is generated by a regular sequence, then $e_{\mathrm{HK}}(I) = \ell_R(R/I)$.

Exercise 8.28. If R is regular, show that $e_{\mathrm{HK}}(I) = \ell_R(R/I)$ for every $\mathfrak{m}$-primary ideal I.

Exercise 8.29 ([76, Lemma 6.1]). Show that $e_{\mathrm{HK}}(I) \geq \frac{1}{d!} e(I)$. Note that this inequality is known to be sharp if $d \geq 2$ by [50].

Monsky's proof of the existence of Hilbert–Kunz multiplicity, however, bears little resemblance to the proof of the existence of Hilbert–Samuel multiplicity. Indeed, the function $e \to \ell_R(R/I^{[p^e]})$ frequently exhibits non-polynomial behavior, and $e_{\mathrm{HK}}(R)$ need not be an integer.

Example 8.30. Consider the characteristic 5 local ring

$$R = (\mathbb{F}_5[w, x, y, z]/\langle w^4 + x^4 + y^4 + z^4 \rangle)_{\langle w, x, y, z \rangle}.$$

C. Han and P. Monsky in have computed in [49] that

$$\ell_R(R/\mathfrak{m}^{[p^e]}) = \frac{168}{61}(5^e)^3 - \frac{107}{61} 3^e$$

and, in particular, we have $e_{\mathrm{HK}}(R) = \frac{168}{61}$.

In a sense, the proof of Theorem 8.27 is not constructive: Monsky proceeds to show that $\{\frac{1}{p^{ed}} \, \ell_R(R/I^{[p^e]})\}_{e \in \mathbb{N}}$ is a Cauchy sequence. As such, the limit is only known to be a real number (and, in particular, not necessarily even rational). The computation of Hilbert–Kunz multiplicity is widely considered to be a difficult problem.

Exercise 8.31. Use Lemma 8.21 to show that $e_{HK}(I)$ exists when R is a domain.

Conjecture 8.32 ([113], cf. [22]). The Hilbert–Kunz multiplicity of the local ring

$$(\mathbb{F}_2[x, y, z, u, v]/\langle uv + x^3 + y^3 + xyz\rangle)_{\langle x,y,z,u,v\rangle}$$

is $\frac{4}{3} - \frac{5}{14\sqrt{7}}$, and in particular not rational.

Example 8.33. Let $p > 2$ be a prime and consider the local rings

$$R_{p,d} = \left(\overline{\mathbb{F}_p}[x_0, \ldots, x_d] \,/ \left\langle \sum_{i=0}^d x_i^2 \right\rangle\right)_{\langle x_0,\ldots,x_s\rangle}.$$

The numbers $e_{HK}(R_{p,d})$ have been explicitly computed [49] and – even for a fixed d – can depend on p in a complicated way. For example, when $d = 4$ we have

$$\frac{29p^2 + 15}{24p^2 + 12}.$$

However, I. Gessel and P. Monsky have shown that the $e_{HK}(R_{p,d})$ have a well-defined limit as $p \to \infty$ equal to 1 plus the coefficient of z^s in the power series expansion of $\sec z + \tan z$.

Perhaps one of the most interesting open problems aims to identify the non-regular rings $R_{p,d}$ having the smallest Hilbert–Kunz multiplicity possible.

Conjecture 8.34. [165] Let $d \geq 1$ and $p > 2$ a prime number. Let R be d-dimensional characteristic p unmixed local ring with residue field $\overline{\mathbb{F}_p}$. If R is not regular, then $e_{HK}(R) \geq e_{HK}(R_{p,d})$ with equality if and only if it is formally isomorphic to $R_{p,d}$, i.e. their respective completions $\widehat{R} \simeq \widehat{R_{p,d}}$ are isomorphic.

This conjecture is known to be true when R has dimension at most six, see [3], and also when R is a complete intersection in arbitrary dimension in [42]. Finally also see [139].

Many topics from previous sections share a close relationship with so-called relative Hilbert–Kunz multiplicities, i.e. the differences $e_{HK}(I) - e_{HK}(J)$ for pairs of $\mathfrak{m}$-primary ideals $I \subseteq J$. For example, as seen below, these differences may be used to test for tight closure and are closely related to the F-signature.

Theorem 8.35 ([70, Theorem 8.17]). *Assume R is a complete local domain. If $I \subseteq J$ are two $\mathfrak{m}$-primary ideals, then $e_{HK}(I) = e_{HK}(J)$ if and only if $I^* = J^*$.*

Proof. The ($\Leftarrow$) direction is not difficult and is left as an exercise to the reader, along with the following hint:

Hint. First show that there exists a $c \in R^\circ$ such that $c J^{[p^e]} \subseteq I^{[p^e]}$ for all $q \gg 0$. Set $S = R/\langle c \rangle$ and consider its Hilbert–Kunz multiplicity with respect to I. Finally show that there exists an integer k such that $(S/(IS)^{[p^e]})^{\oplus k}$ can be mapped onto $J^{[p^e]}/I^{[p^e]}$ for all $e \geq 0$. $\square$

Theorem 8.36 ([78, Proposition 15]). *If R is a ring, then for any two $\mathfrak{m}$-primary ideals $I \subseteq J$*

$$s(R) \leq \frac{e_{\mathrm{HK}}(I) - e_{\mathrm{HK}}(J)}{\ell_R(J/I)}. \tag{8.36.1}$$

Question 8.37. Can one always find $\mathfrak{m}$-primary ideals $I \subseteq J$ such that equality holds in (8.36.1)?

In many cases, such as when R is $\mathbb{Q}$-Gorenstein, the above question has a positive answer. More generally, an affirmative response would immediately imply Conjecture 5.10 [164].

8.5 *F*-ideals, *F*-stable Submodules, and *F*-pure Centers

Historically in commutative algebra, Frobenius has been used heavily to study local cohomology. In particular, if $(R, \mathfrak{m})$ is a local ring, the map $H^i_{\mathfrak{m}}(R) \to H^i_{\mathfrak{m}}(R^{1/p}) \cong H^i_{\mathfrak{m}}(R)$ is called the action of Frobenius on the local cohomology module $H^i_{\mathfrak{m}}(R)$ and denoted by F (more generally, one also has a similar action on $H^i_J(R)$ for any ideal $J \subseteq R$). Of course, one can iterate F, e-times, and obtain higher Frobenius actions $F^e : H^i_{\mathfrak{m}}(R) \to H^i_{\mathfrak{m}}(R)$.

Remark 8.38. If one is willing to use Čech cohomology to write down specific elements of $H^i_J(R)$, then the Frobenius action can be understood as raising those elements to their pth power. See [143] for more details.

Fix $F : H^i_{\mathfrak{m}}(R) \to H^i_{\mathfrak{m}}(R)$ consider now the following ascending chain of submodules.

$$\ker F \subseteq \ker F^2 \subseteq \ker F^3 \subseteq \cdots$$

In [64] (also see [105], [46] and [13]) it was shown that this ascending chain eventually stabilizes, even though the module in question is Artinian, and not generally Noetherian. Set N to be that stable submodule. It is obvious that $F(N) \subseteq N$. On the other hand, Karen Smith observed that $0^*_{H^{\dim R}_{\mathfrak{m}}(R)}$ is the unique largest submodule $M \subseteq H^{\dim R}_{\mathfrak{m}}(R)$, with non-zero annihilator such that $F(M) \subseteq M$, see [144]. Motivated by this, she made the following definition:

Definition 8.39 ([143]). An ideal $I \subseteq R$ is called an *F-ideal* if $M_I = \mathrm{Ann}_{H^d_{\mathfrak{m}}(R)} I$ satisfies the condition $F(M_I) \subseteq M_I$.

Suppose that $(R, \mathfrak{m})$ is Gorenstein. Then as in Subsection 3.3, we have a map $\Phi_R : R^{1/p} \to R$. The Matlis dual of this map is $F : H^d_{\mathfrak{m}}(R) \to H^d_{\mathfrak{m}}(R)$ by local duality, see Theorem A.6.

Exercise 8.40. Still assuming that R is Gorenstein, prove that I is an F-ideal if and only if $\Phi_R(I^{1/p}) \subseteq I$.

It turns out that this notion is very closely related to *log canonical centers* in characteristic zero. Motivated by this connection we define the following.

Definition 8.41 ([25, 126]). A prime ideal $Q \in \operatorname{Spec} R$ is called an *F-pure center* if for every $e > 0$ and every $\phi \in \operatorname{Hom}_R(R^{1/p^e}, R)$, one has $\phi(Q^{1/p^e}) \subseteq Q$. It is very common to also assume that R_Q is F-pure.

More generally, given some fixed $\phi \in \operatorname{Hom}_R(R^{1/p^e}, R)$, an ideal $Q \in \operatorname{Spec} R$ is called an *F-pure center of* (R, ϕ), if $\phi(Q^{1/p^e}) \subseteq Q$. If additionally ϕ is a Frobenius splitting, then Q (or the variety it defines) is called *compatibly ϕ-split*.

Exercise 8.42. Suppose that R is F-pure and $Q \in \operatorname{Spec} R$ is an *F-pure center*. Show that R/Q is also F-pure. Compare with [8, 87, 91] keeping in mind that F-pure singularities are closely related to log canonical singularities cf. Exercise 8.14.

Exercise 8.43 ([126], cf. [2]). Suppose that R is F-pure and $Q \in \operatorname{Spec} R$ is an *F-pure center* which is maximal with respect to inclusion. Prove that R/Q is strongly F-regular. Compare with [88]. If R is local, prove further that Q is the splitting prime, Definition 8.24.

The structure of Frobenius stable submodules (and their annihilators) has been an important object of study in commutative algebra for several decades. In particular, several questions about their finiteness have been asked, and also answered, see for example [39], [41] and [134]. These questions are closely related to the finiteness of F-pure centers or compatibly ϕ-split ideals. See [124, 96] for answers to this question and see [13, 133] for generalizations.

Exercise* 8.44 ([126]). Suppose that (X, Δ) is a log $\mathbb{Q}$-Gorenstein pair of any characteristic, see Definition 4.10. Then a subscheme $Z \subseteq X$ is called a *log canonical center* if there exists a proper birational map $\pi : \widetilde{X} \to X$ with $\widetilde{X}$ normal and a prime divisor E on $\widetilde{X}$ such that $\pi(E) = Z$ and also such that the coefficient of E in $K_{\widetilde{X}} - \pi^*(K_X + \Delta)$ is -1.

Suppose now that $(X = \operatorname{Spec} R, \Delta)$ is a log $\mathbb{Q}$-Gorenstein pair of characteristic $p > 0$ and that $\Delta = \Delta_\phi$ for some $\phi : R^{1/p^e} \to R^{1/p^e}$ as in (4.15.1). Show that every log canonical center of (X, Δ) is an F-pure center of (R, ϕ).

A Canonical Modules and Duality

A.1 Canonical Modules, Cohen–Macaulay and Gorenstein Rings

Throughout this section, we restrict ourselves to rings of finite type over a field k. The generalization of the material in this section to rings of essentially finite type is obtained via localization, and so will be left to the reader as an exercise. In particular, we assume that $R = k[x_1, \ldots, x_n]/I = S/I$.

All the material in this section can be found in [27] or [59].

Definition A.1. Suppose that R is as above and additionally that R is equidimensional of dimension d. Then we define the *canonical module*, ω_R of R, to be the R-module

$$\omega_R := \text{Ext}_S^{n-d}(R, S).$$

We state several facts about canonical modules for the convenience of the reader. Please see [60], [59] or [27] for details and generalizations.

  (i) If R is a normal domain, then ω_R is isomorphic to an unmixed ideal of height one in R. In particular, it can be identified with a divisor on Spec R. Any such divisor is called a *canonical divisor*, see also Appendix B.

 (ii) If $R = S/\langle f \rangle$, then it is easy to check that $\omega_R \cong R = S/\langle f \rangle$. (Write down the long exact sequence computing Ext.)

(iii) The canonical module as defined seems to depend on the choice of generators and relations (geometrically speaking, it depends on the embedding). In the context we are working in, ω_R is in fact unique up to isomorphism. In greater generality, the canonical module is only unique up to tensoring with locally-free rank-one R-module.

Definition A.2. With R equidimensional of dimension d, we say that R is *Cohen–Macaulay* if $\text{Ext}_S^i(R, S) = 0$ for all $i \neq n - d$. We say that R is *Gorenstein* if R is Cohen–Macaulay and additionally if for each maximal ideal $\mathfrak{m} \in \text{Spec } R$ we have that $(\omega_R)_\mathfrak{m} \cong R_\mathfrak{m}$ (abstractly).

For the reference of the reader we also recall some facts about Cohen–Macaulay and Gorenstein rings.

  (i) In a Cohen–Macaulay ring, ω_R has finite injective dimension and so in a Gorenstein ring, R has finite injective dimension.

 (ii) If $R = S/(f)$ then R is Cohen–Macaulay and Gorenstein (this also holds if R is a complete intersection).

(iii) A regular ring is always Gorenstein, and in particular, it is Cohen–Macaulay.

(iv) A local ring $(R, \mathfrak{m})$ is Cohen–Macaulay if and only if $H_\mathfrak{m}^i(R) = 0$ for all $0 \leq i < \dim R$.

(v) If $g \in R$ is a regular element and R is local, then $R/\langle g \rangle$ is Gorenstein (respectively Cohen–Macaulay) if and only if R is Gorenstein (respectively Cohen–Macaulay).[12]

Finally, we include one more definition.

Definition A.3. A normal ring R is called $\mathbb{Q}$-*Gorenstein* if the canonical module ω_R, when viewed as a height-one fractional ideal $\omega_R \subseteq K(R)$, has a symbolic power $\omega_R^{(n)}$ which is locally free (for some $n > 0$).

Equivalently, after viewing $\omega_R \subseteq R$ as a fractional ideal, one may associate a divisor K_R on Spec R. The symbolic power statement then is the same as saying that nK_R is Cartier.

A.2 Duality

In this section we discuss duality and transformation rules for canonical modules. First we recall Matlis duality and the surrounding definitions. Throughout this section, we restrict ourselves to rings essentially of finite type over a field.

Definition A.4 (Injective hull, [26, 27, 59, 60]). Suppose that $(R, \mathfrak{m})$ is a local ring. An *injective hull E of the residue field $R/\mathfrak{m}$* is a an injective R-module $E \supseteq k$ that satisfies the following property:

- For any non-zero submodule $U \subseteq E$ we have $U \cap k \neq \{0\}$.

Injective hulls of the residue field are unique up to non-unique isomorphism. They are in a very precise sense the smallest injective module containing E, see [27, Proposition 3.2.2] for additional discussion.

Theorem A.5 (Matlis Duality, [26, 27, 59, 60]). *Suppose that $(R, \mathfrak{m})$ is a local ring and that E is the injective hull of the residue field. Then the functor $\mathrm{Hom}_R(\_, E)$ is a faithful exact functor on the category of Noetherian R-modules. More-over, applying this functor twice is naturally isomorphic to the $\_ \otimes_R \hat{R}$ functor where $\hat{R}$ is the completion of R-along $\mathfrak{m}$.*

Additionally and in particular, if R is already complete, then $\mathrm{Hom}_R(\_, E)$ induces an equivalence of categories between Artinian R-modules and Noetherian R-modules (and vice versa).

Now we state a special case of *local-duality*.

Theorem A.6 (Local Duality, [26; 59, Chapter V, Section 6; 60]). *Suppose that $(R, \mathfrak{m})$ is a local ring and that E is the injective hull of the residue field. Then for any finitely generated R-module M:*

$$\mathrm{Hom}_R(\mathrm{Hom}_R(M, \omega_R), E) \cong H_{\mathfrak{m}}^{\dim R}(M).$$

---

[12] Notice that (v) + (iii) also imply (ii).

In particular $H_{\mathfrak{m}}^{\dim R}(\omega_R) \cong E$ so that if R is Gorenstein then $H_{\mathfrak{m}}^{\dim R}(R) \cong E$. Furthermore, if R is Cohen–Macaulay, then we have a natural isomorphism

$$\operatorname{Hom}_R(\operatorname{Ext}_R^i(M, \omega_R), E) \cong H_{\mathfrak{m}}^{\dim R - i}(M)$$

for all $i \geq 0$.

Remark A.7. If one is willing to work in the bounded derived category with finitely generated cohomology $D_{\mathrm{coh}}^b(R)$, then one obtains the more general statement (without any Cohen–Macaulay hypothesis):

$$\operatorname{Hom}_R(\mathbf{R}\operatorname{Hom}_R^{\bullet}(M, \omega_R^{\bullet}), E) \simeq_{\mathrm{qis}} \mathbf{R}\Gamma_{\mathfrak{m}}(M).$$

where $\omega_R^{\bullet}$ is the dualizing complex of R.

Finally, we remark on the following transformation rule for the canonical module

Theorem A.8. *Suppose that $R \subseteq S$ is a finite extension of normal rings essentially of finite type over a field k. Then*

$$\operatorname{Hom}_R(S, \omega_R) \cong \omega_S.$$

Proof. This is contained in for example [27, Theorem 3.3.7(b)] for Cohen–Macaulay local rings and the statement holds more generally for Cohen–Macaulay schemes. In particular, both modules are automatically isomorphic (with a natural isomorphism) on the Cohen–Macaulay-locus. But both modules are reflexive, and thus since the non-Cohen–Macaulay locus is of codimension at least 2, the modules are isomorphic. □

Remark A.9. We will be applying Theorem A.8 to the case of the inclusion $R \subseteq R^{1/p}$. While R is finite type over k, $R^{1/p}$ is of finite type over $k^{1/p}$. If k is perfect, then $k^{1/p} = k$ and the inclusion $R \subseteq R^{1/p}$ can be interpreted as being k-linear (although with possibly different choices of generators and relations for $R^{1/p}$ over k). If k is not perfect, then $R^{1/p}$ need not be finite type over k, but it is if $[k^{1/p} : k] < \infty$ and again in this case the generators and relations for $R^{1/p}$ over k maybe different than those over $k^{1/p}$.

However, as long as $[k^{1/p} : k] < \infty$, then it can be shown that $\omega_{R^{1/p}} \cong (\omega_R)^{1/p}$ or in other words that $\omega_{F_*R} \cong F_*\omega_R$. Also see the discussion around condition (†) in [18, p. 921].

Remark A.10. If one is willing to work in the derived category $D_{\mathrm{coh}}^b(R)$, then Theorem A.8 should be viewed as a generalization of the following special case of duality for a finite morphism where $M \in D_{\mathrm{coh}}^b(S)$:

$$\mathbf{R}\operatorname{Hom}_R^{\bullet}(M, \omega_R^{\bullet}) \cong \mathbf{R}\operatorname{Hom}_S^{\bullet}(M, \omega_S^{\bullet}).$$

Simply take $M = S$.

In fact, there is the following generalization of the above remark.

Theorem A.11 (Grothendieck Duality, [59]). *Suppose that $f : Y \to X$ is a proper morphism of varieties over a field k. Then $\omega_X^{\bullet}$ and $\omega_Y^{\bullet}$ exist and furthermore, for any coherent sheaf $\mathscr{M}$ (or more generally object of $D_{\mathrm{coh}}^b(X)$), we have a functorial isomorphism*

$$\mathbf{R}\,\mathscr{H}om_{\mathscr{O}_X}^{\bullet}(\mathbf{R}f_*\mathscr{M}, \omega_X^{\bullet}) \simeq_{qis} \mathbf{R}f_*\mathbf{R}\,\mathscr{H}om_{\mathscr{O}_Y}^{\bullet}(\mathscr{M}, \omega_Y^{\bullet})$$

in $D_{\mathrm{coh}}^b(X)$. In particular, if we set $\mathscr{M} = \mathscr{O}_Y$, we have an isomorphism:

$$\mathbf{R}\,\mathscr{H}om_{\mathscr{O}_X}^{\bullet}(\mathbf{R}f_*\mathscr{O}_Y, \omega_X^{\bullet}) \simeq_{qis} \mathbf{R}f_*\omega_Y^{\bullet}.$$

Corollary A.12. *Suppose that $\pi : Y \to X$ is a proper morphism of varieties of the same dimension over a field k. Then we have a natural map*

$$\pi_*\omega_Y \to \omega_X.$$

Proof. Consider the natural map $\mathscr{O}_X \to \mathbf{R}\pi_*\mathscr{O}_Y$ and then apply the contra-variant Grothendieck-duality functor $\mathbf{R}\,\mathscr{H}om_{\mathscr{O}_X}(\_, \omega_X^{\bullet})$, use the second half of Theorem A.11 and then take cohomology (the fact that $\mathscr{H}^{-\dim Y}\mathbf{R}f_*\omega_Y^{\bullet} \cong \pi_*\omega_Y$ follows by analyzing the associated spectral sequence). $\square$

B Divisors

In this section, we review divisors on normal algebraic varieties. Divisors are sometimes a stumbling block for commutative algebraists trying to apply the techniques of algebraic geometry. As such, this appendix is designed to serve as a reference for divisors for those already familiar with commutative algebra. For those more geometrically inclined, please read [61, Chapter II, Section 6] or [62].

We treat divisors here only in the case of an affine variety and describe them using symbolic powers. The generalization to non-affine varieties is left to the reader. Of course within the broader field of algebraic geometry, the formalism of divisors is most useful in the study of projective (non-affine) varieties.

Definition B.1. Suppose that R is a normal domain of finite type over a field, and let $X = \mathrm{Spec}\, R$ be the corresponding normal affine algebraic variety. Then a *prime divisor* on X is a codimension 1 subvariety of X, and a *Weil divisor on X* is a formal $\mathbb{Z}$-linear combination of prime divisors. In other words, a Weil divisor is an element of the free Abelian group on the set of all prime divisors.

Remark B.2. A prime divisor is exactly the same data as a height one prime ideal $P \subseteq R$. More generally, a Weil divisor can be viewed as the combined data of a

finite set of height-one prime ideals with formal coefficients n_i. In other words $D = \sum n_i V(P_i)$ where the P_i are prime ideals and $V(P_i) = \{Q \in \operatorname{Spec} R \mid P_i \subseteq Q\} = \operatorname{Spec}(R/P_i) \subseteq X$ is the vanishing locus of P_i.

Given a prime $P \in \operatorname{Spec} R$, and an integer $n > 0$, we use $P^{(n)} = (P^n R_P) \cap R$ to denote the n-th symbolic power of P. If $n = 0$, then $P^{(n)} = R$. If $n < 0$ then $P^{(n)}$ is the fractional ideal which is the inverse to $P^{(|n|)}$. Explicitly, $P^{(n)} = \{x \in K(R) \mid x P^{(|n|)} \subseteq R\}$.

Definition B.3. Given a divisor $D = \sum n_i V(P_i)$ on an algebraic variety $X = \operatorname{Spec} R$, the sheaf $\mathcal{O}_X(D)$ is simply the coherent sheaf of $\mathcal{O}_X$-modules associated with the fractional ideal $\bigcap_i P_i^{(-n_i)}$. In particular, note also that $\mathcal{O}_X(-D)$ is determined by $\bigcap_i P_i^{(n_i)}$.

Because the category of coherent sheaves of $\mathcal{O}_X$-modules is equivalent to the category of finitely generated R-modules, in what follows we will treat $\mathcal{O}_X(D)$ as if it was a fractional ideal and not a sheaf.

Remark B.4. A key property of $\mathcal{O}_X(D) = \bigcap_i P_i^{(-n_i)}$ is that it is S2 as an R-module. Because it has full dimension and R is normal, this means that it is also reflexive as an R-module (in other words, applying the functor $\operatorname{Hom}_R(\_, R)$ twice yields an isomorphic module). Therefore if $\mathcal{O}_X(D) = \bigcap_i P_i^{(-n_i)}$ and $\mathcal{O}_X(E) = \bigcap_i P_i^{(-m_i)}$ then $\mathcal{O}_X(D+E) = \bigcap_i P_i^{(-n_i-m_i)}$ is the largest ideal that agrees with $\mathcal{O}_X(D) \cdot \mathcal{O}_X(E)$ at all the height-one-primes of R. See [62] for additional discussion.

Definition B.5. We now list some common properties/prefixes associated to Weil divisors. Suppose that $D = \sum n_i V(P_i)$ is a Weil divisor on $X = \operatorname{Spec} R$.

(i) D is called *effective* if all of the n_i's are non-negative.

(ii) D is called *Cartier* if for every maximal (equivalently prime) ideal $\mathfrak{m} \in \operatorname{Spec} R$, $(\mathcal{O}_X(D))_\mathfrak{m}$ is a principal ideal. In other words, if $\bigcap_i P_i^{(-n_i)}$ is locally principal.

(iii) D is called *reduced* if all of the n_i's are equal to 1.

(iv) D is called $\mathbb{Q}$-*Cartier* if there exists an integer $n > 0$ such that nD is Cartier. Equivalently, this means $(\bigcap_i P_i^{(-n_i)})^{(n)}$ is locally principal. The *index* of a $\mathbb{Q}$-Cartier divisor is the smallest such n.

(v) D is called a *canonical divisor* if $\mathcal{O}_X(D)$ is (abstractly) isomorphic to a canonical module of R.

(vi) A reduced divisor is said to have *normal crossings* if it is Cartier, and for each $\mathfrak{q} \in \operatorname{Spec} R$ containing the ideal $\mathcal{O}_X(-D)$, $R_\mathfrak{q}$ is regular and $(\mathcal{O}_X(-D))_\mathfrak{q} = (\bigcap_i P_i^{(n_i)})_\mathfrak{q}$ is an ideal generated by a product of minimal generators of the maximal ideal of R_P. If each R/P_i is a regular ring, we then say that D has *simple normal crossings*.

(vii) Two divisors D and E are said to be *linearly equivalent* if $\mathcal{O}_X(D)$ is abstractly isomorphic to $\mathcal{O}_X(E)$. In that case, we write $D \sim E$.

(viii) The non-zero elements $x \in \Gamma(X, \mathcal{O}_X(D))$ are in bijective correspondence with effective divisors linearly equivalent to D.

Exercise B.6. Prove that every divisor in a regular ring is Cartier and that every pair of Cartier divisors in a regular local ring are linearly equivalent.

Exercise B.7. Prove that $V(\langle x, y \rangle)$ on $\operatorname{Spec} k[x, y, z]/(x^2 - yz)$ is not Cartier but is $\mathbb{Q}$-Cartier.

Finally we also describe $\mathbb{Q}$-divisors.

Definition B.8. A $\mathbb{Q}$-*divisor* is a formal sum $\sum_i n_i D_i = \sum_i n_i V(P_i)$ of prime divisors with rational coefficients $n_i \in \mathbb{Q}$. The set of $\mathbb{Q}$-divisors also form a group under addition.

Remark B.9. It is also very natural to define $\mathbb{R}$-divisors. We will not do that here however.

Definition B.10. We now state some common terminology with $\mathbb{Q}$-divisors.
Fix a $\mathbb{Q}$-divisor $\Delta = \sum n_i D_i$

 (i) Δ is called *effective* if all of the n_i's are non-negative.

 (ii) We define $\lceil \Delta \rceil = \sum_i \lceil n_i \rceil D_i$, likewise $\lfloor \Delta \rfloor = \sum_i \lfloor n_i \rfloor D_i$.

(iii) When dealing with a $\mathbb{Q}$-divisor D, we say that D is *integral* if D is simultaneously a Weil-divisor and a $\mathbb{Q}$-divisor (in other words, if all the n_i are integers).

(iv) We say that Δ is a $\mathbb{Q}$-Cartier divisor if there exists an integer $n > 0$ such that $n\Delta$ is an integral divisor and a Cartier divisor. The *index* of a $\mathbb{Q}$-Cartier $\mathbb{Q}$-divisor is the smallest such n.

 (v) We say that two $\mathbb{Q}$-divisors Δ_1 and Δ_2 are $\mathbb{Q}$-linearly equivalent if there exists an integer $n > 0$ such that $n\Delta_1$ and $n\Delta_2$ are linearly equivalent integral Weil-divisors. In this case we write $\Delta_1 \sim_{\mathbb{Q}} \Delta_2$.

C Glossary and Diagrams on Types of Singularities

We collect the various measures of and types of singularities in characteristic p. Most of these are mentioned in the paper. First we display a diagram explaining the relationship between the various singularity classes in characteristic zero and characteristic $p > 0$.
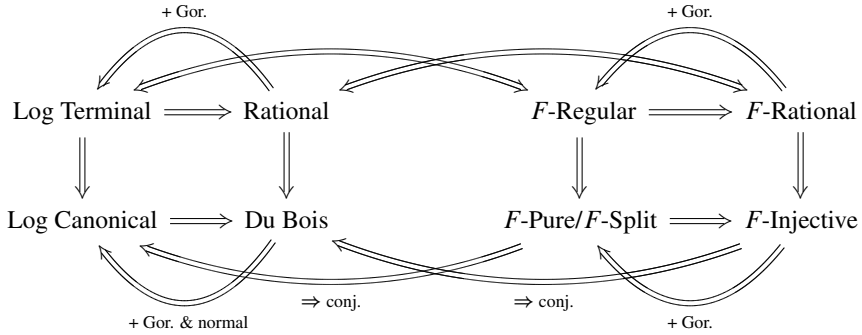
The left-square is classes of singularities in characteristic zero. The right side is classes of singularities in characteristic $p > 0$. An arrow $A \Rightarrow B$ between two classes of singularities means that all singularities of type A are also of type B. For example, the arrow Log terminal $\Rightarrow$ Rational means that all log terminal singularities are rational.

The connecting arrows between the two squares are via reduction to characteristic p, see [51, 57, 110, 125, 144]. There has been some progress on the conjectural direction between F-pure and log canonical singularities, [52, 65, 115, 116, 135, 154].

It should be noted that some of the implications on the characteristic zero side are highly non-trivial, see [38, 91, 93, 122].

C.1 Glossary of Terms

(Big) test ideal. Given an F-finite reduced ring R of characteristic p, the *(big) test ideal* $\tau(R) = \tau_b(R)$ is defined to be the smallest ideal $I \subseteq R$, not contained in any minimal prime, such that $\phi(I^{1/p^e}) \subseteq I$ for all $e \geq 0$ and all $\phi \in \mathrm{Hom}_R(R^{1/p^e}, R)$. It also coincides with $\bigcap_M (0 :_R 0^*_M)$ where M runs over all R-modules. The big test ideal is closely related to the multiplier ideal in characteristic zero, see [53, 146] for the original statements and see [58, 151] for generalizations to pairs.

(Big/finitistic) test element. An element $r \in R$ which is not contained in any minimal prime of R is called a *finitistic test element* if $z \in I^*$ implies that $cz^{p^e} \in I^{[p^e]}$ for all $e \geq 0$. It is called a *big test element* if $z \in 0^*_M$ implies that $0 = c^{1/p^e} \otimes z \in R^{1/p^e} \otimes M$ for all R-modules M. It is an open question whether these two definitions are equivalent. See [70], [107] and [68].

Completely stable (finitistic) test element. An element r in a local ring R, such that r is not contained in any minimal prime of R, is called a *completely stable test (finitistic) element* if it is a finitistic test element and if it remains a finitistic test element after both localization and completion.

Dense F-XXX type. For a given class of singularities "F-XXX" in characteristic p, a characteristic zero scheme X (or pair as appropriate) is said to have *dense F-XXX type* if for all sufficiently large finitely generated $\mathbb{Z}$-algebras A and families $X_A \to \mathrm{Spec}\, A$ of characteristic p-modules of X (in particular, the generic point of

that family agrees with X up to field-base-change), there exists a Zariski-dense set of maximal ideals $\mathfrak{q} \in \operatorname{Spec} A$ such that the fiber $X_{\mathfrak{q}}$ has F-XXX singularities.

Divisorially F-regular. The combined information of a normal variety X in characteristic $p > 0$ and an effective reduced divisor $D \subseteq X$ is called *divisorially F-regular* if for every $c \in R$, not vanishing on any component of D, there is an R-linear map $\phi : R^{1/p^e} \to R$, for some $e > 0$, which sends c^{1/p^e} to 1. Divisorially F-regular pairs were introduced in [57]. Unfortunately for the terminology, divisorially F-regular pairs correspond to *purely log terminal* singularities in characteristic zero, see [153].

F-finite. A reduced ring of characteristic $p > 0$ is called *F-finite* if $R^{1/p}$ is a finite R-module. Every ring essentially of finite type over a perfect field is F-finite. See [98].

F-injective. A reduced F-finite ring of characteristic $p > 0$ is called *F-injective* if the natural map $H^i_{\mathfrak{m}}(R) \to H^i_{\mathfrak{m}}(R^{1/p})$ is injective for every $i \geq 0$ and every maximal ideal $\mathfrak{m} \subseteq R$. See [44]. F-injective rings are closely related to rings with *Du Bois singularities* in characteristic zero, [125].

F-ideal. Suppose that $(R, \mathfrak{m})$ is a local ring. An ideal $I \subseteq R$ is called an *F-ideal* if $M_I := \operatorname{Ann}_{H^d_{\mathfrak{m}}(R)} I$ satisfies the condition $F(M_I) = M_I$, see [143].

F-jumping number. Suppose that R is an F-finite reduced ring and $\mathfrak{a} \subseteq R$ is an ideal. The *F-jumping numbers* of the pair $(R, \mathfrak{a})$ are the real numbers $t \geq 0$ such that $\tau(R, \mathfrak{a}^t) \neq \tau(R, \mathfrak{a}^{t-\varepsilon})$ for all $\varepsilon > 0$.

F-pure. A reduced ring of characteristic $p > 0$ is called *F-pure* if for every R-module M, the map $M \to M \otimes_R R^{1/p}$ is injective. If R is finite type over a perfect field, then this is equivalent to the condition that $R \to R^{1/p}$ splits as a map of R-modules. F-purity was first introduced by Hochster and J. Roberts in [75]. F-pure rings are closely related to rings with *log canonical singularities* in characteristic zero, [57]. See [57, 129, 150] for generalizations to pairs/triples.

F-pure center (a.k.a. center of F-purity). Suppose that R is an F-finite ring. A prime ideal $Q \in \operatorname{Spec} R$ is called an *F-pure center* if for every $e > 0$ and every $\phi \in \operatorname{Hom}_R(R^{1/p^e}, R)$, one has $\phi(Q^{1/p^e}) \subseteq Q$. It is very common to also assume that R_Q is F-pure. See [126].

F-pure threshold. For a given pair $(R, \mathfrak{a})$, the *F-pure threshold of* $(R, \mathfrak{a})$ is the real number $\sup\{s \geq 0 | (R, \mathfrak{a}^s)$ is F-pure$\}$. It was introduced in [156] and is an analog of the log canonical threshold. Also compare with the F-threshold introduced [117].

F-threshold. For a given pair $(R, \mathfrak{a})$ where R is a local ring with maximal ideal $\mathfrak{m}$, the *F-threshold* of the pair is the limit $\lim_{e \to \infty} \frac{\max\{r | \mathfrak{a}^r \not\subseteq \mathfrak{m}^{[p^e]}\}}{p^e}$. This coincides with the F-pure threshold when R is regular, but is distinct otherwise. It was introduced in [117].

F-rational. An F-finite reduced local ring R is called F-*rational* if it is Cohen–Macaulay and there is no proper non-zero submodule $J \subseteq \omega_R$ such that dual to the Frobenius map $F_* \omega_R \to \omega_R$ sends $F_* J$ back into J. Equivalently, R is F-rational if all ideals generated by a full system of parameters are tightly closed. See [45] for the original definitions. F-rational singularities are closely related to *rational singularities* in characteristic zero, see [144], [51] and [110].

F-regular. A ring R of characteristic $p > 0$ is called F-*regular* if all ideals in all localizations of R are tightly closed, see [70].

F-split. A scheme X of finite type over a perfect field characteristic $p > 0$ is called *F-split (or Frobenius split)* if the Frobenius map $\mathcal{O}_X \to \mathcal{O}_X^{1/p}$ splits. If X is affine and F-finite, this is the same as F-pure. The use of F-splittings to study the global geometry of schemes was introduced in [109] and [121]. Also see [48] and [25]. F-split projective schemes are closely related to *log Calabi-Yau pairs* in characteristic zero [130].

F-signature. Suppose that $(R, \mathfrak{m})$ is a local ring of characteristic $p > 0$ with perfect residue field $R/\mathfrak{m}$. Then the F-*signature* of R, denoted $s(R)$, is the limit $\lim_{e \to \infty} a_e / p^{ed}$ where a_e is the number of free R-summands of R^{1/p^e}; in other words $R^{1/p^e} = R^{\oplus a_e} \oplus M$. It was first defined explicitly in [78], also see [148]. The limit was shown to exist by the second author in [158].

F-stable submodule. Suppose M is an R-module with a Frobenius action $F : M \to M$ (an additive map such that $F(rx) = r^p F(x)$). Most typically $M = H_{\mathfrak{m}}^{\dim R}(R)$ and F is the induced action of Frobenius. Then an F-stable submodule $N \subseteq M$ is a submodule $N \subseteq M$ such that $F(N) \subseteq N$.

(FFRT) Finite F-representation type. Suppose we are given an F-finite complete local ring $(R, \mathfrak{m})$ and consider the Krull–Schmidt decomposition $R^{1/p^e} = M_{1,e} \oplus \cdots \oplus M_{n_e,e}$ of R^{1/p^e} for each e. We say that R has *finite F-representation type*, or simply *FFRT*, if the set of isomorphism classes of the $M_{i,e}$ is finite (as e varies). Rings with FFRT were introduced by [148]. It is worth mentioning that tight closure commutes with localization in rings with FFRT [166].

(Finitistic) test ideal. Given a ring R of characteristic p, the *finitistic test ideal* $\tau_{\mathrm{fg}}(R)$ is defined to be $\bigcap_{I \subseteq R} (I : I^*)$ where I^* is the tight closure of I. Classically, finitistic test ideals were known simply as test ideals, see [70].

Frobenius action. Suppose that R is a ring and M is an R-module. A *Frobenius action on M* (or simply an *F-action*) is an additive map $f : M \to M$ satisfying the rule $f(r.m) = r^p.m$ for all $r \in R$ and $m \in M$.

Generalized test ideal. In the literature, the test ideal $\tau(R, \alpha^t)$ (or more generally for more complicated pairs and triples) is often called the *generalized test ideal*. At one point it was believed that the generalized test ideal was not made up of "test elements", but it is made up of appropriately defined test elements, see Exercise 6.17 and [123].

Globally F-regular. A scheme X of characteristic $p > 0$ is called *globally F-regular* if for every effective divisor D there exists an $e > 0$ such that the Frobenius map $\mathcal{O}_X \to (\mathcal{O}_X(D))^{1/p^e}$ splits. If X is affine and F-finite, this is the same as strongly F-regular. Globally F-regular varieties were introduced in [145]. Globally F-regular projective schemes are closely related to *log Fano pairs* in characteristic zero [130].

Hartshorne–Speiser–Lyubeznik (HSL)-number. Given a local ring $(R, \mathfrak{m})$, the *Hartshorne–Speiser–Lyubeznik number* of R (or simply the *HSL-number*) is the smallest natural number $e \geq 0$ such that the kernel of the local cohomology e-iterated Frobenius

$$\ker(H_{\mathfrak{m}}^{\dim R}(R) \to H_{\mathfrak{m}}^{\dim R}(F_*^e R))$$

is equal to the kernel $\ker(H_{\mathfrak{m}}^{\dim R}(R) \to H_{\mathfrak{m}}^{\dim R}(F_*^{e+1} R))$. It is always a finite number by [64, 105]. See [134, Definition 3.14] where this definition is generalized to any Artinian R-module with a Frobenius action, instead of simply $H_{\mathfrak{m}}^{\dim R}(R)$.

Hilbert–Kunz(–Monsky) multiplicity. Given a local ring $(R, \mathfrak{m})$ of characteristic $p > 0$ and an $\mathfrak{m}$-primary ideal $\mathfrak{a}$, the *Hilbert–Kunz multiplicity of $\mathfrak{a} \subseteq R$* is defined to be

$$\lim_{e \to \infty} \mathrm{length}_R(R/\mathfrak{a}^{[p^e]}),$$

it is denoted by $e_{\mathrm{HK}}(\mathfrak{a}, R)$. Although originally thought not to always exist, [98, p. 1011], Monsky showed it did indeed always exist in [111]. It is however notoriously difficult to compute. There are many connections between the Hilbert–Kunz multiplicity and tight closure of ideals as well as the F-signature.

(Open) F-XXX type. For a given class of singularities "F-XXX" in characteristic p, a characteristic zero scheme X (or pair as appropriate) is said to have *dense F-XXX type* if for all sufficiently large finitely generated $\mathbb{Z}$-algebras A and families $X_A \to \mathrm{Spec}\, A$ of characteristic p-modules of X (in particular, the generic point of that family agrees with X up to field-base-change), there exists an open and Zariski-dense $U \subseteq \mathrm{Spec}\, A$ such that for all maximal ideals $\mathfrak{q} \in U$, the fiber $X_{\mathfrak{q}}$ has F-XXX singularities.

Sharply F-pure. A variant of F-purity for pairs introduced in [123]. This variant uses the $\lceil (p^e - 1)\Delta \rceil$ or $\lceil t(p^e - 1) \rceil$-exponent instead of $\lfloor t(p^e - 1) \rfloor$ or $\lceil tp^e \rceil$. One aspect that distinguishes it from previous F-purity definitions for pairs, see [57] [150], is that the test ideal of a sharply F-pure pair is always a radical ideal. See [123, Corollaries 3.15 and 4.3] as well as [127] and [66] for further refinements.

Splitting prime. Given an F-finite F-pure local ring $(R, \mathfrak{m})$ of characteristic $p > 0$, the *splitting prime* $\mathscr{P} \subseteq R$ is defined to be the set $\{c \in R | \phi(c^{1/p^e}) \in \mathfrak{m}, \forall e > 0, \forall \phi \in \mathrm{Hom}_R(R^{1/p^e}, R)\}$. The splitting prime was introduced by Aberbach-Enescu in [2]. It closely related to a *minimal log canonical center* in characteristic zero, see [126]. As an ideal, it is the largest F-pure center.

Strongly F-regular. An F-finite reduced ring of characteristic $p > 0$ is called *strongly F-regular* if for every $c \in R$ not contained in a minimal prime, there is an R-linear map $\phi : R^{1/p^e} \to R$, for some $e > 0$, which sends c^{1/p^e} to 1, see [69]. Strongly F-regular rings are closed related to rings with *log terminal singularities* in characteristic zero, see [57]. See [57, 129, 150] for generalizations to pairs/triples. For generalizations to the non-F-finite setting, see [68].

Strong test ideal. A *strong test ideal* for a ring R is any ideal J (not contained in any minimal prime) such that $JI^* = JI$ for all ideals $I \subseteq R$. They were introduced in [77]. The strong test ideal coincides with the test ideal in many cases, see [55] and [161]. Additional generalizations to modules can be found in [40].

Strongly F-pure. A variant of F-purity for pairs introduced in [57]. A pair (R, Δ) is strongly F-pure if there exists $\phi \in \operatorname{Hom}_R(F_*^e R(\lfloor p^e \Delta \rfloor), R) \subseteq \operatorname{Hom}_R(F_*^e R, R)$ with $\phi(F_*^e R) = R$.

Test ideal. See *big test ideal* or *finitistic test ideal*.

Test element. See *big/finitistic test element*.

Tight closure. The *tight closure I^** of an ideal $I \subseteq R$ is the set of $z \in R$ such that there exists $c \in R$, but not in any minimal prime of R, so that $cz^{p^e} \in I^{[p^e]}$ for all $e \geq 0$. See [70].

q-weak test element. An element $c \in R$ not in any minimal prime is called a *q-weak test element* if for all $p^e \geq q = p^d$, we have that $cx^{p^e} \in I^{[p^e]}$ for all $x \in I^*$ as I ranges over all ideals of R, see [70, Section 6].

Weakly F-regular. A ring R of characteristic $p > 0$ is called *weakly F-regular* if all ideals are tightly closed, see [70]. It is an open question whether weakly F-regular rings are strongly F-regular.

Bibliography

[1] Aberbach, I. M., Enescu, F., Test ideals and base change problems in tight closure theory. Trans Amer Math Soc. 2003;355:619–636 [electronic].

[2] ———, The structure of F-pure rings. Math Z. 2005;250:791–806.

[3] _____ , New estimates of Hilbert–Kunz multiplicities for local rings of fixed dimension. arXiv:1101.5078. 2011.

[4] Aberbach, I. M., Hochster, M., Huneke, C., Localization of tight closure and modules of finite phantom projective dimension. J Reine Angew Math. 1993;434:67–114.

[5] Aberbach, I. M., Leuschke, G. J., The F-signature and strong F-regularity. Math Res Lett. 2003;10:51–56.

[6] Aberbach, I. M., MacCrimmon, B., Some results on test elements. Proc Edinb Math Soc (2). 1999;42:541–549.

[7] Shankar Abhyankar, S., Resolution of singularities of embedded algebraic surfaces. vol. 24 of Pure and applied mathematics. New York: Academic Press; 1966.

[8] Ambro, F., The locus of log canonical singularities, arXiv:math.AG/9806067. 1998.

[9] Anderson, G. W., An elementary approach to L-functions mod p. J Number Theory. 2000;80:291–303.

[10] Artin, M., Wildly ramified $Z/2$ actions in dimension two. Proc Amer Math Soc. 1975;52:60–64.

[11] Blickle, M., Multiplier ideals and modules on toric varieties. Math Z. 2004;248:113–121.

[12] Blickle, M., Test ideals via algebras of p^{-e}-liner maps. J Algebraic Geom. To appear. arXiv:0912.2255. 2009.

[13] Blickle, M., Böckle, G., Cartier modules: finiteness results. J Reine Angew Math. To appear. arXiv:0909.2531. 2009.

[14] Blickle, M., Böckle, G., Minimal Cartier modules and applications to local cohomology. In preparation. 2009.

[15] Blickle, M., Lazarsfeld, R., An informal introduction to multiplier ideals. Trends in commutative algebra. vol. 51 of Mathematical Sciences Research Institute publications. Cambridge: Cambridge University Press; 2004. p. 87–114.

[16] Blickle, M., Mustaţă, M., Smith, K., Discreteness and rationality of F-thresholds. Michigan Math J. 2008;57:43–61.

[17] Blickle, M., Mustaţă, M., Smith, K. E., F-thresholds of hypersurfaces. Trans Amer Math Soc. 2009;361:6549–6565.

[18] Blickle, M., Schwede, K., Takagi, S., Zhang, W., Discreteness and rationality of F-jumping numbers on singular varieties. Math Ann. 2010;347:917–949.

[19] Blickle, M., Schwede, K., Tucker, K., F-signature of pairs. In preparation. 2011.

[20] Brenner, H., Tight closure and projective bundles. J Algebra. 2003;265:45–78.

[21] _____ , Computing the tight closure in dimension two. Math Comp. 2005;74:1495–1518 [electronic].

[22] _____ , The rationality of the Hilbert–Kunz multiplicity in graded dimension two. Math Ann. 2006;334:91–110.

[23] Brenner, H., Herzog, J., Villamayor, O., Three lectures on commutative algebra. In: Colomé-Nin, G., Cortadellas Benítez, T., Elias, J., Zarzuela, S., editors. Lectures from the Winter School on Commutative Algebra and Applications; 2006 Jan 30–Feb 3, Barcelona. vol. 42 of University Lecture Series. Providence, RI: American Mathematical Society; 2008.

[24] Brenner, H., Monsky, P., Tight closure does not commute with localization. Ann of Math (2). 2010;171:571–588.

[25] Brion, M., Kumar, S., Frobenius splitting methods in geometry and representation theory. vol. 231 of Progress in mathematics. Boston, MA: Birkhäuser Boston Inc.; 2005.

[26] Brodmann, M. P., Sharp, R. Y., Local cohomology: an algebraic introduction with geometric applications. vol. 60 of Cambridge studies in advanced mathematics. Cambridge: Cambridge University Press; 1998.

[27] Bruns, W., Herzog, J., Cohen–Macaulay rings. 2nd ed. vol. 39 of Cambridge studies in advanced mathematics. Cambridge: Cambridge University Press; 1998.

[28] Cossart, V., Piltant, O., Resolution of singularities of threefolds in positive characteristic. I. Reduction to local uniformization on Artin–Schreier and purely inseparable coverings. J Algebra. 2008;320:1051–1082.

[29] _____ , Resolution of singularities of threefolds in positive characteristic. II. J Algebra. 2009;321:1836–1976.

[30] Dale Cutkosky, S., Resolution of singularities for 3-folds in positive characteristic. Amer J Math. 2009;131:59–127.

[31] de Fernex, T., Hacon, C. D., Singularities on normal varieties. Compos Math. 2009;145:393–414.

[32] Demailly, J.-P., Ein, L., Lazarsfeld, R., A subadditivity property of multiplier ideals. Michigan Math J. 2000;48:137–156, Dedicated to William Fulton on the occasion of his 60th birthday.

[33] Ein, L., Multiplier ideals, vanishing theorems and applications. Proceedings, Algebraic geometry; 1995, Saanta Cruz. vol. 62 of Proceedings of symposia in pure matheamatics. Providence, RI: American Mathematical Society; 1997. p. 203–219.

[34] Ein, L., Lazarsfeld, R., Smith, K. E., Uniform bounds and symbolic powers on smooth varieties. Invent Math. 2001;144:241–252.

[35] Ein, L., Lazarsfeld, R., Smith, K. E., Varolin, D., Jumping coefficients of multiplier ideals. Duke Math J. 2004;123:469–506.

[36] Eisenbud, D., Commutative algebra [with a view toward algebraic geometry]. vol. 150 of Graduate texts in mathematics. New York: Springer-Verlag; 1995

[37] Eisenstein, E., Generalizations of the restriction theorem for multiplier ideals. arXiv:1001.2841. 2010.

[38] Elkik, R., Rationalité des singularités canoniques. Invent Math. 1981;64:1–6.

[39] Enescu, F., F-injective rings and F-stable primes. Proc Amer Math Soc. 2003;131:3379–3386 [electronic].

[40] _____ , Strong test modules and multiplier ideals. Manuscripta Math. 2003;111:487–498.

[41] Enescu, F., Hochster, M., The Frobenius structure of local cohomology. Algebra Number Theory. 2008;2:721–754.

[42] Enescu, F., Shimomoto, K., On the upper semi-continuity of the Hilbert–Kunz multiplicity. J Algebra. 2005;285:222–237.

[43] Esnault, H., Viehweg, E., Lectures on vanishing theorems. vol. 20 of DMV Seminar. Basel: Birkhäuser Verlag; 1992.

[44] Fedder, R., F-purity and rational singularity. Trans Amer Math Soc. 1983;278:461–480.

[45] Fedder, R., Watanabe, K., A characterization of F-regularity in terms of F-purity. Proceedings, Commutative Algebra; 1987, Berkeley, CA. vol. 15 of Mathematical Sciences Research Institute publications. New York: Springer; 1989. p. 227–245.

[46] Gabber, O., Notes on some t-structures. Geometric aspects of Dwork theory. Vol. I, II. Berlin: Walter de Gruyter GmbH & Co. KG; 2004. p. 711–734.

[47] Grauert, H., Riemenschneider, O., Verschwindungssätze für analytische Kohomologiegruppen auf komplexen Räumen. Invent Math. 1970;11:263–292.

[48] Haboush, W. J., A short proof of the Kempf vanishing theorem. Invent Math. 1980;56:109–112.

[49] Han, C., Monsky, P., Some surprising Hilbert–Kunz functions. Math Z. 1993;214:119–135.

[50] Hanes, D., Notes on the Hilbert–Kunz function. J Algebra. 2003;265:619–630.

[51] Hara, N., A characterization of rational singularities in terms of injectivity of Frobenius maps. Amer J Math. 1998;120:981–996.

[52] _____ , Classification of two-dimensional F-regular and F-pure singularities. Adv Math. 1998;133:33–53.

[53] _____ , Geometric interpretation of tight closure and test ideals. Trans Amer Math Soc. 2001;353:1885–1906 [electronic].

[54] _____ , F-pure thresholds and F-jumping exponents in dimension two [with an appendix by Monsky P]. Math Res Lett. 2006;13:747–760.

[55] Hara, N., Smith, K. E., The strong test ideal. Illinois J. Math. 2001;45:949–964.

[56] Hara, N., Takagi, S., On a generalization of test ideals. Nagoya Math J. 2004;175:59–74.

[57] Hara, N., Watanabe, K.-I., F-regular and F-pure rings vs. log terminal and log canonical singularities. J Algebraic Geom. 2002;11:363–392.

[58] Hara, N., Yoshida, K.-I., A generalization of tight closure and multiplier ideals. Trans Amer Math Soc. 2003;355:3143–3174 [electronic].

[59] Hartshorne, R., Residues and duality [Lecture notes of a seminar on the work of Alexander Grothendieck given at Harvard 1963/64, with an appendix by P. Deligne]. vol. 20 of Lecture notes in mathematics. Berlin: Springer-Verlag; 1966.

[60] _____ , Local cohomology. A seminar given by A. Grothendieck, Harvard University, Fall 1961. Berlin: Springer-Verlag; 1967.

[61] _____ , Algebraic geometry. vol. 52 of Graduate texts in mathematics. New York: Springer-Verlag; 1977.

[62] _____ , Generalized divisors on Gorenstein schemes. Proceedings of Conference on Algebraic Geometry and Ring Theory in honor of Michael Artin, Part III; 1992, Antwerp. 1994. p. 287–339.

[63] _____ , Generalized divisors and biliaison. Illinois J Math. 2007;51:83–98 [electronic].

[64] Hartshorne, R., Speiser, R., Local cohomological dimension in characteristic p. Ann of Math (2). 1977;105:45–79.

[65] Hernández, D., Log canonical singularities and F-purity for polynomials over $\mathbb{C}$, Preprint. http://www-personal.umich.edu/~dhernan/daniel/Research.html. 2011.

[66] _____ , New notions of F-purity. Work in progress. 2011.

[67] Hochster, M., Cyclic purity versus purity in excellent Noetherian rings. Trans Amer Math Soc. 1977;231:463–488.

[68] _____ , Foundations of tight closure theory [lecture notes from a course taught on the University of Michigan, Fall 2007]. http://www.math.lsa.umich.edu/~hochster/711F07/fndtc.pdf. 2007.

[69] Hochster, M., Huneke, C., Tight closure and strong F-regularity. Mém Soc Math Fr (NS). 1989;[Colloque en l'honneur de Pierre Samuel (Orsay, 1987)]:119–133, .

[70] _____ , Tight closure, invariant theory, and the Briançon–Skoda theorem. J Amer Math Soc. 1990;3:31–116.

[71] _____ , F-regularity, test elements, and smooth base change. Trans Amer Math Soc. 1994;346:1–62.

[72] _____ , Comparison of symbolic and ordinary powers of ideals. Invent Math. 2002;147:349–369.

[73] _____ , Tight closure in equal characteristic zero. Preprint. 2006.

[74] _____ , Fine behavior of symbolic powers of ideals. Illinois J Math. 2007;51:171–183 [electronic].

[75] Hochster, M., Roberts, J. L., The purity of the Frobenius and local cohomology. Adv Math. 1976;21:117–172.

[76] Huneke, C., Tight closure and its applications [with an appendix by M. Hochster]. vol. 88 of CBMS regional conference series in mathematics. Washington, DC: Conference Board of the Mathematical Sciences; 1996.

[77] _____ , Tight closure and strong test ideals. J Pure Appl Algebra. 1997;122:243–250.

[78] Huneke, C., Leuschke, G. J., Two theorems about maximal Cohen–Macaulay modules. Math Ann. 2002;324:391–404.

[79] Huneke, C., Swanson, I., Integral closure of ideals, rings, and modules. vol. 336 of London Mathematical Society lecture note series. Cambridge: Cambridge University Press; 2006.

[80] Huneke, C., Yao, Y., Unmixed local rings with minimal Hilbert–Kunz multiplicity are regular. Proc Amer Math Soc. 2002;130:661–665 [electronic].

[81] Katzman, M., The complexity of Frobenius powers of ideals. J Algebra. 1998;203:211–225.

[82] ———, Parameter-test-ideals of Cohen–Macaulay rings. Compos Math. 2008;144:933–948.

[83] ———, A non-finitely generated algebra of Frobenius maps. Proc Amer Math Soc. 2010;138:2381–2383.

[84] Katzman, M., Lyubeznik, G., Zhang, W., On the discreteness and rationality of F-jumping coefficients. J Algebra. 2009;322:3238–3247.

[85] Kawakita, M., Inversion of adjunction on log canonicity. Invent Math. 2007;167:129–133.

[86] Kawamata, Y., A generalization of Kodaira–Ramanujam's vanishing theorem. Math Ann. 1982;261:43–46.

[87] ———, Subadjunction of log canonical divisors for a subvariety of codimension 2. Proceedings, Birational Algebraic Geometry; 1996, Baltimore, MD. vol. 207 of Contemporary Mathematics. Providence, RI: American Mathematical Society; 1997. p. 79–88.

[88] ———, Subadjunction of log canonical divisors. II. Amer J Math. 1998;120:893–899.

[89] Kempf, G., Faye Knudsen, F., Mumford, D., Saint-Donat, B., Toroidal embeddings, I. vol. 339 of Lecture notes in mathematics. Berlin: Springer-Verlag; 1973.

[90] Kollár, J., Singularities of pairs. Proceedings, Algebraic Geometry; 1995, Santa Cruz. vol. 62 of Proceedings of Symposia in Pure Mathematics. Providence, RI: American Mathematical Society; 1997. p. 221–287.

[91] Kollár, J., Kovács, S. J., Log canonical singularities are Du Bois. J Amer Math Soc. 2010;23:791–813.

[92] Kollár, J., Mori, S., Birational geometry of algebraic varieties [with the collaboration of Clemens CH and Corti A]. vol. 134 of Cambridge tracts in mathematics. Cambridge: Cambridge University Press; 1998 [translated from the 1998 Japanese original].

[93] Kovács, S. J., A characterization of rational singularities. Duke Math J. 2000;102:187–191.

[94] Kovács, S. J., Schwede, K., Hodge theory meets the minimal model program: a survey of log canonical and Du Bois singularities. In: Friedman, G., Hunsicker, E., Libgober, A., Maxim, L., editors. Topology of stratified spaces. vol. 58 of Mathematical Sciences Research Institute publications. Cambridge: Cambridge University Press; 2011. p. 51–94.

[95] Kovács, S. J., Schwede, K., Smith, K. E., The canonical sheaf of Du Bois singularities. Adv Math. 2010;224:1618–1640.

[96] Kumar, S., Mehta, V. B., Finiteness of the number of compatibly split subvarieties. Int Math Res Not IMRN. 2009:3595–3597.

[97] Kunz, E., Characterizations of regular local rings for characteristic p. Amer J Math. 1969;91:772–784.

[98] ———, On Noetherian rings of characteristic p. Amer J Math. 1976;98:999–1013.

[99] ———, Kähler differentials. Advanced lectures in mathematics. Braunschweig: Friedr. Vieweg & Sohn; 1986.

[100] Lazarsfeld, R., Positivity for vector bundles, and multiplier ideals. In: Positivity in algebraic geometry. II. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge [Results in mathematics and related areas, 3rd series]. vol. 49 of A series of modern surveys in mathematics. Berlin: Springer-Verlag; 2004,

[101] Lazarsfeld, R., Lee, K., Local syzygies of multiplier ideals. Invent Math. 2007;167:409–418.

[102] Lech, C., Inequalities related to certain couples of local rings. Acta Math. 1964;112:69–89.

[103] Lipman, J., Desingularization of two-dimensional schemes. Ann of Math (2). 1978;107:151–207.

[104] ———, Adjoints of ideals in regular local rings [with an appendix by Dale Cutkosky S]. Math Res Lett. 1994;1:739–755.

[105] Lyubeznik, G., F-modules: applications to local cohomology and D-modules in characteristic $p > 0$. J Reine Angew Math. 1997;491:65–130.

[106] Lyubeznik, G., Smith, K. E., Strong and weak F-regularity are equivalent for graded rings. Amer J Math. 1999;121:1279–1290.

[107] ———, On the commutation of the test ideal with localization and completion. Trans Amer Math Soc. 2001;353:3149–3180 [electronic].

[108] MA., McDermott. Test ideals in diagonal hypersurface rings. II. J Algebra. 2003;264:296–304.

[109] Mehta, V. B., Ramanathan, A., Frobenius splitting and cohomology vanishing for Schubert varieties. Ann of Math (2). 1985;122:27–40.

[110] Mehta, V. B., Srinivas, V., A characterization of rational singularities. Asian J Math. 1997;1:249–271.

[111] Monsky, P., The Hilbert–Kunz function. Math Ann. 1983;263:43–49.

[112] Monsky, P., Rationality of Hilbert–Kunz multiplicities: a likely counterexample. Michigan Math J. 2008;57[special volume in honor of Melvin Hochster]:605–613.

[113] ———, Transcendence of some Hilbert–Kunz multiplicities (modulo a conjecture). arXiv:0908.0971. 2009.

[114] Mustață, M., The multiplier ideals of a sum of ideals. Trans Amer Math Soc. 2002;354:205–217 [electronic].

[115] _____ , Ordinary varieties and the comparison between multiplier ideals and test ideals II. Proc Amer Math Soc. To appear. arXiv:1012.2915. 2010.

[116] Mustaţă, M., Srinivas, V., Ordinary varieties and the comparison between multiplier ideals and test ideals. Nagoya Math J. To appear. arXiv:1012.2818. 2010.

[117] Mustaţă, M., Takagi, S., Watanabe, K.-I., F-thresholds and Bernstein–Sato polynomials. Proceedings, European Congress of Mathematics. Zürich: European Mathematical Society; 2005. p. 341–364.

[118] Mustaţă, M., Yoshida, K.-I., Test ideals vs. multiplier ideals. Nagoya Math J. 2009;193:111–128.

[119] Nadel, A. M., Multiplier ideal sheaves and existence of Kähler–Einstein metrics of positive scalar curvature. Proc Natl Acad Sci USA. 1989;86:7299–7300.

[120] Peskine, C., Szpiro, L., Dimension projective finie et cohomologie locale. Applications à la démonstration de conjectures de M. Auslander, H. Bass, A. Grothendieck. Publ Math Inst Hautes Études Sci. 1973:47–119.

[121] Ramanan, S., Ramanathan, A., Projective normality of flag varieties and Schubert varieties. Invent Math. 1985;79:217–224.

[122] Saito, M., Mixed Hodge complexes on algebraic varieties. Math Ann. 2000;316:283–331.

[123] Schwede, K., Generalized test ideals, sharp F-purity, and sharp test elements. Math Res Lett. 2008;15:1251–1261.

[124] _____ , F-adjunction. Algebra Number Theory. 2009;3:907–950.

[125] _____ , F-injective singularities are Du Bois. Amer J Math. 2009;131:445–473.

[126] _____ , Centers of F-purity. Math Z. 2010;265:687–714.

[127] _____ , A refinement of sharply F-pure and strongly F-regular pairs. J Commut Algebra. 2010;2:91–109.

[128] _____ , A note on discreteness of F-jumping numbers. Proc Amer Math Soc. 2011;139:3895–3901.

[129] _____ , Test ideals in non-$\mathbb{Q}$-Gorenstein rings. Trans Amer Math Soc. 2011;363:5925–5941.

[130] Schwede, K., Smith, K. E., Globally F-regular and log Fano varieties. Adv Math. 2010;224:863–894.

[131] Schwede, K., Takagi, S., Rational singularities associated to pairs. Michigan Math J. 2008;57:625–658.

[132] Schwede, K., Tucker, K., On the behavior of test ideals under finite morphisms. arXiv:1003.433. 2010.

[133] _____ , On the number of compatibly Frobenius split subvarieties, prime F-ideals, and log canonical centers. Ann Inst Fourier (Grenoble). 2010;60:1515–1531.

[134] Sharp, R. Y., Graded annihilators of modules over the Frobenius skew polynomial ring, and tight closure. Trans Amer Math Soc. 2007;359:4237–4258 [electronic].

[135] Shibuta, T., Takagi, S., Log canonical thresholds of binomial ideals. Manuscripta Math. 2009;130:45–61.

[136] Singh, A. K., A computation of tight closure in diagonal hypersurfaces. J Algebra. 1998;203:579–589.

[137] ———, Deformation of F-purity and F-regularity. J Pure Appl Algebra. 1999;140:137–148.

[138] ———, F-regularity does not deform. Amer J Math. 1999;121:919–929.

[139] ———, The F-signature of an affine semigroup ring. J Pure Appl Algebra. 2005;196:313–321.

[140] Siu, Y. T., Multiplier ideal sheaves in complex and algebraic geometry. Sci China Ser A. 2005;48:1–31.

[141] ———, Dynamic multiplier ideal sheaves and the construction of rational curves in Fano manifolds. Complex analysis and digital geometry. vol. 86 of Acta Univ. Upsaliensis Skr. Uppsala Univ. C Organ. Hist. Uppsala: Uppsala Universitet; 2009. p. 323–360.

[142] Smith, K. E., Tight closure of parameter ideals. Invent Math. 1994;115:41–60.

[143] Smith, K. E., Test ideals in local rings. Trans Amer Math Soc. 1995;347:3453–3472.

[144] ———, F-rational rings have rational singularities. Amer J Math. 1997;119:159–180.

[145] ———, Globally F-regular varieties: applications to vanishing theorems for quotients of Fano varieties. Michigan Math J. 2000;48[dedicated to William Fulton on the occasion of his 60th birthday]:553–572.

[146] ———, The multiplier ideal is a universal test ideal. Comm Algebra. 2000;28[special issue in honor of Robin Hartshorne]:5915–5929.

[147] ———, Tight closure and vanishing theorems. Proceedings, School on Vanishing Theorems and Effective Results in Algebraic Geometry; 2000, Trieste. vol. 6 of ICTP Lecture Notes. Trieste: Abdus Salam International Center of Theoretical Physics; 2001. p. 149–213.

[148] Smith, K. E., Van den Bergh, M., Simplicity of rings of differential operators in prime characteristic. Proc Lond Math Soc (3). 1997;75:32–62.

[149] Stubbs, J. F., Potent elements and tight closure in Artinian modules [PhD thesis]. Ann Arbor, MI: ProQuest LLC, University of Michigan; 2008.

[150] Takagi, S., F-singularities of pairs and inversion of adjunction of arbitrary codimension. Invent Math. 2004;157:123–146.

[151] ———, An interpretation of multiplier ideals via tight closure. J Algebraic Geom. 2004;13:393–415.

[152] ———, Formulas for multiplier ideals on singular varieties. Amer J Math. 2006;128:1345–1362.

[153] ———, A characteristic p analogue of plt singularities and adjoint ideals. Math Z. 2008;259:321–341.

[154] _____ , Adjoint ideals and a correspondence between log canonicity and F-purity. arXiv:1105.0072. 2011.

[155] Takagi, S., Takahashi, R., D-modules over rings with finite F-representation type. Math Res Lett. 2008;15:563–581.

[156] Takagi, S., Watanabe, K.-I., On F-pure thresholds. J Algebra. 2004;282:278–297.

[157] Takagi, S., Yoshida, K.-I., Generalized test ideals and symbolic powers. Michigan Math J. 2008;57[special volume in honor of Melvin Hochster]:711–724.

[158] Tucker, K., F-signature exists. arXiv:1103.4173. 2011.

[159] Vassilev, J. C., Test ideals in quotients of F-finite regular local rings. Trans Amer Math Soc. 1998;350:4041–4051.

[160] Viehweg, E., Vanishing theorems. J Reine Angew Math. 1982;335:1–8.

[161] Vraciu, A., Strong test ideals. J Pure Appl Algebra. 2002;167:361–373.

[162] _____ , A new version of α-tight closure. Nagoya Math J. 2008;192:1–25.

[163] Watanabe, K.-I., Yoshida, K.-I., Hilbert–Kunz multiplicity and an inequality between multiplicity and colength. J Algebra. 2000;230:295–317.

[164] _____ , Minimal relative Hilbert–Kunz multiplicity. Illinois J Math. 2004;48:273–294.

[165] _____ , Hilbert–Kunz multiplicity of three-dimensional local rings. Nagoya Math J. 2005;177:47–75.

[166] Yao, Y., Modules with finite F-representation type. J Lond Math Soc (2). 2005;72:53–72.

Author Information

Karl Schwede, Department of Mathematics, The Pennsylvania State University, University Park, PA, USA.
E-mail: schwede@math.psu.edu

Kevin Tucker, Department of Mathematics, Princeton University, Princeton, NJ, USA.
E-mail: kftucker@princeton.edu

Finite-dimensional Vector Spaces with Frobenius Action

Florian Enescu

Abstract. We present the structure of finite-dimensional vector spaces that admit a Frobenius action, with emphasis on the case of vector spaces over a perfect field where the module theory over noncommutative principal ideal domains allows for a unified treatment.

Keywords. Frobenius Homomorphism, Frobenius Action, Antinilpotent Module, Noncommutative PID, Perfect Field.

2010 Mathematics Subject Classification. 13A35.

1 Introduction

Among all the modules defined over a commutative ring of positive characteristic a special class arises naturally. These are the modules that admit a Frobenius action and their properties have been studied extensively in commutative algebra in recent years. More precisely, if A is a commutative ring of prime characteristic p, then, for an A-module M, a Frobenius action is an additive map $F_M : M \to M$ such that $F_M(am) = a^p F_M(m)$ for all $a \in A, m \in M$. Perhaps the most important example of nontrivial A-modules with a natural Frobenius action is given by the local cohomology modules of A with support in an ideal I of A, namely $H_I^i(A), i = 0, 1, \ldots$. The Frobenius action on these local cohomology modules is induced from the natural action on the ring via the Čech complex. One remarkable point is that important properties of a local ring $(A, \mathfrak{m})$ can be often rephrased in terms of the Frobenius action on the local cohomology modules of A with support in its maximal ideal. This approach has been developed and exploited by many of authors who produced significant results in the theory of rings of positive characteristic, with many of these results connected to either tight closure theory or birational geometry (see [4–9, 11–13, 17, 18, 20–25, 30–41] for a representative but incomplete list).

The particular case of finite dimensional vector spaces that admit a Frobenius action has connections to other areas of mathematics, such as number theory and Lie algebras. However, this case was not systematically studied and presented, with results developed only as needed, scattered through the literature, and often rediscovered by different authors. A coherent and complete presentation of this theory has not been available so far, even if it is considered a classical subject. Work for the vector space

case has been included in papers of Blickle and Böckle [9], Hochster [17], Harthsorne
and Speiser [16], Lyubeznik [23] and Yoshino [43]. This paper is meant to serve the
commutative algebra community, by providing a place where the contributions on this
subject are collected. Moreover, there is one particular current direction of research
where we expect that the study here will be useful. The notion of F-injectivity for rings
of positive characteristic has been studied at length in the past decade or so. Most of
the work has been carried in the case of Cohen–Macaulay rings where F-injectivity is
considerably easier to handle. We expect that the results and techniques collected here
to help in the study of F-injective rings that are generalized Cohen–Macaulay. In this
case, the local cohomology modules of index strictly less that the dimension of the
ring have finite length, and hence they could be investigated with the tools presented
here. We included one result, Theorem 7.14, that illustrates this idea.

Our plan is to provide a unifying point of view to the theory of finite dimensional
vector spaces with a Frobenius action, including the most important results of the
theory and exploring connections to current research. We framed our presentation by
following some classical work of N. Jacobson which applies naturally in the case of
vector spaces over a perfect field, and puts the theory in a new light. Moreover, it gives
the opportunity to the reader to rediscover and appreciate important work in module
theory which nowadays is not included in standard textbooks of modern algebra. This
work is the classification of finitely generated modules over noncommutative principal
ideal domains based on the work of Asano [1, 2], Nakayama [29], Teichmüller [42],
and presented beautifully by Jacobson in his classical treatise [26].

2 A Noncommutative Principal Ideal Domain

We will first introduce the objects of our study. Let K be a field of positive characteris-
tic p, where p is prime. Then K admits the natural Frobenius homomorphism defined
by $F(k) = k^p$, for all $k \in K$.

Let $K\{F\}$ be the skew polynomial ring in the indeterminate F with coefficients in
K, modulo the relations given by $Fk = k^p F$, for all $k \in K$.

More precisely, this ring is defined by considering the set of all formal expressions
$\sum_{i=0}^{n} a_i F^i$ where F is an indeterminate, $n \in \mathbb{N}$ and $a_i \in K$ for all $i = 0, \ldots, n$.
The elements of this set will be called polynomials in F by analogy to the commuta-
tive case. Endow this set with the operations of addition and multiplication in the
following way: the addition is the natural addition operation of polynomials and the
multiplication has the property that

$$ a F^k \cdot b F^l := a F^k b F^l = a b^{p^k} F^k F^l = a b^{p^k} F^{k+l}, $$

for all $a, b \in K, k, l \in \mathbb{N}$, and it is extended to arbitrary polynomials via the distribu-
tive property of multiplication over addition.

It is a routine check to verify that this set together with these two operations forms a noncommutative ring. We denote this ring by $K\{F\}$ and call its elements (skew) polynomials.

This construction can be performed in a more general setting where K can be replaced by any ring R and F by a ring endomorphism of R. Rings obtained in such way are called *skew polynomials rings* and are a basic construction in noncommutative ring theory, see Chaper 1 in [15] and Chapter 1 in [28].

Let V be a finite dimensional K-vector space and $F_V : V \to V$ a Frobenius action on V, that is F_V is additive and $F_V(kv) = k^p F_V(v)$ for all $k \in K$ and $v \in V$. Allowing a Frobenius action on V is equivalent to endowing V with a left $K\{F\}$-module structure by putting $F \cdot v = F_V(v)$. For these reasons, we will simply denote the action on V by $F = F_V$.

Therefore the study of vector spaces with a Frobenius action is equivalent to that of the category of left modules over the skew polynomial ring $K\{F\}$. Skew polynomial rings have been long-studied, and in what follows we will present the applications to their module theory with an eye towards the case we have in mind, that of finite dimensional vector spaces with a Frobenius action. It should be noted here that a notion of Cartier modules has been defined recently by Blickle and Böckle in [9]. A vector space V over a field K of positive characteristic p is called a Cartier vector space if it admits a Cartier map, that is an additive map $C_V : V \to V$ such that $C_V(a^p v) = a C_V(v)$ for all $a \in K, v \in V$. These vector spaces are exactly the right modules over the ring $K\{F\}$. The connection between left and right modules over the skew polynomial ring have been studied recently in [36] in addition to [9]. The theory that we present in this paper can be developed analogously for right modules, but we will not pursue it here.

If $f = a_0 + a_1 F + \cdots + a_n F^n \in K\{F\}$ with $a_n \neq 0$, we say that f has degree n and write $\deg(f) = n$. Using the degree function one can easily check that $K\{F\}$ is a domain. The degree function also gives a division and remainder type theorem:

Proposition 2.1. *Let f, g be two polynomials in $K\{F\}$. Assume that $g \neq 0$.*

(i) *There exists uniquely determined $q, r \in K\{F\}$ such that $f = qg + r$ and either $r = 0$ or $\deg(r) < \deg(g)$.*

(ii) *Assume that $F : K \to K$ is a automorphism, i.e. K is perfect. Then there exists uniquely determined $q, r \in K\{F\}$ such that $f = gq + r$ and either $r = 0$ or $\deg(r) < \deg(g)$.*

Proof. The proof is a routine exercise. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\Box$

This proposition enables one to show the following important result (see Theorem 1.11 in [15] for a more general setting and a proof).

Theorem 2.2. *The ring $K\{F\}$ is a left principal ideal domain (i.e. all left ideals are principal). If K is perfect then $K\{F\}$ is a left and right principal ideal domain (i.e. all left ideals and all right ideals are principal).*

Definition 2.3. A noncommutative ring R that is a left and right principal ideal domain will be called a *noncommutative PID*. In this paper, all such examples will be of noncommutative rings, so a noncommutative PID will be sometimes called simply a PID.

We have the following important properties of a noncommutative PID.

Proposition 2.4. *Let R be a noncommutative PID. Then R is left and right Noetherian. Moreover, the descending chain condition holds for chains of left (respectively, right) ideal that have nonzero intersection. Therefore if $0 \neq a \in R$ then R/Ra is left Artinian and R/aR is right Artinian.*

3 Ideal Theory and Divisibility in Noncommutative PIDs

In this section we let R denote a noncommutative PID. We present some of the basic features of ideal theory and divisibility in such a ring, using Jacobson's treatment, [26], as reference. We included proofs for some of the results, while in some cases we only indicated what is behind the proofs. When explanations are missing we invite the reader to consult the original work which is quite readable even today.

Two-sided ideals of R will be simply referred to as ideals. A left (respectively, right) generator for an left (respectively, right) ideal I is an element a such that $I = Ra$ (respectively, $I = aR$). Two elements a, b in R are called *left associated* if there exist $u, v \in R$ such that $a = ub, b = va$. These conditions imply that $uv = vu = 1$ if $a \neq 0$ or, equivalently, $b \neq 0$. Hence, for a left ideal in R, the left generators a and b for I are left associated. Similarly, one can talk about right associated elements.

If I is an ideal in R, then $I = Ra = bR$ for some $a, b \in R$. Then $a = bu, b = va$ for $u, v \in R$. This implies that $a = vau, b = vbu$. Since $au \in I$, then $au = wa$, for some $w \in R$ and then we get $a = vau = vwa$. So, $1 = vw$ and this gives that v is invertible. Also, similarly one gets that u is invertible as well.

In conclusion a is a left and right generator for I (and so is b). Such an element a with the property that $Ra = aR$ is called a *two-sided generator* in R. So, any left (or right) generator of an ideal I of R is a two-sided generator.

Definition 3.1. Let R be a PID and $a \in R$, nonzero and not a unit.

  (i) We say that a is *irreducible* if it cannot be written as the product of two nonzero, nonunits from R.

 (ii) We say that a is *indecomposable* if R/Ra is indecomposable as a left R-module.

It is easy to see that a is irreducible in R if and only of R/Ra is nonzero simple left R-module.

Definition 3.2. Let $a, b \in R$ nonzero elements. The *greatest left common divisor* of a, b is an element $d \in R$ such that $a = da', b = db'$ and for any other element $d' \in R$ with $a = d'a'', b = d'b''$ there exists $c \in R$ such that $d = d'c$. We denote this element by $(a, b)_l$. In similar fashion one can define the *least common right multiple* of a and b which is denoted by $[a, b]_r$: it is the element m such that $m = xa = yb$ and for any other common right multiple m' of a and b there exists z such that $m' = zm$.

Furthermore, one can define a greatest right common divisor denoted by $(a, b)_r$ and the least left common multiple denoted by $[a, b]_l$.

Proposition 3.3. *Let $a, b \in R$ nonzero. The greatest common left (respectively, right) divisor and the least common right (respectively, left) multiple exist and are nonzero and unique up to multiplication by units on the right (respectively, left).*

An important notion for our purposes is that of similarity. It is defined as follows:

Definition 3.4. Let $a, b \in R$ both nonzero.

We say that a and b are *left (respectively right) similar* if and only if there exists $u \in R$ such that

$$R = Ru + Rb, \quad Rau = Ru \cap Rb,$$

(respectively, $R = uR + bR$, $uaR = uR \cap bR$.)

An important characterization of similarity that explains its relevance is given below.

Proposition 3.5. *Let $a, b \in R$ both nonzero.*

Then a and b are right similar if and only if they are left similar if and only if $R/Ra \simeq R/Rb$ as R-left modules if and only if $R/aR \simeq R/bR$ as R-right modules.

Proof. Assume that a, b are left similar. Then the map $f : R/Ra \to R/Rb$ define by $f(c + Ra) = cu + Rb$ is well-defined and an isomorphism:

Indeed, $c - c' \in Ra$ implies $cu - c'u \in Rau = Ru \cap Rb \subset Rb$, so $cu + Rb = c'u + Rb$. Also, $cu \in Rb$ implies that $cu \in Ru \cap Rb = Rau$ and so $c \in Ra$. Finally, since $1 = ru + sb$ for some $r, s \in R$ and therefore $c = cru + csb$ or $c = cru \in Rb$. Hence $f(cr + Ra) = cru + Rb = c + Rb$.

Now assume that that $f : R/Ra \to R/Rb$ is an isomorphism and let $u \in R$ such that $f(1 + Ra) = u + Rb$. So $f(c + Ra) = c(u + Rb) = cu + Rb$ for all $c \in R$. In particular, $au \in Rb$. So $Rau \subset Ru \cap Rb$. On the other hand, to show that $Ru \cap Rb \subset Rau$, note that if $cu \in Rb$, then $f(c + Ra) = 0$ so $c \in Ra$ because f is injective. This shows that $cu \in Rau$ which is want we wanted.

Finally, since $1 + Rb \in Im(f)$ then there exists $c \in R$ such that $cu + Rb = 1 + Rb$. This immediately shows that $R = Ru + Rb$.

We also know that $au = vb$ for some $v \in R$. We plan to show that $vr \cap aR = vbR$ and $vR + aR = R$ which shows that a, b are right similar.

First let $z \in R$ such that $aR + vR = zR$. Then $a = zr, v = zs$ for some $r, s \in R$. Therefore, $zru = zsb$ so $ru = sb \in Ru \cap Rb = Rau$ which shows that $ru = tau$ or $r = ta = tzr$ and hence $1 = tz$ Therefore $R = zR = vr + aR$.

Let $w \in R$ such that $vR \cap aR = wR$. Then since $au = vb \in aR \cap vR = wR$ we see that $au = vb = ws$ for some $s \in S$. But $w = vr = at$, for some $r, t \in R$. In conclusion, $vb = vrs$, $au = ats$ and so $b = rs$ and $u = ts$. This gives that $R = Rb + Ru \subset Rs$. Hence s is invertible and then, because $vb = ws$, we get that $vbR = wR$. In conclusion, $vR \cap aR = vbR$.

Reversing the roles of left and right we see now that the result follows.   □

Therefore elements that are left (or right) similar will be called similar elements. An application of the Jordan–Hölder theorem gives the following result.

Proposition 3.6. *Let $a \in R$ be a nonzero and not a unit. Then $a = b_1 \cdots b_n$ with b_i irreducible. If $a = c_1 \cdots c_m$ with c_i irreducible, then $m = n$ and the b's and c's may be be paired in similar pairs.*

The number n will be called the length of a and denoted by $\lambda(a)$. It is also equal to the length of a composition series for R/Ra. The following relation can be established.

Proposition 3.7. *For any $a, b \in$ nonzero and nonunits we have that*

$$\lambda(ab) = \lambda([a, b]_r) + \lambda((a, b)_l).$$

Proposition 3.8. *Let $a \in R$ be nonzero and not a unit. Then $a = [b_1, \ldots, b_n]_r$ where each b_i is indecomposable and*

$$(b_i, [b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n]_r)_l = 1.$$

In addition if $a = [c_1, \cdots, c_m]_r$, where each c_i is indecomposable, and

$$(c_i, [c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_m]_r)_l = 1,$$

then $m = n$ and b's and c's can be paired in similar pairs.

Proof. This is an application of the Krull–Schmidt Theorem.   □

Definition 3.9. Let $a, b \in R$. We say that a is a total divisor of b if there is a two-sided ideal I such that $Rb \subseteq I \subseteq Ra$. We will write $a \mid_t b$.

Proposition 3.10 (Teichmüller's condition). *Let $a, b \in R$. Then a is a total divisor of b if and only if $RbR \subseteq Ra \cap aR$.*

Proof. First assume that $RbR \subseteq Ra \cap aR$.

Since $Rb \subseteq RbR \subseteq Ra$ and RbR is a two-sided ideal we conclude that $a \mid_t b$.

Now assume that $a \mid_t b$.

Let I be an ideal generated by x such that $Rb \subseteq I = Rx = xR \subseteq Ra$.

Clearly, $Rb \subseteq xR$ implies that $RbR \subseteq xR \subseteq Ra$.

Let $aR + xR = dR$, so $au + xv = d$ for some $u, v \in R$. Since $x = wa$ for some $w \in R$ we have that

$$wd = wau + wxv = wau + xw'v = wau + waw'v = w(au + aw'v)$$

with $w' \in R$ since $Rx = xR$.

So, $d = au + aw'v$ which implies that $d \in aR$.

But then $I = Rx = xR \subseteq dR \subseteq aR$.

In conclusion $I \subseteq Ra \cap aR$ which implies that $RbR \subseteq Ra \cap aR$. $\square$

Remark 3.11. We would like to observe that total divisibility is invariant under similarity, more precisely, if $a \mid_t b$, a and c are similar, and b and d are similar, then $c \mid_t d$. This is Theorem 14 on page 40 in [26].

Proposition 3.12. *Let R be a PID.*

 (i) *If $I \subset J$ are two-sided ideals, then $I = J \cdot J'$ where J' is a two-sided ideal.*

 (ii) *If I is a proper two-sided ideal then $I = J_1 \cdots J_n$ where each J_i is a two-sided maximal ideal.*

(iii) *Any two maximal two-sided ideals I, J commute, that is $IJ = JI$.*

(iv) *The two-sided ideals form a commutative semigroup under multiplication, and, for any proper two-sided ideal I, the factorization of I into a product of maximal two-sided ideals is unique.*

3.1 Examples in $K\{F\}$

For an element $f \in R = K\{F\}$ the degree of f is in fact equal to $\dim_K(\frac{R}{Rf})$, so the degree of an element of R is an invariant under similarity. Proposition 3.6 shows that the degree of the irreducible elements in the factorization of f depend only on f.

To construct elements similar to f, let $u \in R$ be a unit. Then $Ru = R$ and hence $Ru \cap Rf = Rf$ and $R = Ru + Rf$. Therefore any generator of Rf that can be written in the form gu will provide an element $g \in R$ similar to f. But a generator for Rf is of the form vf with v unit, and so $vf = gu$ or $g = vfu^{-1}$. In conclusion an element of the form vfw with v, w units in R is similar to f.

For a concrete example let us take $f = F^n - \lambda$ with $\lambda \in K$. For $w, u \in K$ and nonzero we get that $g = vw^{p^n} F^n - vw\lambda$ is similar to f. Hence, $g = F^n - w^{-p^n + 1}\lambda$

are monic polynomials that are similar to f. This example shows that similar elements do not generate necessarily the same left (or right) ideals.

Proposition 3.13. *Let K be a perfect field.*

(i) *Assume that $K = \mathbb{F}_{p^k}$. Let $f = \sum_{i=0}^n a_i F^i$ with $0 \neq a_n \in K$. Let $\mathrm{Supp}(f) = \{i : a_i \neq 0\}$. Then f is a two-sided generator if and only if k divides $\gcd(j - i : i \leq j$ with $i, j \in \mathrm{Supp}(f))$ (naturally, if $\mathrm{Supp}(f)$ has one element, we assume that the condition is empty).*

(ii) *Assume that K is not finite. Then every ideal I is generated by F^n for some $n \geq 0$.*

Proof. (i) If $I = Rf = fR$, then by degree considerations we have that for all $a \in K$, there exists $b \in K$ such that $af = fb$. In fact, since F^n generates an ideal for any n, as can easily be checked, this condition is in fact necessary and sufficient for f to satisfy $Rf = fR$.

The equality $af = fb$ implies that for all $i = 0, \ldots, n$

$$aa_i = a_i b^{p^i},$$

which in turn is equivalent to

$$a = b^{p^i}$$

for all $i \in \mathrm{Supp}(f)$ which, in conjunction with K perfect, says that $b^{p^i} = b^{p^j}$ for all $b \in K$ and $i \leq j$ with $i, j \in \mathrm{Supp}(f)$.

This is indeed equivalent to $c = c^{p^{j-i}}$, for all $c \in K$ and $i \leq j$ with $i, j \in \mathrm{Supp}(f)$. Since $K = \mathbb{F}_{p^k}$ we get that $\mathbb{F}_{p^k} \subseteq \mathbb{F}_{p^{j-i}}$, that is, $k \mid j - i$, for all $i \leq j$ with $i, j \in \mathrm{Supp}(f)$.

(ii) When K is not finite, the proof above shows that the only possibility is that

$$|\mathrm{Supp}(f)| = 1,$$

which represents the claim. $\square$

Remark 3.14. Let $K = \mathbb{F}_{p^k}$. For degree n polynomials $f = \sum_{i=0}^n a_i F^i$ with $a_0 \neq 0$, the condition in Proposition 3.13 is equivalent to $k \mid i$ for all $i \in \mathrm{Supp}(f)$. Therefore, any two-sided generator $f \in K\{F\}$ is a product between a power of F and a polynomial with nonzero constant coefficient and only nonzero degrees divisible by k in its support.

Example 3.15. Let $K = \mathbb{F}_{p^2}$. Then $f = F^6 + F^4 - F^2 - 1$ is a two-sided generator for $R = K\{F\}$ according to the above Proposition.

Proposition 3.16. *Let $a, b \in R = K\{F\}$ such that $a \mid_t b$. Assume that K is perfect, not finite. Then $a = uF^k$ where $k \geq 0$ and $u \in K$.*

Proof. Since $a \mid_t b$, there exists an ideal I of R such that $I \subseteq Ra$. But K is not finite so by Proposition 3.13 we get that I is generated by F^l for some $l \geq 0$.

Therefore $F^l = ra$ with $r \in R$.

It is clear that F is irreducible in $R = K\{F\}$ so by the unique factorization theorem one has that $a = uF^k$ where $k \geq 0$. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Example 3.17. Over a finite field, there exist many interesting examples of pairs $a, b \in K\{F\}$ such that $a \mid_t b$. For example let $K = \mathbb{F}_{p^2}$ and let $a = F^3 + F^2 + F + 1$ and $b = F^7 + F^6 + F^5 + F^4 - F^3 - F^2 - F - 1$. According to the Proposition 3.13 neither a nor b are two-sided generators in R.

However $b = (F + 1)(F^6 + F^4 - F^2 - 1)$ and

$$F^6 + F^4 - F^2 - 1 = (F^3 - F^2 + F - 1)(F^3 + F^2 + F + 1).$$

As seen earlier, $F^6 + F^4 - F^2 - 1$ is a two-sided generator, so $a \mid_t b$.

4 Matrix Transformations over Noncommutative PIDs

In this section we are considering matrices with entires in a noncommutative PID R. The collection of $n \times m$ matrices with entries in R will be denoted by $M_{n,m}(R)$.

First we would like to note that a noncommutative PID R can be embedded in a division ring Q as follows: consider pairs of the form $(a, b) \in R \times R \setminus \{0\}$ and let $(a, b) \equiv (c, d)$ if $[b, d]_r = bb_1 = dd_1$ implies $ab_1 = cd_1$. This defines an equivalence relation and the equivalence class of a pair (a, b) will be denoted by a/b.

The addition of two classes is defined by $a/b + c/d = (ab_1 + cd_1)/m$ where b_1, d_1 are such that $[b, d]_r = bb_1 = dd_1$. The multiplication is defined as follows: $(a/b) \cdot (c/d) = (ab_2)/(dc_2)$ if $c \neq 0, [b, c]_r = bb_2 = cc_2$. If $c = 0$, we simply put $(a/b) \cdot (0/d) = 0/d$. It is well known that Q defined in this fashion is a division ring and that R can be naturally embedded in Q.

Since R can be embedded in a division ring then for two $n \times n$ matrices U, V with entries in R such that $UV = 1$ we see that $VU = 1$ as well.

Let A, B be two $n \times r$ matrices with entries in R. We say that A, B are *associates* if $B = UAV$ where U, V are invertible matrices in $M_{n,n}(R)$, respectively $M_{r,r}(R)$.

Let E_{ij} denote the square matrix that has 1 on the main diagonal and the position (i, j), and zero for the rest.

The following represents a list of elementary transformations for a given matrix $A \in M_{n,r}(R)$:

 (i) Adding to the ith column the jth column of the matrix A multiplied on the right by q. Similarly, adding to the ith row the jth row of the matrix A multiplied on the left by q. The operations are $A(1 + E_{ji}q)$, respectively $(1 + E_{ij}q)A$.

(ii) Interchanging the ith and the jth rows (columns) of A. This corresponds to $A(1 + E_{ij} + E_{ji} - E_{ii} - E_{jj})$, respectively $(1 + E_{ij} + E_{ji} - E_{ii} - E_{jj})A$.

(iii) Multiplying the ith column (row) on the right (left) by a unit u. This corresponds to $A(1 + (u - 1)E_{ii})$, respectively $(1 + (u - 1)E_{ii})A$.

In addition to these transformations, given a matrix A with row

$$(c_1, \ldots, c_{i-1}, a, c_{i+1}, \ldots, c_{j-1}, b, c_{j+1}, \ldots, c_n)$$

there is a matrix associated to A of the form AV where V is invertible with row i equal to

$$(c_1, \ldots, c_{i-1}, d, c_{i+1}, \ldots, c_{j-1}, 0, c_{j+1}, \ldots, c_n),$$

where $d = (a, b)_l$. A similar statement holds for the columns of A with the new matrix of the form UA where U is invertible. Such transformation will be called special transformations.

We sketch here the construction of the matrix V that can be used in a special transformation. Since $(a, b)_l = d$ one can find $p, q, r, s \in R$ such that $pa + qb = d$ and $ra + sb = 0$ and $Rr + Rs = R$. The it can be checked that the matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

is invertible. Finally the matrix $U = (u_{ij})_{1 \le i, j \le n}$ has the following entries: $u_{hh} = 1$ for $h \ne i, j$, $u_{ii} = p$, $u_{jj} = s$, $u_{ij} = r$, $u_{ji} = q$ and the rest of the entries are zero.

Repeated application of elementary and special transformations leads to the following:

Theorem 4.1. *Any matrix* $A \in M_{n,r}(R)$ *has an associate with nonzero elements* $d_1, d_2, \ldots, d_s$ *on the main diagonal only such that* $s \le \min(n, r)$ *and* d_i *is a total divisor of* d_j *for* $i < j$:

$$\begin{pmatrix} d_1 & 0 & \cdots \\ 0 & d_2 & \ddots \\ \vdots & \ddots & \ddots \end{pmatrix}.$$

Proof. We will sketch here the procedure that gives an associate of A as in the conclusion of the theorem. The idea is to use elementary transformations and therefore arrange that A is associated to a matrix that has in the upper left corner a nonzero element of smallest length. If this element a_{11} is not a left factor of any of the a_{1i} (or a right factor of any of the a_{j1}) then after elementary transformations one can replace a_{11} by an element of smaller length. After a finite number of elementary transformations, we therefore obtain an element in the upper left corner that is a left factor (respectively, right factor) of any element in the first row (respectively, first column).

One can perform repeated elementary transformations to obtain an associated matrix to A that has a nonzero entry in the upper left corner and zeros on the rest of the entries on the first row and first column. Continuing like this we produce an associated matrix to A that has only nonzero entries on the diagonal, say $d_1, d_2, \ldots, d_s$.

Let us show that we may assume that $d_i \mid_t d_j$ for all $i < j$. In the case that there exists $b \neq 0$ such that d_i is not a left factor of d_j, go ahead and rename $i = 1$, $j = 2$ for simplicity. The upper left corner of the matrix is of the form

$$\begin{pmatrix} d_1 & bd_2 \\ 0 & d_2 \end{pmatrix}$$

after an elementary transformation. The highest left factor of d_1 and bd_2 has length less that the length of d_1. We can repeat the diagonalization process to obtain an associated matrix with an upper left corner entry of length smaller than the length of d_1. Repeated application of this process produces an associated diagonal matrix where d_i is a left factor for all bd_j for all nonzero b and all $i < j$. But then obviously $Rd_j \subset Rd_jR \subset d_iR$ which shows that $d_i \mid_t d_j$. $\qquad\square$

5 Module Theory over Noncommutative PIDs

Any cyclic R-module M is isomorphic to R/Ra where $a \in R$. If $M = Rm$, then $Ra = \mathrm{Ann}_R(m) = \{r \in R : rm = 0\}$. We call the element m *torsion* if $\mathrm{Ann}_R(m) \neq 0$. Since in this case $\mathrm{Ann}_R(m) = R\mu$ for some $0 \neq \mu \in R$ we say that μ is the *order* of m and denoted by $\mathrm{ord}(m)$. Any two orders of m are left associated.

Let M be an R-module. It can be checked that $T(M) = \{m \in M : \mathrm{ord}(m) \neq 0\}$ is a submodule of M. The reader that has difficulty verifying this statement will find helpful the observation that the intersection of two left nonzero ideals is a nonzero left ideal. As always, if $M = T(M)$ we say that M is a *torsion* R-module.

The following result follows from the Krull–Schmidt Theorem for modules (p. 115 in [27]).

Proposition 5.1. *Let M be an R-module that satisfies the* (ACC) *and* (DCC) *conditions on its left submodules. Then*

$$M \simeq I_1 \oplus \cdots \oplus I_k,$$

where I_l are indecomposable R-modules for all $l = 1, \ldots, k$. For any other similar decomposition into indecomposable R-modules

$$M \simeq L_1 \oplus \cdots \oplus L_h,$$

we have $k = h$ and, up to renumbering, $I_l \simeq L_l$ for all $l = 1, \ldots, k$.

In what follows we will need some basic considerations on linear maps of free modules over a ring R and matrices with entries in R. We will of course use this in the noncommutative setting, so we will review these facts in this case as many basic books discuss them only in the special commutative case.

Let $\phi : R^m \to R^n$ be an R-linear map. Fix $u_1, \ldots, u_m$ and $v_1, \ldots, v_n$ be bases of R^m, respectively R^n, and write $\phi(u_i) = \sum_{j=1}^n a_{ij} v_j$ for all $i = 1, \ldots, m$. Then if $r = \sum_{i=1}^m r_i u_i$, then $\phi(r) = \sum_{i=1}^m r_i \phi(u_i) = \sum_{j=1}^n \sum_{i=1}^m (r_i a_{ij}) v_j$. If we set $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq m}$, the map ϕ can be described by

$$(r_1, \ldots, r_n) \longmapsto (r_1, \ldots, r_n) A.$$

A simple check establishes the existence of a group isomorphism

$$\Theta : (\mathrm{Hom}_R(R^m, R^n), +) \longrightarrow (M_{m,n}(R), +)$$

given by

$$\phi \longmapsto A.$$

Obviously, the map $\Theta = \Theta_{u,v}(\phi)$ depends on the bases $u = \{u_1, \ldots, u_m\}$ and $v = \{v_1, \ldots, v_n\}$, and we will not indicate the chosen bases, when the choice is clear from the context. The construction of a well-defined $\Theta_{u,v}(\phi)$ requires that v is a basis for R^n, while u only needs to be a set of generators for R^m.

Now consider another R-linear map $\psi : R^n \to R^h$ and let $w_1, \ldots, w_h$ be a basis for R^h. Let $\psi(v_j) = \sum_{l=1}^h b_{jl} w_l$, for all $j = 1, \ldots, n$. Therefore

$$
\begin{aligned}
(\psi \circ \phi)(r) &= \sum_{i=1}^m r_i (\psi \circ \phi)(u_i) \\
&= \sum_{i=1}^m r_i \psi \left(\sum_{j=1}^n a_{ij} v_j \right) \\
&= \sum_{i=1}^m r_i \sum_{j=1}^n a_{ij} \psi(v_j) \\
&= \sum_{i=1}^m r_i \left(\sum_{j=1}^n a_{ij} b_{jl} \right) w_l.
\end{aligned}
$$

This computation shows that

$$\Theta_{u,w}(\psi \circ \phi) = AB = \Theta_{u,v}(\phi) \cdot \Theta_{v,w}(\psi).$$

Now consider two bases for R^n, $e = \{e_1, \ldots, e_n\}$ and $f = \{f_1, \ldots, f_n\}$. Write $e_i = \sum_{j=1}^n t_{ij} f_j$ and denote $T = (t_{ij})_{1 \leq i, j \leq n}$, an $n \times n$-matrix with entries from R, referred to as the transition matrix between bases.

This can be written in matrix form as

$$e = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = T \cdot \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} = T \cdot f.$$

It is clear that $\Theta_{e,f}(1_{R^n}) = T$. Similarly we can write $f = S \cdot e$ where S is an $n \times n$-matrix with entries in R. In particular, $I_n = \Theta_{e,e}(1_{R^n}) = \Theta_{e,f}(1_{R^n}) \cdot \Theta_{f,e}(1_{R^n}) = TS$. Similarly, $ST = I_n$.

Now let $\phi : R^m \to R^n$ and we fix bases $u = \{u_1, \ldots, u_m\}$ and $v = \{v_1, \ldots, v_n\}$. Assume that $u' = \{u'_1, \ldots, u'_m\}$ and $v' = \{v'_1, \ldots, v'_n\}$ are bases for R^m and R^n and let C, D be the transition matrices such that $u' = Cu, v' = Dv$. Note that $\Theta_{u',u}(1_{R^m}) = C$ and $\Theta_{v,v'}(1_{R^n}) = D^{-1}$.

Then $\Theta_{u',v}(\phi) = \Theta_{u',v}(1_{R^m}\phi) = \Theta_{u',u}(1_{R^m})\Theta_{u,v}(\phi) = C\Theta_{u,v}(\phi)$, and, similarly, $\Theta_{u,v}(\phi) = \Theta_{u,v'}(\phi)D$.

Using this, we can see that $\Theta_{u',v'}(\phi) = C\Theta_{u,v}(\phi)D^{-1}$.

The following two results have proofs similar to their well-known counterparts in the commutative case and are not included below (see Theorems 17 and 18 in [26]).

Theorem 5.2. *Let G be a free R-module that admits a basis with n elements and $N \subset G$ a submodule. Then N is also free and there exists a basis of N with $m \leq n$ elements.*

Theorem 5.3. *Let M be a finitely generated R-module. Then there exists a finite rank free submodule G of M such that*

$$M = T(M) \oplus G.$$

Theorem 5.4. *If M is a finitely generated torsion R-module, then there exist nonzero elements $f_1, \ldots, f_n$ in R such that f_i is a total divisor of f_{i+1} for all $i = 1, \ldots, n-1$ and*

$$M \simeq \frac{R}{Rf_1} \oplus \cdots \oplus \frac{R}{Rf_n}.$$

Proof. Since M is finitely generated over R we can map a free R-module onto M via an R-module homomorphism ϕ, $\phi : R^n \to M \to 0$. Let $N = \text{Ker}(\phi)$. According to Theorem 5.2, N admits a basis $f_1, \ldots, f_m$ with m elements, where $m \leq n$. Denote $e = \{e_1, \ldots, e_n\}$ the standard basis in R^n.

Therefore $M = \text{Coker}(i : N \hookrightarrow R^n)$. Let $\Theta(i) = A$ and note that according to our earlier observations, a change of bases for N and R^n to say f', respectively e' produces a new matrix $\Theta_{f',e'}(i)$ that is associate of A.

Therefore we can apply the matrix considerations from an earlier section and con-
clude that for an appropriate choice of bases for N and R^n we have

$$\Theta(i) = \begin{pmatrix} f_1 & 0 & \cdots \\ 0 & f_2 & \ddots \\ \vdots & \ddots & \ddots \end{pmatrix}$$

with f_i is a total divisor for f_j for all $j > i$. Let s the number of nonzero f_i's. Clearly
$s \leq n$. Since $\operatorname{Coker}(\Theta(i)) = R/Rf_1 \oplus R/Rf_2 \oplus \cdots \oplus R/Rf_s \oplus R^{n-s}$, we can
conclude that $s = n$ since otherwise M has nontorsion elements. The statement of the
theorem is now clear. $\square$

Corollary 5.5. (i) *Let M be a finitely generated indecomposable R-module. Then
    M is cyclic.*

 (ii) *Any R-module M that satisfies the (ACC) and (DCC) conditions on its left sub-
    modules is a direct sum of cyclic indecomposable R-modules of the form R/Rm,
    $m \in R$. The elements m that appear in the decomposition are determined up to
    similarity and their number is an invariant of the module M.*

(iii) *If M is finitely generated R-torsion module, then there exist n and nonzero
    $e_1, \ldots, e_n$ such that for all $i = 1, \ldots, n$, R/Re_i is indecomposable and*

$$M \simeq R/Re_1 \oplus \cdots \oplus R/Re_n.$$

*The number n is uniquely determined by M and the elements $e_1, \ldots, e_n \in R$ are
    determined up to similarity.*

The elements in the above Corollary are called *elementary divisors* of M, in the case
M is R-torsion and finitely generated. In the general case when M is finitely gener-
ated, but not necessarily R-torsion, the elementary divisors of M are by definition the
elementary divisors of $T(M)$.

6 Computing the Invariant Factors

Let $F : V \to V$ be a Frobenius action on V. Let $\{v_1, \ldots, v_n\}$ denote a basis for V
and write

$$F(v_i) = \sum_{j=1}^{n} a_{ij} v_j, \quad i = 1, \ldots, n, \ a_{ij} \in K.$$

Therefore

$$F\left(\sum_{i=1}^{n} x_i v_i\right) = \sum_{i=1}^{n} x_i^p F(v_i) = \sum_{i=1}^{n} x_i^p \sum_{j=1}^{n} a_{ij} v_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x_i^p a_{ij}\right) v_j.$$

If we write $(x_1, \ldots, x_n)$ for $\sum_{j=1}^{n} x_j v_j$ and $A = (a_{ij})_{1 \leq i,j \leq n}$ then the above equation can be summarized as

$$F(x_1, \ldots, x_n) = (x_1^p, \ldots, x_n^p) \cdot A$$

The $R = K\{F\}$-structure on V is defined by $F \cdot v = F(v)$. So given a fixed basis $\{v_1, \ldots, v_n\}$ of V, the action F is determined by the matrix A and vice versa. We would like to outline the computation of the invariant factors of V as an R-module from the matrix A.

Note that we can define a R-module homomorphism $\phi : R^n \to V$ by letting $\phi(e_i) = v_i$ where $e = \{e_1, \ldots, e_n\}$ form a basis for R^n. This is obviously a surjection since V is generated over K and hence over $K\{F\}$ by $v_1, \ldots, v_n$.

Let us notice that V is torsion over R. Indeed, since $\dim_K(V) < \infty$, for any $v \in V$, there exists n such that $v, F(v), \ldots, F^n(v)$ are K-linearly dependent and so there exist $a_0, \ldots, a_n$ in K, not all zero, such that $a_0 v + a_1 F(v) + \cdots + a_n F^n(v) = 0$. One can assume that $a_n \neq 0$ and note that this implies that $(a_0 + a_1 F + \cdots + a_n F^n) \cdot v = 0$. In conclusion, Theorem 5.4 can be applied.

Theorem 6.1. *Let V be a K-vector space with basis $\{v_1, \ldots, v_n\}$. Assume that V admits a Frobenius action F over K and let A be the matrix associated to this action with respect to the chosen basis.*

Consider the natural R-homomorphism $\phi : R^n \to V$ sending each element e_i of the basis to v_i for all $i = 1, \ldots, n$. Then a basis for $W = \mathrm{Ker}(\phi)$ is given by the set of vectors

$$(F I_n - A) \cdot \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

(interpreted as a matrix multiplication).

Proof. Let

$$\begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix} = (F \cdot 1_n - A) \cdot \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix},$$

therefore

$$f_i = F \cdot e_i - \sum_{j=1}^{n} a_{ij} e_j.$$

Note that $\phi(f_i) = F\phi(e_i) - \sum_{j=1}^{n} a_{ij} \phi(e_j) = F(v_i) - \sum_{j=1}^{n} a_{ij} v_j = 0$ which shows that each f_i belongs to W.

To prove that $f_1, \ldots, f_n$ generate W let us denote by W' the R-submodule generated by these elements. The goal is to check that $W' = W$. Consider the K-subspace of R^n, E, generated by $e_1, \ldots, e_n$. Clearly, $F \cdot e_i = f_i + \sum_{j=1}^n a_{ij} e_j$ and so belongs to $W' + E$. Using this fact, we can immediately check that $W' + E$ is an R-submodule of R^n. Now, it contains all $e_1, \ldots, e_n$ so it must equal R^n. Let $w \in W \subset R^n$ and write $w = w' + e$ with $w' = \sum_{i=1}^n r_i f_i$ and $e = \sum_{i=1}^n a_i e_i$ where each $r_i \in R$ and $a_i \in K$. But $\phi(w) = 0$. We already know that $\phi(w') = 0$, so we obtain $\phi(e) = 0$ which leads to $\sum_{i=1}^n a_i \phi(e_i) = \sum_{i=1}^n a_i v_i = 0$ therefore $a_i = 0$ for all $i = 1, \ldots, n$. Hence $w = w' \in W'$ and the equality $W' = W$ is verified.

To check that $f_1, \ldots, f_n$ are linearly independent over R let us consider $r_1, \ldots, r_n \in R$ such that

$$r_1 f_1 + r_2 f_2 + \cdots + r_n f_n = 0.$$

Now each nonzero r_i has a leading term of the form $a_{n_i} F^{n_i}$ with $a_{n_i} \in K, a_{n_i} \neq 0$. Consider the above relation in the highest degree for which F appears on the left hand side, and note that it leads to a relation of the form $\sum_i a_{n_i} e_i = 0$, where the sum runs over a nonempty subset of the set of indices i such that $r_i \neq 0$. But $e_1, \ldots, e_n$ are linearly independent over K, so in fact we must have $r_i = 0$ for all i. □

Corollary 6.2. *Let V be a K-vector space with basis $\{v_1, \ldots, v_n\}$. Assume that V admits a Frobenius action F over K and let A be the matrix associated to this action with respect to the chosen basis.*

Then the invariant factors of V as an R-module are the invariant factors of $F \cdot 1_n - A$.

Proof. Construct a surjection $\phi : R^n \to V$ by mapping the elements of a basis $e = \{e_1, \ldots, e_n\}$ to V by $\phi(e_i) = v_i$. Let $W = \mathrm{Ker}(\phi)$.

In the proof of Theorem 5.4 the invariant factors of V are obtained as the invariant factors of the matrix $\Theta(i)$ where $i : W \to V$ is the natural inclusion.

With the notations from Theorem 6.1, we have that $f = \{f_1, \ldots, f_n\}$ is basis of W. But $f_i = F \cdot e_i - \sum_{j=1}^n a_{ij} e_j$ and so $\Theta_{f,e}(i) = F \cdot 1_n - A$. □

Let us present a example.

Example 6.3. Let K be a field of characteristic $p > 2$, $V = K^2$ and denote $v_1 = (1, 0), v_2 = (0, 1)$ for the canonical basis for V.

Let $A = \left(\begin{smallmatrix} 1 & 0 \\ -2 & 0 \end{smallmatrix}\right)$ and define a Frobenius action on V such that its matrix with respect to the chosen basis equals A, that is $F(v_1) = v_1, F(v_2) = -2v_1$.

For arbitrary $(x, y) \in V$, we have $F(x, y) = (x^p, y^p) \cdot \left(\begin{smallmatrix} 1 & 0 \\ -2 & 0 \end{smallmatrix}\right) = (x^p - 2y^p, 0)$.

Consider now

$$F \cdot I_n - A = \begin{pmatrix} F - 1 & 0 \\ 2 & F \end{pmatrix}.$$

We will perform the elementary and special transformations described in Section 4 in order to compute the invariant factors. An important feature is that we can multiply

a rown on the left and add to another row, and we can multiply a column on the right and add it to another column as described in Section 5. The rows will be denoted by R_1, R_2 and columns by C_1, C_2 and the transformations will be described as follows: $R_1' = R_1 + aR_2$ means for example that the we replace the old row R_1 by a new one obtained by first multiplying row R_2 on the left by a and then adding it to row R_1. Therefore

$$\begin{pmatrix} F-1 & 0 \\ 2 & F \end{pmatrix} \underset{\sim}{\overset{R_1'=(-1/2^p)FR_2+R_1}{}} \begin{pmatrix} -1 & (-1/2^p)F^2 \\ 2 & F \end{pmatrix}$$

and

$$\begin{pmatrix} -1 & (-1/2^p)F^2 \\ 2 & F \end{pmatrix} \underset{\sim}{\overset{R_2'=2R_1+R_2}{}} \begin{pmatrix} -1 & (-1/2^p)F^2 \\ 0 & F-(2/2^p)F^2 \end{pmatrix}$$

Continuing like this we obtain

$$\begin{pmatrix} -1 & (-1/2^p)F^2 \\ 0 & F-(2/2^p)F^2 \end{pmatrix} \underset{\sim}{\overset{C_2'=C_1(-1/2^p)F^2+C_2}{}} \begin{pmatrix} -1 & 0 \\ 0 & F-(2/2^p)F^2 \end{pmatrix}$$

and further

$$\begin{pmatrix} -1 & 0 \\ 0 & F-(2/2^p)F^2 \end{pmatrix} \sim \begin{pmatrix} (1/2^{p-1})F^2-F & 0 \\ 0 & 1 \end{pmatrix}$$

Therefore V is R-isomorphic to

$$\frac{R}{((1/2^{p-1})F^2 - F)R},$$

and we can understand better the action of F on V by inspecting the elementary transformations performed on $F \cdot I_n - A$.

These elementary transformations correspond to multiplying $F \cdot I_n - A$ on the left by

$$X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & (-1/2^p)F \\ 0 & 1 \end{pmatrix}$$

and on the right by

$$Y = \begin{pmatrix} 1 & (-1/2^p)F^2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

But

$$X = \begin{pmatrix} 2 & (-1/2^{p-1})F+1 \\ -1 & (1/2^p)F \end{pmatrix}$$

while

$$Y = \begin{pmatrix} (1/2^p)F^2 & 1 \\ -1 & 0 \end{pmatrix}.$$

We know that $V = \operatorname{Coker}(i)$ where $i : W \to R^2$, and as in the proof of Theorem 5.4 the matrix

$$\begin{pmatrix} (1/2^{p-1})F^2 - F & 0 \\ 0 & 1 \end{pmatrix}$$

is the matrix of the map i with respect to the basis $X \cdot f$ for W and the basis $Y^{-1} \cdot e$ for R^2.

Now the

$$Y^{-1} \cdot e = \begin{pmatrix} 0 & -1 \\ 1 & (1/2^p)F^2 \end{pmatrix} \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} -e_2 \\ e_1 + (1/2^p)F^2 e_2 \end{pmatrix}.$$

Under the isomorphism

$$\frac{R}{((1/2^{p-1})F^2 - F)R} \simeq V$$

the class of the element 1 on the left corresponds to the image of the class of $-e_2$ in $V = \operatorname{Coker}(i)$ on the right therefore. So 1 corrresponds to $-v_2$.

Note that $\frac{R}{((1/2^{p-1})F^2 - F)R}$ has K-basis $w_1 = 1, w_2 = F$. The reader might want to know what basis of V this is. Our above calculations have shown that 1 corresponds to $-v_2$ and, of course, F will correspond to $F(-v_2) = (-1)^p F(v_2) = -(-2v_1) = 2v_1$.

In particular we obtain that V is R-generated by $-v_2$ and $\operatorname{Ann}_R(-v_2) = (F^2 - 2^{p-1}F)$.

6.1 Injective Frobenius Actions on Finite Dimensional Vector Spaces over a Perfect Field

In the study of modules with Frobenius action the case when the action is injective plays an especially important role.

Proposition 6.4. *Let K be a perfect field and V be a finitely dimensional vector space with a Frobenius action F. Fix a basis for V say $v = \{v_1, \ldots, v_n\}$ and denote by A the matrix associated to F. Then F is injective if and only if A is invertible in $M_n(K)$.*

Proof. The proof is a simple exercise.   □

The following theorem, that we could not find in the literature, is a simple consequence to the theory developed so far.

Theorem 6.5. *Let K be an infinite perfect field and V be a finitely dimensional K-vector space. Assume that V admits an injective Frobenius action. Then V is R-cyclic.*

Proof. We have noted earlier that V is necessarily a torsion R-module. Therefore V is R-isomorphic to a direct sum of the form $\oplus_{i=1}^{s} R/Rf_i$, where $f_1, \ldots, f_s$ are the invariant factors of V regarded as an R-module.

The invariant factors $f_1, \ldots, f_s$ have the property $f_i \mid_t f_{i+1}$, $i = 1, \ldots, s-1$. This implies that there exist ideals I_i such that $Rf_i \subset I \subset Rf_{i+1}$. However, ideals in R are of the form (F^k) for some k by Proposition 3.13. So let $I_i = (F^{k_i})$ for all $i = 1, \ldots, s-1$. Since $F^{k_i} \in Rf_{i+1}$, and f_{i+1} kills a nonzero element of V as can be readily seen from the R-structure of V, we see that F^{k_i} kills a nonzero element of V. But F is an injective action on V so we conclude that $f_i = 0$ for all $i \geq 2$ which leads to the conclusion of the theorem. $\qquad\square$

We can use this theorem to give a proof of a result of Dieudonné. This result is well-known and has appeared in many texts.

Theorem 6.6 (Dieudonné). *Let K be an algebraically closed field and V a finite dimensional K-vector space with an injective Frobenius action $F_K : V \to V$. Then V admits a K-basis which is fixed under F.*

We will give an extension here that is suited to our point of view and it has been known to the experts. For example, the reader might consult [4] (Section 3.6.1) for a nice proof that has some similarities with the one below.

Theorem 6.7. *Let K be a perfect field and V a finite dimensional K-vector space with an injective Frobenius action $F_K : V \to V$. Then there exists a finite field extension $K \subset L$ such that the Frobenius action on $V_L = L \otimes_K V$ given by*

$$F_L : V_L \to V_L, \quad F_L = 1_L \otimes F_K$$

admits an L-basis which is fixed under F_L.

Proof. According to Theorem 6.5 we know that $V = R/Rf$ where $f \in R = K\{F\}$. We can assume that $f = F^n - \sum_{i=1}^{n} \lambda_i F^{i-1}$, with $\lambda_1 \neq 0$ because F acts injectively on V.

Let us fix the following basis of V: $v_i = F^{i-1}$, $i = 1, \ldots, n$. With respect to this basis the matrix of the Frobenius action is given by

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \cdots & \lambda_n \end{pmatrix}.$$

If $v = x_1 v_1 + \cdots + x_n v_n$, then $F(v) = v$ leads to the following system of equations

$$x_i^p + x_n^p \lambda_{i+1} = x_{i+1}, \quad i = 0, \ldots, n-1, \quad x_0 = 0.$$

Substituting recursively we obtain $\sum_{i=1}^{n} x_n^{p^{n-i+1}} \lambda_i^{p^{n-i}} - x_n = 0$ which is a polynomial over K admitting distinct roots, because its derivative is invertible. Call these roots $x_{1,n}, x_{2,n}, \ldots, x_{p^n,n}$. Adjoining these solutions to K we get a finite field extension L of K.

Once $x_n = x_{k,n}$ is obtained we see that the corresponding $x_1, \ldots, x_{n-1}$ can be calculated immediately with $x_j = x_{k,j} = \sum_{i=1}^{j} x_{k,n}^{p^{n-i+1}} \lambda_i^{p^{n-i}}$.

We claim that for n distinct nonzero choices of $x_{k,n}$, $k = 1, \ldots, n$, the elements of V_L given by

$$w_j = x_{j,1}v_1 + \cdots + x_{j,n}v_n$$

with $j = 1, \ldots, n$ form a basis for V_L. It is clear that $F_L(w_j) = w_j$.

The transition matrix from basis $v_1, \ldots, v_n$ to basis $w_1, \ldots, w_n$ has kth row equal to

$$\left(x_{k,n}^{p} \lambda_1, \ \ldots, \ \sum_{i=1}^{j} x_{k,n}^{p^{n-i+1}} \lambda_i^{p^{n-i}}, \ \ldots \right).$$

We need to show that this matrix has nonzero determinant. Since $\lambda_1 \neq 0$, we can in fact assume $\lambda_1 = 1$, and now simple column operations show that the determinant of the transition matrix is a Vandermonde determinant in the nonzero distinct elements $x_{1,n}, \ldots, x_{n,n}$, which is therefore different from zero. $\square$

Definition 6.8. Let V be a K-vector space with a Frobenius action. For a subset S of V, $\langle S \rangle_K$ denotes the K-subspace of V generated by the elements of S. Then the *stable part* of V is the subspace $V_s = \bigcap_{e \geq 0} \langle F^e(V) \rangle_K$. The *nilpotent part* of V is the subspace $V_{\text{nil}} = \{v \in V : F^e(v) = 0 \text{ for some } e \geq 0\}$. It is clear that both V_s and V_{nil} inherit the Frobenius action from V. Also, V is called *semisimple* if $\langle F(V) \rangle_K = V$. Therefore V_s is semisimple.

Proposition 6.9. *Let K be perfect field. Let V be a K-vector space with a Frobenius action. Then $V = V_s \oplus V_{\text{nil}}$.*

Proof. Since K is perfect then $\langle F^e(V) \rangle_K = F^e(V)$ for all $e \geq 0$. There exists $e_0 \geq 0$ such that $V_s = F^e(V)$ for all $e \geq e_0$. Also since V_{nil} is finite dimensional we can find $m \geq 0$ such that $F^m(V_{\text{nil}}) = 0$. One can assume $m \geq e_0$.

Let $v \in V_s \cap V_{\text{nil}}$. Then $v = F^m(w)$ for some $w \in V$. So, $0 = F^m(v) = F^{2m}(w)$ hence $w \in V_{\text{nil}}$. But this gives $F^m(w) = 0$, or $v = 0$. Therefore, $V_s \cap V_{\text{nil}} = 0$.

Now, let $v \in V$. Since $F^m(v) \in V_s$ then $F^m(v) = F^{m+e_0}(w)$ for some $w \in V$. So, $F^m(v - F^{e_0}(w)) = 0$ or in other words $v - F^{e_0}(w) \in V_{\text{nil}}$.

Now note that $v = v - F^{e_0}(w) + F^{e_0}(w)$ and that $F^{e_0}(w) \in F^{e_0}(V) = V_s$. $\square$

The following result has appeared first in [19], based on ideas of Lang, and then Hochster gave another proof more recently, see [17]. It extends Dieudonné's result, Theorem 6.6, in a complementary way to Theorem 6.7.

Theorem 6.10. *Let V be a K-vector space and K a separably closed field. Then V_s admits a basis that is fixed by F.*

7 The Antinilpotent Case

In this section we will present some applications to the case of antinilpotent vector spaces. The notion of an antinilpotent module was introduced in [13] with respect to modules that admit a Frobenius action. It has applications in the study of local cohomology modules of a local ring A with support in its maximal ideal. These local cohomology modules are Artinian, but not finitely generated. However, to understand the notion of antinilpotency it is natural to first consider it in the context of simpler situations, such as finite dimensional vector spaces, and finitely generated modules over a commutative Noetherian ring. The treatment of vector spaces with Frobenius action which is the subject of the paper will be applied in this section.

We will first start with reviewing the antinilpotency of modules. In this section, A denotes a commutative Noetherian ring of positive characteristic p where p is prime. Let M be an A-module and assume that there exist an additive map $F = F_M : M \to M$ such that $F(am) = a^p F(m)$ for all $a \in A, m \in M$. We call $F = F_M$ a Frobenius action on M.

Definition 7.1. Let M be an A-module that admits a Frobenius action $F : M \to M$. We say that M is *antinilpotent* (with respect to F) if for any F-compatible (or F-invariant) submodule N the induced map $F : M/N \to M/N$ is injective. This is equivalent to the condition that F does not act nilpotently on (equivalently, does not kill) any nonzero subquotient Q/N of F-compatible submodules Q, N of M.

Let $S \subset A$ be a multiplicative set and M be an A-module with a Frobenius action. Then F extends naturally to a Frobenius action on $S^{-1}M$ by $F(\frac{m}{s}) = \frac{F(m)}{s^p}$ for all $m \in M, s \in S$. If M is antinilpotent, then $S^{-1}M$ is antinilpotent as well.

The following result represents the motivation behind the study of antinilpotent modules. For a commutative ring A of prime characteristic p, we say that A is F-pure if $F : A \to A$ is a pure homomorphism of A-modules.

Theorem 7.2 (Enescu–Hochster, [13]). *Let $(A, \mathfrak{m})$ be an F-pure Gorenstein local ring of dimension d. Then $H^d_{\mathfrak{m}}(A)$ is antinilpotent with respect to the canonical Frobenius action on it.*

Under the Gorenstein hypothesis, the F-purity of A is equivalent to the injectivity of the Frobenius action on $H^d_{\mathfrak{m}}(A)$. So, when A is Gorenstein, Theorem 7.2 says that the injectivity of the Frobenius action implies a stronger form of injectivity, namely antinilpotency. Therefore, it makes sense to understand the connection between these two concepts in a general setting.

An interesting property of antinilpotent modules is highlighted by the next result.

Theorem 7.3 (Enescu–Hochster, [13]). *Let M be an Artinian A-module. Assume that M admits a Frobenius action F such that M is antinilpotent. Then M has finitely many submodules that are F-compatibile.*

Let M be an A-module and $F : M \to M$ a Frobenius action on M. For a submodule N of M we denote $\langle F(N) \rangle_A$ the A-submodule generated by $F(N)$ in M.

Lemma 7.4. *Let M be an A-module, and $F : M \to M$ an injective Frobenius action on M. Then M is antinilpotent if and only if for all F-compatible submodules N of M, $\langle F(N) \rangle_A = N$.*

Proof. First assume that M is antinilpotent and let N be an F-compatible submodule of M. Then we have an induced Frobenius action $F : \frac{N}{\langle F(N) \rangle_A} \to \frac{N}{\langle F(N) \rangle_A}$ which is trivially kills $\frac{N}{\langle F(N) \rangle_A}$. Thefore, $N = \langle F(N) \rangle_A$, since M is antinilpotent.

For the converse, let N be an F-compatible submodule of M. We plan to show that $F : \frac{M}{N} \to \frac{M}{N}$ is injective, or, in other words, if $m \in M$ with $F(m) \in N$, then $m \in N$.

Let $N_0 = Rm + N$. Clearly, $F(N_0) \subset \langle F(N_0) \rangle_A \subseteq \langle F(N) \rangle_A \subseteq N \subseteq N_0$ which means that N_0 is F-compatible. By hypothesis, $\langle F(N_0) \rangle_A = N_0$, so $N = N_0$. Therefore $m \in N$. $\qquad\qquad\qquad\square$

Let A be a ring and $\mathfrak{m}$ a maximal ideal of A. Let V be a vector space over $A/\mathfrak{m}$ and consider the natural A-module structure on V obtained by restriction of scalars to A, denoted by $V(\mathfrak{m})$. As sets $V = V(\mathfrak{m})$. Obviously, if F is a Frobenius action on V over $A/\mathfrak{m}$, one obtains a natural Frobenius action on $V(\mathfrak{m})$ as an A-module.

Proposition 7.5. (i) *Let $(A, \mathfrak{m})$ be a local ring and M a finitely generated A-module with an antinilpotent Frobenius action. Then $\mathfrak{m} M = 0$ and hence $M = V(\mathfrak{m})$, where in fact $V = M$ regarded as $A/\mathfrak{m}$-vector space and V is finite-dimensional and antinilpotent.*

 (ii) *Let A be a Noetherian ring and M be an antinilpotent module that is finitely generated over A. Then there exist a finite set Λ of maximal ideals of A and antinilpotent $A/\mathfrak{m}_i$-vector spaces V_i, for any $\mathfrak{m}_i \in \Lambda$ such that $M = \bigoplus_{\mathfrak{m}_i \in \Lambda} V_i(\mathfrak{m}_i)$.*

Proof. For (i), for any ideal I, F acts injectively on $IM/I^2 M$. On the other hand F kills $IM/I^2 M$ and so $IM = I^2 M$. Therefore $IM = 0$ and in particular $\mathfrak{m} M = 0$. The rest of assertions follow.

(ii) Again $I^2 M = IM$ for all I ideals in A and this is preserved under localization. Note that $M \to \prod_{\mathfrak{m} \in \mathrm{Max}(A)} M_\mathfrak{m}$ is injective. By (1) $\mathfrak{m} M_\mathfrak{m} = 0$. So $M_\mathfrak{m} = V(\mathfrak{m})$ for some $A/\mathfrak{m}$-vector space V. Now it follows easily that the image of M is of the form stated in the conclusion. The fact the only a finite number of maximal ideals appear in the product giving M comes from the fact that M is Noetherian. $\qquad\square$

Let $F_*A = A^{(1)}$ be the right A-algebra obtained on A via the Frobenius map $F : A \to A$ by restriction of scalars. By convention, $A^{(1)}$ equals A as a left A-module. Let M be an A-module with a Frobenius action $F_M : M \to M$. Let $F_*(M) = A^{(1)} \otimes_A M$.

It is easy to check that the Frobenius actions on M are in one-to-one correspondence to elements of $\mathrm{Hom}_A(F_*(M), M)$ (as in Remark 3.2 in [25]). Under this correspondence F_M maps to ω_M, where $\omega_M(a \otimes m) = a F(m)$, for all $a \in A, m \in M$.

This construction is functorial in the sense that if $g : N \to M$ is an A-linear map with compatible Frobenius action

$$
\begin{array}{ccc}
N & \xrightarrow{\ g\ } & M \\
{\scriptstyle F_N}\downarrow & & \downarrow{\scriptstyle F_M} \\
N & \xrightarrow{\ g\ } & M
\end{array}
$$

then the following diagram of A-linear maps

$$
\begin{array}{ccc}
A^{(1)} \otimes_A N & \xrightarrow{\ 1\otimes g\ } & A^{(1)} \otimes_A M \\
{\scriptstyle \omega_N}\downarrow & & \downarrow{\scriptstyle \omega_M} \\
N & \xrightarrow{\ g\ } & M
\end{array}
$$

commutes.

An example of an A-linear map compatible with the Frobenius actions is the inclusion map $i : N \to M$ defined by an F-compatible submodule N of M. Note that $\langle F(N) \rangle_A = \omega_N(A^{(1)} \otimes_A N)$.

Proposition 7.6. *Let V be a finite dimensional vector space with a Frobenius action $F : V \to V$ and corresponding $\omega_V : K^{(1)} \otimes_K V \to V$. Then V is antinilpotent if and only if ω_V is isomorphism if and only if ω_V is injective if and only if ω_V is surjective.*

Proof. The composition of $V \to K^{(1)} \otimes_K V \xrightarrow{\omega_V} V$ gives the Frobenius action on V so the injectivity of ω_V implies that F is injective.

First note that $\dim_{K^{(1)}}(K^{(1)} \otimes_K V) = \dim_K(V)$. But on the left $K^{(1)}$ is simply K. Therefore the surjectivity of ω_V implies that ω_V is an isomorphism of K-vector spaces.

Now consider an F-compatible K-subspace V' of V. Since K is field we get that $K^{(1)} \otimes_K V' \xhookrightarrow{i} K^{(1)} \otimes_K V$. Moreover we have the following commutative diagram

$$
\begin{array}{ccc}
K^{(1)} \otimes_K V' & \xrightarrow{\ 1\otimes i\ } & K^{(1)} \otimes_K V \\
{\scriptstyle \omega_{V'}}\downarrow & & \downarrow{\scriptstyle \omega_V} \\
V' & \xrightarrow{\ i\ } & V
\end{array}
$$

which implies that $K^{(1)} \otimes_K V' \to V'$ is injective. As above, by dimension considerations, it must also be surjective, hence $\langle F(V') \rangle_K = V'$ which implies that V is antinilpotent, according to Lemma 7.4.

For the converse, if V is antinilpotent then $\omega_V(K^{(1)} \otimes_K V) = V$ by Lemma 7.4, hence ω_V is surjective $\square$

Corollary 7.7. *Let K be a perfect field. Let V be a finite dimensional K-vector space that admits a Frobenius action. Then the Frobenius action is injective if and only if V is antinilpotent.*

Proof. Fix a basis for V. If the Frobenius action F is injective, then Proposition 6.4 shows that the matrix describing the action is invertible. But this matrix coincides with the one describing the map ω_V therefore Theorem 7.6 applies. $\square$

Corollary 7.8. *Let $K \subseteq L$ be a finite field extension. Consider the Frobenius map on L which can be regarded as a Frobenius action of L as K-vector space.*
Then L is antinilpotent over K if and only if $K \subset L$ is separable.

Proof. It suffices to note that $K^{(1)} \otimes_K L \to L$ is injective if and only if $K \subset L$ is separable. $\square$

We would like to give now an example of a finite dimensional K-vector space V that admits an injective Frobenius action, but it is not antinilpotent. Note that the base field K is not perfect.

Example 7.9. Let α be a solution of the equation $t^3 + t^2 = 1$ over $\mathbb{F}_3$. Let X be an indeterminate and construct $K = \mathbb{F}_3(\alpha)(X) \subset L = \mathbb{F}_3(\alpha)(\sqrt[3]{X})$.

Let $V = L^2$. Since L is finite over K of degree 3 then $\dim_K(V) = 6$.

We define the following Frobenius action

$$F(x_1, x_2) = (x_1^3, x_2^3) \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (x_1^3, x_1^3 + x_2^3),$$

for all $x_1, x_2 \in L$.

It is an immediate check to see that F is injective.

Let $W = K \cdot (\alpha, -1) \subset V$.

Let $a \in K$. Then $F(a(\alpha, -1)) = a^3 F(\alpha, -1) = a^3(\alpha^3, \alpha^3 - 1) = a^3(\alpha^3, -\alpha^2) = \alpha^2 \cdot a(\alpha, -1) \notin W$, since $\alpha^2 \notin \mathbb{F}_3$.

But if $v = \sqrt[3]{X}(\alpha, -1)$, we get $F(v) = \alpha^2 \cdot X(\alpha, -1) \in W$, while $v \notin W$.

This shows that V is not antinilpotent with respect to the action considered.

We explain now a relationship between the notion of $\mathbb{F}$-modules, due to Lyubeznik [23] who in turn was inspired by work of Harthsorne–Speiser [16], and antinilpotent modules.

Definition 7.10. Let M be an A-module with a Frobenius action $F : M \rightarrow M$. We say that M is an $\mathbb{F}$-module if the map

$$A^{(1)} \otimes_A M \rightarrow M$$

is an A-isomorphism of modules. Note that, as an left A-algebra, $A^{(1)} = A$.

Over a regular ring A, every $\mathbb{F}$-module M has the property that a submodule N is an $\mathbb{F}$-module if and only if $\langle F(N) \rangle_A = N$.

Corollary 7.11. *A finite dimensional vector space V over a field K is an $\mathbb{F}$-module if and only if it is antinilpotent.*

When $K = \mathbb{F}_p$ we note that a Frobenius action of a K-vector space is simply a K-linear function. In this situation the antinilpotency of V is equivalent to the injectivity of F on V as it is clear from the characterization in Theorem 7.6. In this case since V is finite is clear that there are finitely many (F-compatible) subspaces of V.

One question that arises in this context is the following. Assume that K is now an (infinite) field and let $T : V \rightarrow V$ be a K-linear map. Is it true that there are at most finitely many subspaces V' of V compatible with T, i.e. $T(V') \subset V'$?

The reader can check that this is the case if and only if V has no repeated elementary divisors, when K is infinite.

We would like to close with an extension of Theorem 4.21 in [13] that shows how the results in this survey might be used in current research.

Proposition 7.12. *Let $(A, \mathfrak{m})$ be a complete local ring with perfect residue field K. Assume that A has prime characteristic p, and let M be an A-module of finite length that admits a Frobenius action F. If F acts injectively on M then M is antinilpotent with respect to F.*

Proof. Note that A contains a copy of K. Hence, since M is of finite length over A, M is a finite dimensional vector space over K. The action F is injective on M when M is regarded as a K-vector space so by Corollary 7.7 it follows that M is antinilpotent as a K-vector space. This automatically makes M antinilpotent as an A-module as well. $\square$

Definition 7.13. Let $(A, \mathfrak{m})$ be a local ring of dimension d. We say that A is generalized Cohen–Macaulay if $H^i_\mathfrak{m}(A)$ is of finite length over A, for all $i < d$. A local ring of prime characteristic $p > 0$ $(A, \mathfrak{m})$ is called FH-finite if, for all $i = 0, \dots, d$, the module $H^i_\mathfrak{m}(A)$ has only finitely many F-compatible submodules.

Theorem 7.14. *Let $(A, \mathfrak{m})$ be a local, complete domain. Assume that A is F-injective, generalized Cohen–Macaulay with perfect residue field K. If the test ideal of A is $\mathfrak{m}$-primary, then A is FH-finite.*

Proof. Since for all $0 \le i \le d - 1$, $H_{\mathfrak{m}}^i(A)$ are of finite length over A, we have that each $H_{\mathfrak{m}}^i(A)$ is antinilpotent with regard to the natural Frobenius action because this action is injective, by Proposition 7.12.

Let $V = 0_H^*$ where $H = H_{\mathfrak{m}}^d(A)$. Denote by τ the test ideal of A. Then it is known that $\tau \cdot V = 0$ and that V is the largest proper F-compatible submodule of H by a theorem of K. E. Smith. Since V is Artinian and τ is $\mathfrak{m}$-primary it follows that V is of finite length over A. Again we conclude that V is antinilpotent, by Proposition 7.12.

To conclude that the action on H is antinilpotent we need to show that F acts injectively on the quotient H/V. But H/V is a simple $K\{F\}$-module. This means that we only need to check that F does not kill H/V.

Let $x_1, \ldots, x_d$ a system of parameters for A. Think of H as the last cohomology module in Čech complex associated to $x_1, \ldots, x_d$. The elements of H can be thought of as classes $[\frac{a}{(x_1 \cdots x_d)^t}]$ with $a \in A$ and $t \ge 0$. Denote by 1 the element $[\frac{1}{x_1 \cdots x_d}]$. Note that this element generates H as an $A\{F\}$-module. Now assume that F kills H/V. Then $F(1) \in V$. But $F(1)$ also generates H as an $A\{F\}$-module. So this implies that $H \subseteq V$ which is a contradiction.

Therefore H and hence all modules $H_{\mathfrak{m}}^i(A)$ are antinilpotent with respect to the canonical Frobenius action. But then Theorem 4.14 in [13] shows that A is FH-finite. □

Bibliography

[1] Asano, K., Nichtkommutative Hauptidealringe, vol. 696 of Actualités. sci. indust. Hermann, Paris 1938.

[2] Asano, K., Arithmetische Idealtheorie in nichtkommutativen Ringen. Jap J Math. 1939; 16:1–36.

[3] Aberbach, I. M., Enescu, F., Test ideals and base change problems in tight closure theory. Trans Amer Math Soc. 2003;355(2):619–636 [electronic].

[4] Blickle, M., The intersection homology $\mathcal{D}$-module in finite characteristic [PhD thesis]. University of Michigan; 2001.

[5] Blickle, M., The intersection homology $\mathcal{D}$-module in finite characteristic. Math Ann. 2004;328(3):425–450.

[6] Blickle, M., Intersection homology $\mathcal{D}$-modules in finite characteristic. In: Mathematisches Institut, Georg-August-Universität Göttingen: Seminars 2003/2004. Göttingen: Universitätsdrucke Göttingen; 2004. p. 91–98.

[7] Blickle, M., Singularities in positive characteristic via D-modules and Frobenius [habilitation thesis]. Universität Essen; 2007.

[8] Blickle, M., Minimal γ-sheaves. Algebra Number Theory. 2008;2(3):347–368.

[9] Blickle, M., Böckle, G., Cartier modules: finiteness results. arXiv:math/0909.2531.

[10] Dieudonné, J., Lie groups and Lie hyperalgebras over a field of characteristic $p > 0$ II. Amer J Math. 1955;77:218–244.

[11] Enescu, F. F-injective rings and F-stable primes. Proc Amer Math Soc. 2003;131(11): 3379–3386.

[12] Enescu, F., Local cohomology and F-stability. J Algebra. 2009;322(9):3063–3077.

[13] Enescu, F., Hochster, M., Frobenius structure of local cohomology. Algebra Number Theory. 2008;2(7):721–754.

[14] Fedder, R., Watanabe, K.-I., A characterization of F-regularity in term of F-purity. In: Commutative algebra. vol. 15 of Mathematical Sciences Research Institute publications. 1989. p. 227–245.

[15] Goodearl, K. R., Warfield Jr, R. B., An introduction to noncommutative Noetherian rings. vol. 16 of London Mathematical Society student texts. Cambridge University Press; 1989.

[16] Harthsorne, R., Speiser, E., Local cohomological dimension in characteristic $p > 0$. Ann Math. 1977;105:45–79.

[17] Hochster, M., Some finiteness properties of Lyubeznik's $\mathcal{F}$-modules. In: Algebra, geometry and their interactions. vol. 448 of Contemporary Mathematics. Providence, RI: American Mathematical Society; 2007. p. 119–127.

[18] Hochster, M., Roberts, J. L., The purity of the Frobenius and local cohomology. Adv Math. 1976;21(2):117–172.

[19] Katz, N., Une formule de congruence pour la fonction ξ, Expose XXII. In: Deligne P, Katz N, editors. Groupes de monodromie en géométrie algébrique. II, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II). vol. 340 of Lecture notes in mathematics. Berlin-New York: Springer-Verlag; 1973.

[20] Katzman, M., Parameter-test-ideals of Cohen–Macaulay rings. Compos Math. 2008; 144(4):933–948.

[21] Katzman, M., A non-finitely generated algebra of Frobenius maps. Proc Amer Math Soc. 2010;138(7):2381–2383.

[22] Katzman, M., Frobenius maps on injective hulls and their applications to tight closure. J Lond Math Soc (2). 2010;81(3):589–607.

[23] Lyubeznik, G., F-modules: applications to local cohomology and D-modules in characteristic $p > 0$. J Reine Angew Math. 1997;491:65–130.

[24] Lyubeznik, G., On the vanishing of local cohomology in characteristic $p > 0$. Compos Math. 2006;142(1):207–221.

[25] Lyubeznik, G., Smith, K. E., On the commutation of the test ideal with localization and completion. Trans Amer Math Soc. 353:8 (2001); 3149–3180.

[26] Jacobson, N., The theory of rings. vol. 2 of Mathematical surveys and monographs. New York: American Mathematical Society; 1943.

[27] Jacobson, N., Basic Algebra II. 2nd ed. Dover Publications; 2009.

[28] McConnell, J. C., Robson, J. C., Noncommutative Noetherian rings [with the cooperation of Small, L. W.]. Revised ed. vol. 30 of Graduate studies in mathematics. Providence, RI: American Mathematical Society; 2001.

[29] Nakayama, T., A note on the elementary divisor theory in non-commutative domains. Bull Amer Math Soc. 1938;44(10):719–723.

[30] Schwede, K., Centers of F-purity. Math Z. 2010;265(3):687–714.

[31] Schwede, K., Tucker, K., On the number of compatibly Frobenius split subvarieties, prime F-ideals, and log canonical centers. Ann Inst Fourier (Grenoble). 2010;60(5): 1515–1531.

[32] Sharp, R. Y., On the Hartshorne–Speiser–Lyubeznik theorem about Artinian modules with a Frobenius action. Proc Amer Math Soc. 2007;135(3):665–670 [electronic].

[33] Sharp, R. Y., Graded annihilators of modules over the Frobenius skew polynomial ring, and tight closure. Trans Amer Math Soc. 2007;359(9):4237–4258 [electronic].

[34] Sharp, R. Y., Graded annihilators and tight closure test ideals. J Algebra. 2009;322(9): 3410–3426.

[35] Sharp, R. Y., An excellent F-pure ring of prime characteristic has a big tight closure test element. Trans Amer Math Soc. 2010;362(10):5455–5481.

[36] Sharp, R. Y., Yoshino, Y., Right and left modules over the Frobenius skew polynomial ring in the F-finite case. Math Proc Cambridge Philos Soc. To appear.

[37] Smith, K. E., Tight closure of parameter ideals. Invent Math. 1994;115(1):41–60.

[38] Smith, K. E., Test ideals in local rings. Trans Amer Math Soc. 1995;347(9):3453–3472.

[39] Smith, K. E., The D-module structure of F-split rings. Math Res Lett. 1995;2(4):377–386.

[40] Smith, K. E., F-rational rings have rational singularities. Amer J Math. 1997;119(1): 159–180.

[41] Smith, K. E., Vanishing, singularities and effective bounds via prime characteristic local algebra. Proceedings, Algebraic Geometry; 1995, Santa Cruz. vol. 62, part 1 of Proceedings of symposia in pure mathematics. Providence, RI: American Mathematical Society; 1997. p. 289–325.

[42] Teichmüller, O., Der Elementarteilersatz für nichtkommutative Ringe. Sitzungsberichte der Preussischen Akademie der Wissenschaften. 1937.

[43] Yoshino, Y., Skew-polynomial rings of Frobenius type and the theory of tight closure. Comm Algebra. 1994;22(7):2473–2502.

Author Information

Florian Enescu, Department of Mathematics and Statistics, Georgia State University, Atlanta GA, USA.
E-mail: fenescu@gsu.edu

Finiteness and Homological Conditions
in Commutative Group Rings

Sarah Glaz and Ryan Schwarz

Abstract. This article surveys the known results for several related families of ring properties in the context of commutative group rings. These properties include finiteness conditions, homological conditions, and conditions that connect these two families. We briefly survey the classical results, highlight the recent progress, and point out open problems and possible future directions of investigation in these areas.

Keywords. Group Rings, Noetherian Rings, Coherent Rings, Finite Conductor Rings, Weak Global Dimension, Von Neumann Regular Rings, Semihereditary Rings, Prüfer Conditions, Zero Divisors, PP Rings, PF Rings.

2010 Mathematics Subject Classification. 13B99, 13D05, 13E99, 13F05.

In memory of James Brewer, with respect and affection.

1 Introduction

Let R be a commutative ring with identity and let G be an Abelian group written multiplicatively. The group ring RG is the free R module on the elements of G with multiplication induced by G. An element x in RG has a unique expression: $x = \sum_{g \in G} x_g g$, where $x_g \in R$ and all but finitely many x_g are zero. With addition, multiplication, and scalar multiplication by elements of R defined analogously to the standard polynomial operations, RG becomes a commutative R algebra.

Properties of the group ring RG, particularly in conjunction with questions of descent and ascent of these properties between R and RG, have been of interest for at least 70 years. In his book *Commutative Semigroup Rings* [14], Gilmer traces the beginning of a systematic interest in the nature of RG, for general rings R and groups G, to Higman's article [28] published in 1940. The commutative case became of interest in its own right when the general results reached a stage of specialization at the start of the 1960s. Many of the classical ring theoretic results for the commutative case were collected in two books published in 1983–84: Gilmer [14], and Karpilovsky [32].

In this article, we survey the known results for several related families of properties in the context of commutative group rings. These properties include: finiteness properties (such as Noetherianess, coherence, quasi coherence, and finite conductor properties), homological properties (such as weak global dimension behavior, von Neumann regularity, semihereditary, and regularity properties), and properties which connect

these two families (such as zero divisor controlling conditions, and Prüfer conditions). Most of the work in this area has been done after the publication of [14], and [32], and employs homological algebra techniques – a direction that was not considered in [14], and only marginally touched in [32]. In addition to highlighting the recent progress in these areas, the article points out open problems and possible future directions of investigation.

Section 1 explores finiteness conditions in the commutative group ring setting. Particularly, this section includes the necessary and sufficient conditions for a group ring to be Noetherian or Artinian (Connell [9]); the necessary and sufficient conditions for a group ring to be coherent (Glaz [16]); and a discussion, particular cases, and open questions, regarding the finite-conductor and quasi coherence properties. This discussion brings in a number of factoriality properties that are closely related to the finite conductor condition, such as GCD, G-GCD and UFD conditions.

Section 2 delves into homological conditions in the group ring setting. The section includes the determination of necessary and sufficient conditions for a group ring to be von Neumann regular (Auslander [2], McLaughlin [37], and Villamayor [44]), semihereditary (Glaz [16]), or coherent regular (Glaz [20]). It also exhibits a formula connecting the weak global dimension of RG with the weak global dimension of R and rank G (Douglas [11], Glaz [16]), and ends with a discussion of possible future directions of exploration of properties such as global dimension, Cohen–Macaulay and Gorenstein ring conditions.

Section 3 considers three zero divisor controlling conditions that can be explored by homological techniques: the PP condition, the PF condition, and the condition that $Q(R)$, the total ring of fractions of the ring R, is von Neumann regular. The section includes the determination of conditions for ascent and descent of these properties between R and RG, (Schwarz and Glaz [43]). It also highlights the applications of these results to the exploration of Prüfer conditions in group ring setting (Schwarz and Glaz [43]). The Prüfer conditions under exploration include arithmetical rings, Gaussian rings, locally Prüfer rings, and Prüfer rings.

2 Finiteness Conditions

Let RG be the group ring associated with a commutative ring R and a multiplicative Abelian group G. The first finiteness conditions to be considered were the properties of being a Noetherian or an Artinian ring. The results in this direction are due to Connell [9].

Theorem 2.1 ([9]). *Let R be a commutative ring and let G be an Abelian group. Then RG is a Noetherian ring if and only if R is a Noetherian ring and G is a finitely generated group.*

As a corollary of this result, Connell [9] determined when a commutative group ring is Artinian.

Corollary 2.2 ([9]). *Let R be a commutative ring and let G be an Abelian group. Then RG is an Artinian ring if and only if R is an Artinian ring and G is a finite group.*

The next finiteness property to be considered was coherence. We start by recalling a few definitions.

Definition 2.3. Let R be a commutative ring. R is said to be *stably coherent* if the polynomial rings in finitely many variables over R are all coherent rings.

It is well known that contrary to the situation for Noetherian rings, the coherence of a ring R does not necessarily ascend to $R[x]$, the polynomial ring in one variable over R (see, for example, [17, Chapter 7] for Soublin's example of such a case). But it is still an open question whether the coherence of the polynomial ring in one variable over a ring R implies the coherence of the polynomial rings in any finite number of variables over R. In all cases where the coherence of R ascends to $R[x]$ this is indeed the case, although the proofs do not employ an inductive argument on the number of variables (as is the case for Noetherian rings). The class of rings which are known to be stably coherent is of considerable size. To name a few: Noetherian rings, von Neumann regular rings, semihereditary rings, coherent rings of global dimension two, and others, are all stably coherent rings. For more details see [17, Chapter 7].

Definition 2.4. Let G be a multiplicative Abelian group. The *rank of G*, denoted by rank G can be defined as follows: A set of non identity elements of G, $\{g_1, \ldots, g_k\}$, is called *independent* if the equation $g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k} = 1$, where $0 < n_i \in \mathbb{Z}$, implies that $g_1^{n_1} = g_2^{n_2} = \cdots = g_k^{n_k} = 1$. An infinite set of elements of G is called independent if every finite subset of it is independent. By Zorn's Lemma, for every group G we can select an independent set of elements that contains only elements of infinite order and is maximal with respect to this property. The cardinality of this set is rank G. Note that if rank $G > 0$, then G contains a free subgroup of order rank G.

With these definitions we can now describe the conditions under which RG is a coherent ring. The necessary and sufficient conditions for the coherence of RG were found by Glaz [16].

Theorem 2.5 ([16]). *Let R be a commutative ring and let G be an Abelian group.*

 (i) *If G is a torsion group, then RG is a coherent ring if and only if R is a coherent ring.*

 (ii) *If $0 < \operatorname{rank} G = n < \infty$, then RG is a coherent ring if and only if the polynomial ring in n variables over R is a coherent ring.*

(iii) *If rank $G = \infty$, then RG is a coherent ring if and only if R is a stably coherent ring.*

Several finiteness properties exist which relax the coherence conditions on the ring without completely eliminating them. Prominent among those are the finite conductor and quasi coherence properties.

Definition 2.6. Let R be a commutative ring. For an element c in R denote by $(0 : c)$ the annihilator of c. R is said to be a *finite conductor ring* if $aR \cap bR$ and $(0 : c)$ are finitely generated ideals of R for all elements a, b, and c in R. A ring R is said to be a *quasi coherent ring* if $a_1 R \cap \cdots \cap a_n R$ and $(0 : c)$ are finitely generated ideals of R for all elements $a_1, \ldots, a_n$, and c in R.

The finite conductor property for integral domains first came into prominence in McAdam's work [36]. Quasi coherence for integral domains was defined by Dobbs [10]. The definitions for general rings are due to Glaz [18]. The theory of these rings is developed in [18]; while [19] provides a survey of the results in this direction and a multitude of examples. Among the class of finite conductor (also quasi coherent) rings we count all coherent rings, UFDs, and GCD domains (that is, integral domains where any two non zero elements have a greatest common divisor), and G-GCD domains (that is, integral domains in which the intersection of two invertible ideals is an invertible ideal). Glaz [18] generalized this last class of rings to rings with zero divisors, and called them G-GCD rings (A ring R is a G-GCD ring if principal ideals of R are projective and the intersection of any two finitely generated flat ideals of R is a finitely generated flat ideal of R). Neither the finite conductor, not the quasi coherence properties have been investigated in the general group ring setting. A few cases, where the finite conductor (or quasi coherent) ring is a particular integral domain, have been solved by Gilmer and Parker [15]. We provide these results in Theorems 2.7 and 2.9 below:

Theorem 2.7 ([15]). *Let R be a commutative ring and let G be an Abelian group. Then RG is a GCD domain if and only if R is a GCD domain and G is a torsion free group.*

Definition 2.8. Let G be an Abelian group. G is said to be *cyclically Noetherian* if G satisfies the ascending chain conditions for cyclic subgroups.

Theorem 2.9 ([15]). *Let R be an integral domain and let G be a torsion free Abelian group. Then RG is a UFD if and only if R is a UFD and G is cyclically Noetherian.*

In the general ring setting, it follows from [19, Proposition 3.2] that both the finite conductor and the quasi coherence properties descend from RG to R. Regarding ascent of these properties from R to RG, [19, Proposition 3.1] reduces the question to the case where G is finitely generated. Beyond this not much is known about the ascent of either property, not even for the simple case, where R is a G-GCD ring and the structure of RG can be made very explicit (for example, when G an infinite cyclic group). We venture to make the following conjecture:

Conjecture 2.10. If R is a G-GCD ring and G is a finitely generated free Abelian group, then the finite conductor and the quasi coherent properties ascend from R to RG.

A further exploration of these conditions in the group ring setting may shed light on a problem that is still open: Are the finite conductor and the quasi coherence properties distinct [18, 19]?

3 Homological Dimensions and Regularity

Let RG be the group ring associated with a commutative ring R and a multiplicative Abelian group G. The first homological condition to be considered in the commutative group ring setting was von Neumann regularity, that is, the case of weak global dimension equal to zero. The determination of conditions under which RG is von Neumann regular, given in Theorem 3.2, was discovered independently, and almost simultaneously, by Auslander in 1957 [2], McLaughlin in 1958 [37], and Villamayor in 1959 [44]. Their work was also the first to mention a condition linking the ring R and the group G that plays an important role in the majority of results involving homological considerations.

Definition 3.1. Let G be an Abelian group and let R be a commutative ring. R *is said to be uniquely divisible by the order of every element of G if for every g in G of finite order n, n divides every element $r \in R$, and if for $r \in R$, we have $r = ns = nt$ for some $t, s \in R$, then $s = t$.*

Since R is a ring with identity, R is uniquely divisible by an integer n if and only if n is a unit in R. It follows that for an Abelian group G the condition of Definition 3.1 is equivalent to asking that for every element g of G, with order of g equal to p, where p is a prime number, p is a unit in R.

Theorem 3.2 ([2,37,44]). *Let R be a commutative ring and let G be an Abelian group. RG is a von Neumann regular ring if and only if the following three conditions hold:*

(i) *R is a von Neumann regular ring.*

(ii) *G is a torsion group.*

(iii) *R is uniquely divisible by the order of every element of G.*

A year after the solution of the von Neumann regular case, Douglas [11] found a general connection between the weak global dimension of R and that of RG. This result was proved independently and by a different method for the case where R is a coherent ring by Glaz in 1987 [16]. Combining the conditions required for the coherence of RG with the formulas for the weak global dimension made it possible to determine when a commutative group ring is semihereditary.

Theorem 3.3 ([11, 16]). *Let R be a commutative ring and let G be an Abelian group. Then* w. gl. dim $RG < \infty$ *if and only if the following three conditions hold:*

(i) w. gl. dim $R < \infty$

(ii) rank $G < \infty$

(iii) *R is uniquely divisible by the order of every element of G*

Moreover, when condition (iii) *holds we have:*

$$\text{w. gl. dim } RG = \text{w. gl. dim } R + \text{rank } G.$$

One corollary of this theorem is another proof of the characterization of von Neumann regular group rings given in Theorem 3.2.

Recall that a ring R is a *semihereditary* ring if every finitely generated ideal of R is projective. The class of semihereditary rings possesses the next level of homological complexity after the class of von Neumann regular rings. Specifically:

Theorem 3.4 ([17]). *Let R be a commutative ring. The following conditions are equivalent:*

(i) *R is a semihereditary ring.*

(ii) *R is a coherent ring and* w. gl. dim $R \le 1$.

(iii) *$Q(R)$, the total ring of fractions of R, is a von Neumann regular ring and R_m is a valuation domain for every maximal ideal m of R.*

Equipped with this characterization Glaz [16] determined necessary and sufficient conditions for a group ring to be semihereditary.

Theorem 3.5 ([16]). *Let R be a commutative ring and let G be an Abelian group. Then RG is a semihereditary ring if and only if exactly one of the following conditions hold:*

(i) *R is a von Neumann regular ring,* rank $G = 1$, *and R is uniquely divisible by the order of every element of G.*

(ii) *R is a semihereditary ring, G is a torsion group, and R is uniquely divisible by the order of every element of G.*

Since the group ring of an infinite cyclic group over R is isomorphic to $R[x, x^{-1}]$, where x is an indeterminate over R, we obtain as a bonus the following corollary.

Corollary 3.6 ([16]). *Let R be a commutative ring and let x be an indeterminate over R. Then $R[x, x^{-1}]$ is a semihereditary ring if and only if R is a von Neumann regular ring.*

Definition 3.7. A commutative ring R is said to be a *regular ring* if every finitely generated ideal of R has finite projective dimension.

This notion coincides with the usual definition of regularity if the ring R is Noetherian. The notion had been extended to coherent rings with a considerable degree of success. Examples of coherent regular rings include all coherent rings of finite weak global dimension. In particular von Neumann regular rings and semihereditary rings are coherent regular rings. But, contrary to the situation for Noetherian rings, there are local coherent regular rings of infinite weak global dimension. One such ring is, for example, $k[[x_1, x_2, \dots]]$, the power series ring in infinitely many indeterminates over a field k. For a detailed account of the notion of regularity in the context of coherent rings, see [17, Chapter 6].

It was therefore natural that the determination of necessary and sufficient conditions for a group ring to be coherent of finite weak global dimension raised the following question [16]: When is a group ring a coherent regular ring? This was answered by Glaz in the follow up paper [20].

Theorem 3.8 ([20]). *Let R be a commutative ring and let G be an Abelian group such that RG is a coherent ring. Then RG is a regular ring if and only if the following two conditions hold:*

(i) *R is a coherent regular ring.*

(ii) *R is uniquely divisible by the order of every element of G.*

We note that it is not known if this result holds without the coherence assumption. In general, although the notion of regularity of rings makes sense without any finiteness assumption, the theory of regular rings that do not possess some finiteness condition is still to be developed. Not much is known about regular rings that are not, at least, coherent.

There are a number of open homological questions whose solutions will considerably enrich our knowledge of the nature of group rings. A natural occurring question is:

Question 3.9. Under what conditions can one find a formula (perhaps similar to the formula found in Theorem 3.3) that connects the global dimension of RG, the global dimension of R and some invariant of the group G?

Very little progress has been made in this direction. Particularly, the only known result is in the case of global dimension zero, the so called *semisimple rings*. This is a classical result called Maschke's Theorem, stated in Theorem 3.10, which can be found, for example, in [32]. It is not known in general under what conditions a commutative group ring is semisimple or hereditary (that is, of global dimension equal to one).

Theorem 3.10 ([32]). *Let G be a finite group and let K be a field. Then KG is a semisimple ring if and only if the characteristic of K does not divide the order of the group G.*

Another interesting direction to consider is a relatively recent development in coherent ring theory, the extension of the Cohen–Macaulay and Gorenstein ring notions to the non-Noetherian setting. Theories of coherent Cohen–Macaulay and Gorenstein rings have been developed by Hamilton, Marley, and Hummel (see, for example, [25, 26, 29]). [30] provides an in-depth overview of the recent developments in the subject and an extensive bibliography. It will be of much interest to explore the conditions under which coherent group rings acquire the Cohen–Macaulay or Gorenstein properties.

4 Zero Divisor Controlling Conditions

Let RG be the group ring associated with a commutative ring R and a multiplicative Abelian group G. This section focuses on the recent results obtained by Schwarz and Glaz [43] regarding a number of zero divisor controlling conditions that can be explored using homological algebra techniques and some of the applications of these results to Prüfer conditions. The determination of conditions under which RG is a domain goes back Higman's 1940 article [28]:

Theorem 4.1 ([28]). *Let R be a commutative ring and let G be an Abelian group. Then RG is an integral domain if and only if R is an integral domain and G is a torsion free group.*

We note that for a commutative ring the property of being an integral domain may be viewed as a homological condition on principal ideals of the ring. Specifically, a commutative ring R is an integral domain if and only if its principal ideals are free [43]. Therefore Theorem 4.1 states that principal ideals of RG are free if and only if principal ideals of R are free and G is a torsion free group. Related homological conditions on principal ideals yield two other zero divisor controlling conditions.

Definition 4.2. A commutative ring R is said to be a *PP ring* (or *weak Baer ring*) if principal ideals of R are projective. R is said to be a *PF ring* if principal ideals of R are flat.

PP rings were first introduced by Hattori [27] and Endo [12] in 1960. Hattori aimed to develop a torsion theory for modules over general rings. This condition has implications on the nature of the annihilator ideals of elements of the ring, and as such on the nature of the zero divisors. Specifically:

Theorem 4.3 ([4]). *Let R be a commutative ring. The following conditions are equivalent:*

(i) *R is a PP ring.*

(ii) *For every element a in R, the ideal $(0 : a)$ is generated by an idempotent.*

(iii) *Every element of R can be expressed as a product of a non zero divisor and an idempotent.*

Although possessing a weaker condition, PF rings can be more explicitly linked to domains. Specifically:

Theorem 4.4 ([17, 35]). *Let R be a commutative ring. The following conditions are equivalent:*

 (i) *R is a PF ring.*

 (ii) *R_p is a domain for every prime ideal p of R.*

(iii) *R_m is a domain for every maximal ideal m of R.*

(iv) *R is a reduced ring and every maximal ideal m of R contains a unique minimal prime ideal p. In this case $p = \{r \in R$: there is a $u \in R-m$ such that $ur = 0\}$ and $R_p = Q(R_m)$, the quotient field of R_m.*

The two conditions are related to another zero divisor controlling condition, namely the requirement that $Q(R)$, *the total ring of fractions of R is von Neumann regular*. Denote by Min R the set of all minimal prime ideals of R with the induced Zariski topology. The three zero divisor controlling conditions are closely linked in the theorem below, which is Glaz's [17] correction of a result of Quentel [39, 40]:

Theorem 4.5 ([17,39,40]). *Let R be a commutative ring. The following conditions are equivalent:*

 (i) *R is a PP ring.*

 (ii) *R is a PF ring and $Q(R)$ is a von Neumann regular ring.*

(iii) *R is a PF ring and Min R is compact in the Zariski topology.*

PP and PF rings make frequent appearances in the literature in a great variety of contexts. The condition that $Q(R)$ is von Neumann regular appears classically in the characterization of semihereditary rings, Theorem 3.4, and has also appeared in a wide variety of both classical and current investigations. For a small sample of papers where some or all three of these conditions appear, see [1, 7, 12, 13, 17, 27, 31, 33–35, 39–42]. Recently all three conditions, but particularly the condition requiring the total ring of quotients to be von Neumann regular, played an important role in the development of the theory of Prüfer conditions in rings with zero divisors, see [3–6, 23] and [24] for a comprehensive survey of this area. We further elaborate on this point later in this section. In the context of group rings, the (not necessarily commutative) PP condition was touched in Pelaez and Teply [38] and in Chen and Zan [8]. All three conditions are explored in depth in Schwarz and Glaz [43], which contains further references to other works involving these conditions. Most of the following results are taken from Schwarz and Glaz [43].

We first resolved the case of von Neumann regularity of the total ring of quotients.

Theorem 4.6 ([43]). *Let R be a commutative ring, and let G be a group that is either torsion free or R is uniquely divisible by the order of every element of G. If $Q(R)$ is a von Neumann regular ring, then $Q(RG)$ is a von Neumann regular ring.*

We note that the converse of this theorem is not true, even if the group is torsion free. [43] provides an example of a torsion free group G (in fact infinite cyclic) and a ring R with $Q(RG)$ von Neumann regular, but $Q(R)$ not von Neumann regular.

In contrast, if the group is torsion free the situation for the PP and the PF conditions is more symmetrical.

Theorem 4.7 ([43]). *Let R be a commutative ring, and let G be a torsion free group. Then RG is a PF ring if and only if R is a PF ring.*

Putting there two results together we conclude:

Corollary 4.8 ([43]). *Let R be a commutative ring and let G be a torsion free group. Then RG is a PP ring if and only if R is a PP ring.*

We extended the descent results to the general case:

Theorem 4.9 ([43]). *Let R be a commutative ring and let G be an Abelian group. If RG is a PF ring (respectively, a PP ring), then R is a PF ring (respectively, a PP ring) and G is either a torsion free group or R is uniquely divisible by every element of G.*

The converse of Theorem 4.9 does not hold if G is not a torsion free group for either the PP or the PF case. Chen and Zan [8] provide an example of a ring R which is PP and a group G such that R is uniquely divisible by the order of every element of G, but RG is not a PP ring. Schwarz and Glaz [43] show that in this case RG is not a PF ring either.

We conclude this section with an application of the results we obtained for the three zero divisor controlling conditions in this section to the extension of the Prüfer conditions to rings with zero divisors. Prüfer domains admit many equivalent definitions. Through the years several of these conditions were explored in a general ring setting, and although there are strong connections between them, in general these conditions were not found to be equivalent.

Definition 4.10. A ring R is said to be an *arithmetical ring* if ideals of R_m are totally ordered by inclusion for each maximal ideal m of R. Let R be a commutative ring and let $f \in R[x]$, the polynomial ring in one variable over R. The so-called *content of f*, denoted $c(f)$, is the ideal of R generated by the coefficients of f. R is said to be a *Gaussian ring* if $c(fg) = c(f)c(g)$ for all $f, g \in R[x]$. R is said to be a *Prüfer ring* if every finitely generated regular ideal of R is invertible. R is said to be *a locally Prüfer ring* if R_p is a Prüfer ring for every prime ideal p of R.

In particular, we considered the following extensions of a Prüfer domain notion to rings with zero divisors:

  (i) R is a semihereditary ring.

 (ii) w. gl. dim $R \leq 1$.

(iii) R is an arithmetical ring.

(iv) R is a Gaussian ring.

 (v) R is a locally Prüfer ring.

(vi) R is a Prüfer ring.

These six Prüfer conditions had been extensively studied for the last 5 to 7 years. For a comprehensive survey and an extensive list of references on the subject see [4] and [24]. In particular, [3, 6, 22] show that the Prüfer conditions listed above satisfy the following diagram of strict implications.

$$\text{(i)} \Rightarrow \text{(ii)} \Rightarrow \text{(iii)} \Rightarrow \text{(iv)} \Rightarrow \text{(v)} \Rightarrow \text{(vi)}.$$

Glaz [23] and Bazzoni and Glaz [3, 4] found conditions that allow for reversals of implications for properties (i)–(iv) and (vi), while Boynton [6] covered the same ground for property (v). In particular, the three zero divisor controlling conditions described in this section allow several reversals of implications and if $Q(R)$ is a von Neumann regular ring, then conditions (i)–(vi) are equivalent for the ring R.

Theorem 3.5 gives the exact conditions under which a commutative group ring satisfies the first Prüfer condition, that is, the semihereditary condition. As a corollary of Theorem 3.3, we obtain similar conditions for a commutative group ring to satisfy the second Prüfer condition, that is, w. gl. dim $R \leq 1$.

Theorem 4.11 ([43]). *Let R be a commutative ring and let G be an Abelian group. Then* w. gl. dim $RG = 1$ *if and only if exactly one of the following conditions hold:*

  (i) *R is a von Neumann regular ring,* rank $G = 1$, *and R is uniquely divisible by the order of every element of G.*

 (ii) w. gl. dim $R = 1$, *G is a torsion group, and R is uniquely divisible by the order of every element of G.*

Using the result of Theorem 4.6 we can prove the following:

Theorem 4.12 ([43]). *Let R be a commutative ring, and let G be a torsion free or a mixed Abelian group. Then the following conditions are equivalent:*

  (i) *RG is a semihereditary ring.*

 (ii) w. gl. dim $RG = 1$.

(iii) *RG is an arithmetical ring.*

(iv) *RG is a Gaussian ring.*

(v)   *RG is a locally Prüfer ring.*

(vi) *RG is a Prüfer ring.*

(vii) *R is a von Neumann regular ring and* rank $G = 1$.

Some of these equivalences (iii), (vi), and (vii) were proved by different methods in [14] and [15]. As a consequence we obtain as a corollary:

Corollary 4.13 ([43]). *Let R be a commutative ring and let x be an indeterminate over R. Then $R[x, x^{-1}]$ satisfies any of the six Prüfer conditions if and only if R is a von Neumann regular ring.*

If G is a torsion group and R is uniquely divisible by the order of every element of G, we obtain a result similar to Theorem 4.12 under the assumption that the total ring of fractions of R is von Neumann regular.

Theorem 4.14 ([43]). *Let R be a commutative ring such that $Q(R)$, the total ring of fractions of R, is von Neumann regular. Let G be a torsion Abelian group and assume that R is uniquely divisible by the order of every element of G. Then the following conditions are equivalent:*

(i)   *RG is a semihereditary ring.*

(ii) w. gl. dim $RG = 1$

(iii) *RG is an arithmetical ring.*

(iv) *RG is a Gaussian ring.*

(v)   *RG is a locally Prüfer ring.*

(vi) *RG is a Prüfer ring.*

(vii) *R is a semihereditary ring.*

An example is given in [43], which shows that the conclusions of Theorem 4.14 need not hold without the assumption that $Q(R)$ is von Neumann regular. At this point the conditions on R and G under which RG satisfies any of the individual Prüfer conditions (iii)–(vi) are not clear. We note that there are several scattered results in the literature giving conditions under which a commutative group ring satisfies one of the Prüfer conditions (iii)–(vi), but those seem to be ad hoc conditions that do not generalize. For example, below is a result from [14]:

Theorem 4.15 ([14]). *Let R be a local arithmetical ring with maximal ideal m and let $c = \mathrm{char}(R/m)$. Assume that G is a finite group of prime power order p^k, where $c \neq p$. Then RG is an arithmetical ring.*

Some examples of group rings that satisfy some, but not other of the six Prüfer conditions also muddy the waters (see [43] for more details). The answer may, or may not, lie in the exploration of other zero divisor controlling conditions in RG. In any case, it is worthwhile exploring other zero divisor controlling conditions in the group ring setting. See [21] for a survey of many of these conditions that appear in the literature.

As a concluding remark, we point out that some of the properties described in this article in the setting when R is a commutative ring and G is an Abelian group have been extended to the case where G is an Abelian monoid. But not all the properties described in this article were considered in this case. In particular, the recent work on Prüfer conditions and zero divisor controlling conditions have not yet been considered in the Abelian monoid setting. Given that in the past such extensions yielded rich and interesting results, this is one direction worth pursuing.

Bibliography

[1] Albrecht, U., Dauns, J., Fuchs, L., Torsion-freeness and non-singularity over right PP rings. J Algebra. 2005;285:98–119.

[2] Auslander, M., On regular group rings. Proc Amer Math Soc. 1957;8:658–664.

[3] Bazzoni, S., Glaz, S., The Gaussian property of total rings of quotients. J Algebra. 2007; 310:180–193.

[4] Bazzoni, S., Glaz, S., Prüfer rings, Multiplicative ideal theory in commutative algebra. Springer; 2006. p. 55–72.

[5] Boynton, J., Pullbacks of arithmetical rings. Comm Algebra. 2007;35:1–14.

[6] Boynton, J., Pullbacks of Prüfer rings. J Algebra. 2008;320:2559–2566.

[7] Chen, J., Ding, N., Yousif, M. F., On generalizations of PF-rings. Comm Algebra. 2004; 32(2):521–533.

[8] Chen, J., Zan, L., PP properties of group rings. Int Electron J Algebra. 2008;3:117–124.

[9] Connell, I. G., On the group ring. Canad J Math. 1963;15:650–685.

[10] Dobbs, D., On going down for simple overrings. Proc Amer Math Soc. 1973;39:515–519.

[11] Douglas, A., The weak global dimension of the group rings of Abelian groups. J Lond Math Soc. 1961;36:371–381.

[12] Endo, S., Note on PP Rings. Nagoya Math J. 1960;17:167–170.

[13] Evans, M. W., On commutative PP rings. Pacific J Math. 1972;41:687–697.

[14] Gilmer, R., Commutative semigroup rings. Chicago lectures in mathematics. Chicago: University of Chicago Press; 1984.

[15] Gilmer, R., Parker, T., Divisibility properties in semigroup rings. Michigan Math J. 1974; 21:65–86.

[16] Glaz, S., On the weak dimension of coherent group rings. Comm Algebra. 1987;15: 1841–1858.

[17] Glaz, S., Commutative coherent rings. vol. 1371 of Lecture notes in mathematics. Berlin: Springer-Verlag; 1989.

[18] Glaz, S., Finite conductor rings. Proc Amer Math Soc. 2000;129:2833–2843.

[19] Glaz, S., Finite conductor rings with zero divisors. In: Non-Noetherian commutative ring theory. vol. 520 of Mathematics and its Applications. 2000. p. 251–270.

[20] Glaz, S., Regular symmetric algebras. J Algebra. 1988;112:129–138.

[21] Glaz, S., Controlling the zero divisors of a commutative ring. vol. 231 of Lecture notes in pure and applied mathematics. New York: Marcel Dekker; 2003. p. 191–212.

[22] Glaz, S., Prüfer conditions in rings with zero divisors. vol. 241 of Lecture notes in pure and applied mathematics. CRC Press; 2005. 272–282.

[23] Glaz, S., Weak dimension of Gaussian rings. Proc Amer Math Soc. 2005;133:2507–2513.

[24] Glaz, S., Schwarz, R., Prüfer conditions in commutative rings. Arab J Sci Eng. 2011;36: 967–983.

[25] Hamilton, T. D., Weak Bourbaki unmixed rings: a step towards non Noetherian Cohen–Macaulayness. Rocky Mountain J Math. 2004:34.

[26] Hamilton, T. D., Marley, T., Non Noetherian Cohen–Macaulay rings. J Algebra. 2007; 307:343–360.

[27] Hattori, A., A foundation of torsion theory for modules over general rings. Nagoya Math J. 1960;17:147–158.

[28] Higman, G., The units of group-rings. Proc Lond Math Soc (2). 1940;42:231–248.

[29] Hummel, L., Marley, T., The Auslander Bridger formula and the Gorenstein property for coherent rings. J Commut Algebra. 1 (2009).

[30] Hummel, L., Recent progress in coherent rings: a homological perspective. Preprint.

[31] Jøndrup, S., PP ring and finitely generated flat ideals. Proc Amer Math Soc. 1971;28: 431–435.

[32] Karpilovsky, G., Commutative group algebras. vol. 78 of Pure and applied mathematics. New York: Marcel Dekker; 1983.

[33] Kim, H., Kim, T. I., PF rings of generalized power series. Kyungpook Math J. 2007;47: 127–132.

[34] Knox, M. L., Levy, R., McGovern, W., Shapiro, J., Generalizations of complemented rings with applications to rings of functions. J Algebra Appl. 2009;8:17–40.

[35] Matlis, E., The minimal prime spectrum of a reduced ring. Illinois J Math. 1983;27: 353–391.

[36] McAdam, S., Two conductor theorem. J Algebra. 1972;23:239–240.

[37] McLaughlin, J. E., A note on regular group rings. Michigan Math J. 1958;5:127–128.

[38] Pelaez, M. G., Teply, M. L., On semihereditary and PP monoid rings. Semigroup Forum 2001;62:399–402.

[39] Quentel, Y., Sur la compacité du spectre minimal d'un anneau. Bull Soc Math France. 1971;99:265–272.

[40] Quentel, Y., Sur la compacité du spectre minimal d'un anneau [erratum]. Bull Soc Math France. 1971;100:461.

[41] Rangaswamy, K., Representing Baer rings as endomorphism rings. Math Ann. 1970;190: 167–176.

[42] Rangaswamy, K., Regular and Baer rings. Proc Amer Math Soc. 1974;42:345–348.

[43] Schwarz, R., Glaz, S., Commutative group rings with von Neumann regular total rings of quotients. Preprint.

[44] Villamayor, O. E., On weak dimensions of algebras. Pacific J Math. 1959;9:941–951.

Author Information

Sarah Glaz, Department of Mathematics, University of Connecticut, Storrs, CT 06269, USA.
E-mail: `sarah.glaz@uconn.edu`

Ryan Schwarz, Department of Mathematics, University of Connecticut, Storrs, CT 06269, USA.
E-mail: `ryan.schwarz@uconn.edu`

Regular Pullbacks

Jason G. Boynton and Sean Sather-Wagstaff

Abstract. We investigate transference of ring-theoretic properties in certain pullback constructions, focusing on the Noetherian property, Prüfer conditions, coherence, the n-generator property, and factorization. This paper contains both new results on the subject and a survey of some of the literature.

Keywords. Atomic Domains, Coherent Rings, n-Generator Property, Noetherian Rings, Prüfer Rings, Pullbacks.

2010 Mathematics Subject Classification. 13A15, 13E05, 13E15, 13F05, 13F20.

Dedicated to the memory of Jim Brewer, with gratitude and respect.

1 Introduction

Let R be a commutative ring with identity. A classical theorem in dimension theory states that the Krull dimension of the polynomial ring $R[X]$ is between $n+1$ and $2n+1$ where $n = \dim(R)$. Moreover, it was shown by Seidenberg [35, Theorem 3] that for every pair of nonnegative integers m, n such that $n + 1 \leq m \leq 2n + 1$, there exists an integrally closed quasilocal domain R such that $\dim(R) = n$ and $\dim(R[x]) = m$. The ring R is constructed using what we now know of as the "classical" $D + M$ construction, introduced (as best we know) by Krull [30] and popularized by Gilmer [26, Appendix 2].

For the classical construction, start with a valuation domain V containing a retract field K, meaning that $V = K + M$ where M is the unique maximal ideal of V. Let D be a subring of K, and form the subring $D + M \subset V$. This is the situation considered by Dobbs and Papick [16]. A more general version of this is introduced by Brewer and Rutter [10] where the valuation condition in the ring $T = K + M$ is dropped. Brewer and Rutter lay much of the foundation for this subject, focusing on the transference of properties between $D + M$ and the rings D and $K + M$. A sample of their results is contained in the next theorem.

Theorem 1.1. *Given an integral domain of the form $T = K + M$ where K is a field and D is a subring of K, the following statements hold for the ring $R = D + M$:*

(i) [10, Theorem 4] *The ring R is Noetherian if and only if T is Noetherian, D is a field and $[K : D] < \infty$.*

(ii) [10, Theorem 3] *The ring R is coherent if and only if T is coherent and either (M is T-finite, D is a field, and $[K : D] < \infty$) or (T_M is a valuation ring, D is coherent, and $Q(D) = K$).*

(iii) [10, Theorem 5] *The ring R is a Prüfer domain if and only if T and D are Prüfer domains and $Q(D) = K$.*

(iv) [10, Theorem 10] *The ring R is a Prüfer domain with the n-generator property if and only if T and D are Prüfer domains with the n-generator property.*

The $D + M$ construction is a special case of a pullback. Moreover, it is a particular pullback coming from a *conductor square*. Since this construction is the focus of this paper, we describe it here explicitly. Start with a ring surjection $\eta_1 : T \twoheadrightarrow B$ and an inclusion of rings $\iota_1 : A \hookrightarrow B$ with $B \neq 0$, hence $A \neq 0$. Let R denote the pullback of these maps, that is, the subring of $A \times T$ consisting of all elements (a, t) such that $\iota_1(a) = \eta_1(t)$. The natural maps $\eta_2 : R \twoheadrightarrow A$ and $\iota_2 : R \hookrightarrow T$ yield a commutative diagram of ring homomorphisms

$$
\begin{array}{ccc}
R & \overset{\iota_2}{\hookrightarrow} & T \\
\eta_2 \downarrow & & \downarrow \eta_1 \\
A & \underset{\iota_1}{\hookrightarrow} & B
\end{array}
\qquad (\square)
$$

such that $\mathrm{Ker}(\eta_2)$ and $\mathrm{Ker}(\eta_1)$ are isomorphic via ι_2. (We abuse notation in the sequel, viewing R as a subring of T, and writing $\mathrm{Ker}(\eta_2) = \mathrm{Ker}(\eta_1)$.) The common ideal $\mathrm{Ker}(\eta_i)$ is the largest common ideal of R and T; it is denoted C and called the *conductor* of T into R. When C contains a T-regular element, we say that the conductor square ($\square$) is *regular*.

Conductor squares can also be built as follows. Let T be a commutative ring with subring R, and suppose that R and T have a common, non-zero ideal. We call the largest common ideal C the *conductor* of T into R. Setting $A = R/C$ and $B = T/C$, we obtain a commutative diagram ($\square$) which is a conductor square. For additional information on pullbacks, see Fontana, Huckaba, and Papick [21, Chapter I].

It is common in the study of pullback constructions to assume that T is an integral domain and that C is a maximal ideal of T. However, important examples are obtained by allowing zero-divisors in the pullback square. For example, let D be an integral domain with field of fractions K, and let $E = \{e_1, \ldots, e_r\} \subset D$. Setting $T = K[X]$ and $C = (X - e_1) \cdots (X - e_r)K[X]$, we have $B = T/C \cong \prod_{i=1}^{r} K$. Using $A = \prod_{i=1}^{r} D$ in the conductor square, we get $R = \mathrm{Int}(E, D) = \{g \in K[X] \mid g(E) \subset D\}$, the ring of integer-valued polynomials on D determined by the subset E. Observe that

the rings A and B are not integral domains. It is worth noting that McQuillan [33, Proposition 5] explicitly identifies $\text{Int}(E, D)$ as $C + \sum_{i=1}^{r} D\phi_i$ where $\phi_1, \ldots, \phi_r$ are the Lagrange interpolation polynomials of degree $r - 1$. Other important examples using pullbacks are collected by Lucas [32].

The point of this paper is to investigate the following question of Chapman and Glaz [12, Open Problem 50]: What ring-theoretic properties transfer in the conductor square ($\square$) when C is not a maximal (or even a prime) ideal of T? We take our motivation from Theorem 1.1, and from other similar results, e.g., [1, 9, 27, 33].

In this paper, we survey some of the results in the literature for conductor squares, and we include some results that are (as best we know) new. We include specific references for the older results, not necessarily to the original article where they appeared, but we only include proofs for these results in a few cases. Given the wealth of research in this area, we cannot hope to survey every known result. Our choices reflect our current research interests. The articles of Gabelli and Houston [25] and Kabbaj [29] contain excellent surveys of other aspects of this area.

The new results focus on regular conductor squares. Our perspective is that the regularity condition implies that the rings R and T are not too far apart. (For instance, see Proposition 2.5.) This is akin to Glaz's assumption in [27] that the map $R \hookrightarrow T$ be a "flat epimorphism." It is worth noting that Sections 2–5 contain both new and old results, while Sections 6 and 7 consist entirely of survey material.

2 Some Background

We begin with some preliminary results regarding general pullback constructions. Recall that the *total quotient ring* of a commutative ring U is the localization $Q(U) := V^{-1}U$ where V is the set of non-zero-divisors of U. An *overring* of U is a U-algebra W that is isomorphic (as a U-algebra) to a subring of $Q(U)$. Also, given a ring homomorphism $f : U \to W$ and a multiplicatively closed subset $S \subseteq W$, the localization of W as a U-module $S^{-1}W$ is a U-algebra under the natural operations; moreover, it is an $S^{-1}U$-algebra that is isomorphic to the localization $f(S)^{-1}W \simeq (S^{-1}U) \otimes_U W$.

Lemma 2.1. *Consider the conductor square ($\square$).*

(i) [27, p. 149] *There is an isomorphism $B \simeq A \otimes_R T$.*

(ii) [21, Lemma 1.1.4(3)] *If $P \in \text{Spec}(R)$ and $C \nsubseteq P$, then there is a unique $Q \in \text{Spec}(T)$ such that $Q \cap R = P$; moreover, the induced map $R_P \to T_Q$ is an isomorphism.*

(iii) *If $T \simeq S^{-1}R$ for some multiplicatively closed set $S \subset R$, then $B \simeq S^{-1}A$; moreover, B is an overring of A.*

(iv) *If C is finitely generated over R, then it is finitely generated over T. The converse holds if $R \hookrightarrow T$ is finite.*

(v) *The extension $A \hookrightarrow B$ is of finite type (resp. integral, finite) if and only if $R \hookrightarrow T$ is of finite type (resp. integral, finite).*

Proof. (iii) If $T \simeq S^{-1}R$, then $B \simeq A \otimes_R T \simeq A \otimes_R (S^{-1}R) \simeq S^{-1}A$. To see that $B \simeq S^{-1}A$ is an overring of A, use the fact that the map $A \hookrightarrow B \simeq S^{-1}A \simeq \eta_2(S)^{-1}A$ is a monomorphism to conclude that $\eta_2(S)$ consists of non-zero-divisors for A, so B is naturally a subring of $Q(A)$.

(iv) For one implication, assume that $C = Rc_1 + \cdots + Rc_n$. Since C is an ideal of R and an ideal of T, we have $C = TC = Tc_1 + \cdots + Tc_n$, so C is finitely generated over T.

For the converse, suppose that $T = Rt_1 + \cdots + Rt_m$ and that $C = Tc_1 + \cdots + Tc_n$. Then for each $c \in C$ we have $c = \sum_{i=1}^{n} s_i c_i = \sum_{i \leq n}(\sum_{j \leq m} r_{ij} t_j) c_i = \sum_{i,j} r_{ij}(t_j c_i)$. It follows that $\{t_j c_i\}$ is a set of generators for C over R.

(v) If $R \hookrightarrow T$ is of finite type (resp. integral, finite), then $A \hookrightarrow B$ is of finite type (resp. integral, finite) by part (i). The converse holds by [21, Lemma 1.1.4 (7)]. □

It is reasonable to ask if "finitely presented" can be added to the list of finiteness conditions in Lemma 2.1 (v) above. In the result that follows, we find that under certain conditions, this is indeed the case.

Lemma 2.2. *Consider the conductor square ($\square$).*

 (i) *If T is finitely presented over R, then B is finitely presented over A.*

(ii) *If T is finitely generated over R, B is finitely presented over A, and C is finitely presented (over R or T), then T is finitely presented over R.*

Proof. (i) Assume that T is finitely presented over R, and consider an exact sequence $R^n \to R^m \to T \to 0$ over R. It follows that T is finitely generated over R. The right-exactness of $- \otimes_R A$ provides an exact sequence

$$R^n \otimes_R A \to R^m \otimes_R A \to T \otimes_R A \to 0$$

over A. From the isomorphism $T \otimes_R A \cong B$, this yields an exact sequence $A^n \to A^m \to B \to 0$ over A, so B is finitely presented over A.

(ii) Assume that T is finitely generated over R, B is finitely presented over A, and C is finitely presented (over R or T). Since T is finitely generated over R, there is an R-module epimorphism $\alpha: R^m \twoheadrightarrow T$. To show that T is finitely presented over R, it suffices to show that $\text{Ker}(\alpha)$ is finitely generated over R.

As in the proof of part (i), the right-exactness of $- \otimes_R A$ provides an A-module epimorphism $\overline{\alpha}: A^m \twoheadrightarrow B$. The maps α and $\overline{\alpha}$ fit into the following commutative

diagram with exact rows and columns:

$$
\begin{array}{ccccc}
R^m & \xrightarrow{\ f^m\ } & A^m & \longrightarrow & 0 \\
{\scriptstyle \alpha}\downarrow & & {\scriptstyle \bar{\alpha}}\downarrow & & \\
T & \xrightarrow{\ f'\ } & B & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \\
0 & & 0. & &
\end{array}
$$

Here, the maps $f\colon R \to A$ and $f'\colon T \to B$ are the natural ones from the conductor square ($\square$). In particular, we have $\mathrm{Ker}(f^m) = C^m$ and $\mathrm{Ker}(f') = C$. Given this commutative diagram, we conclude that $\alpha(\mathrm{Ker}(f^m)) \subseteq \mathrm{Ker}(f')$, yielding the next commutative diagram with exact rows and columns:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & C^m & \xrightarrow{\ \epsilon\ } & R^m & \xrightarrow{\ f^m\ } & A^m & \longrightarrow & 0 \\
& & {\scriptstyle \alpha'}\downarrow & & {\scriptstyle \alpha}\downarrow & & {\scriptstyle \bar{\alpha}}\downarrow & & \\
0 & \longrightarrow & C & \xrightarrow{\ i\ } & T & \xrightarrow{\ f'\ } & B & \longrightarrow & 0 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
& & 0 & & 0 & & 0. & &
\end{array}
$$

Here, the maps i and ϵ are the inclusions, and α' is the restriction of α to $\mathrm{Ker}(f^m) = C^m$.

Claim 1. The map α' is T-linear. The map $\alpha\colon R^m \to T$ is R-linear, so there are elements $t_1, \ldots, t_m \in T$ such that $\alpha(r_1, \ldots, r_m) = \sum_{j=1}^m r_j t_j$. It follows that $\alpha'(c_1, \ldots, c_m) = \sum_{j=1}^m c_j t_j$, and that α' respects T-scalar multiplication.

Claim 2. The map α' is surjective. (This is a fairly routine diagram chase with a twist.) Let $c \in C$. Since f^m is surjective, there is a vector $\mathbf{r} = (r_1, \ldots, r_m) \in R^m$ such that $\sum_{j=1}^m r_j t_j = \alpha(\mathbf{r}) = 1$. Hence, $c\mathbf{r} = (cr_1, \ldots, cr_m) \in C^m$ is an element such that $\alpha'(c\mathbf{r}) = \sum_{j=1}^m cr_j t_j = c(\sum_{j=1}^m r_j t_j) = c(1) = c$.

Claim 3. The module $\mathrm{Ker}(\alpha')$ is finitely generated over T and over R. Since α' is R-linear and T-linear, we know that $\mathrm{Ker}(\alpha')$ is an R-module and a T-module.

Assume first that C is finitely presented over T. It follows that C^m is finitely generated over T, and the exact sequence

$$
0 \to \mathrm{Ker}(\alpha') \to C^m \xrightarrow{\ \alpha'\ } C \to 0
$$

implies that $\mathrm{Ker}(\alpha')$ is finitely generated over T; see [34, Corollary 3.63]. Since T is finitely generated over R, this implies that $\mathrm{Ker}(\alpha')$ is finitely generated over R.

Assume next that C is finitely presented over R. The argument of the previous paragraph implies that $\mathrm{Ker}(\alpha')$ is finitely generated over R. Since $\mathrm{Ker}(\alpha')$ is a T-module and T is an R-algebra, it follows that $\mathrm{Ker}(\alpha')$ is finitely generated over T. This completes the proof of Claim 3.

The Snake Lemma provides the following exact sequence:

$$0 \to \mathrm{Ker}(\alpha') \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\overline{\alpha}) \to 0.$$

Since B is finitely presented over A, we know that $\mathrm{Ker}(\overline{\alpha})$ is finitely generated over A, hence over R. Claim 3 implies that $\mathrm{Ker}(\alpha')$ is finitely generated over R, so the above exact sequence implies that $\mathrm{Ker}(\alpha)$ is finitely generated over R, as desired. $\square$

The next result concerns local rings and pullbacks. Here, we observe how the local property transfers in a general pullback of the type ($\square$).

Proposition 2.3. *Consider the conductor square* ($\square$).

(i) [21, Lemma 1.1.5] *If R is local, then C is contained in the Jacobson radical of T and there is a* 1-1 *correspondence between the maximal ideals of B and the maximal ideals of T.*

(ii) *If A and T are local rings, then R is a local ring.*

(iii) *The rings R and B are local if and only if A and T are local.*

Proof. (ii) Since A is local, it has a unique maximal ideal $\overline{M}$ for some maximal ideal M of R.

We claim that $C \subseteq N$ for each maximal ideal N of R. By way of contradiction, suppose that $C \nsubseteq N$. Lemma 2.1 (ii) provides a unique prime ideal N' of T such that $N' \cap R = N$. The uniqueness of N', with the fact that N is maximal, implies that N' is maximal. Since T is local, it follows that N' is the unique maximal ideal of T. The fact that T is local and $C \neq T$ implies that $C \subset N'$; but the condition $N' \cap R = N$ contradicts the assumption $C \nsubseteq N$.

Using the claim with the prime correspondence for quotient rings, we conclude that R is local with unique maximal ideal M

(iii) ($\Rightarrow$) As R is local, so is A. As B is local, part (i) implies that T is local.

($\Leftarrow$) As T is local, so is B; and R is local by part (ii). $\square$

Notation 2.4. Given the conductor square ($\square$) and a prime ideal P of R that contains C, we may use the R-flatness of R_P to build a new square ($\square_P$) with conductor ideal C_P displayed below.

$$
\begin{array}{ccc}
R_P & \hookrightarrow & T_P \\
\downarrow & & \downarrow \\
A_P & \hookrightarrow & B_P
\end{array}
\qquad (\square_P)
$$

Our next result is particular to regular conductor squares of the type ($\square$). Part (i) is from the folklore of the subject; as best we know, parts (ii) and (iii) are new. Although the proofs of parts (i) and (ii) are very straightforward, they prove to be extremely useful in the sequel. In a sense, part (ii) says that T is very close to R. Part (iii) is a generalization of [10, Lemma 1].

Proposition 2.5. *Consider the regular conductor square* ($\square$).

(i) *T is an overring of R.*

(ii) *C contains an isomorphic copy of the R-module T.*

(iii) *If C is finitely generated over R, then every maximal ideal in B contracts to a maximal ideal in R.*

Proof. First we select any T-regular element $c \in C$

(i) One readily checks that the map $T \to Q(R)$ given by $t \mapsto \frac{ct}{c}$ is a well-defined monomorphism.

(ii) Since c is T-regular, there is an R-module isomorphism $T \simeq Tc \subseteq C \subseteq R$.

(iii) Fix a maximal ideal $\mathfrak{n} \subset B$, and let $\mathfrak{N}$ denote the contraction of $\mathfrak{n}$ in T along the surjection $T \twoheadrightarrow B$. Then $\mathfrak{N}$ is a maximal ideal of T containing C. Set $\mathfrak{p} = A \cap \mathfrak{n}$.

Claim. $C/\mathfrak{N}C \neq 0$. Since c is not annihilated by any element of T, we have $0 \neq c/1 \in C_{\mathfrak{N}}$. In particular, the module $C_{\mathfrak{N}}$ is non-zero. Also, since C is finitely generated over R, it is finitely generated over T. Hence $C_{\mathfrak{N}}$ is finitely generated over $T_{\mathfrak{N}}$. Nakayama's Lemma implies that $0 \neq C_{\mathfrak{N}}/\mathfrak{N}C_{\mathfrak{N}} \cong C/\mathfrak{N}C$.

Claim. $C/\mathfrak{N}C$ is a finitely generated $A/\mathfrak{p}$-module. Let $\mathfrak{P}$ denote the contraction of $\mathfrak{p}$ in R along the surjection $R \twoheadrightarrow A$. Via the composition $R \to A \to B$, we have $\mathfrak{P}B = \mathfrak{p}B \subseteq \mathfrak{n}$. It follows that $C/\mathfrak{N}C$ is a module over $R/\mathfrak{P} \cong A/\mathfrak{p}$ via the structure $\overline{a} \cdot \overline{c} = \overline{a \cdot c}$. Since C is finitely generated over R, it follows that $C/\mathfrak{N}C$ is also finitely generated over R, hence over $R/\mathfrak{P} \cong A/\mathfrak{p}$.

It remains to show that $\mathfrak{p}$ is maximal. The quotient $C/\mathfrak{N}C$ is a non-zero vector space over the field $T/\mathfrak{N} \cong B/\mathfrak{n}$, so there is a $B/\mathfrak{n}$-module epimorphism $C/\mathfrak{n}C \twoheadrightarrow B/\mathfrak{n}$. By construction, this is an $A/\mathfrak{p}$-module epimorphism. Since $C/\mathfrak{n}C$ is finitely generated over $A/\mathfrak{p}$, it follows that $B/\mathfrak{n}$ is finitely generated over $A/\mathfrak{p}$. That is, the extension $A/\mathfrak{p} \hookrightarrow B/\mathfrak{n}$ is module-finite. Thus, we have $\dim(A/\mathfrak{p}) = \dim(B/\mathfrak{n}) = 0$, so $\mathfrak{p}$ is maximal. $\square$

3 Pullbacks of Noetherian Rings

In this section, we investigate the transference of Noetherianicity in a conductor square of the type ($\square$). We begin by recalling the next result which relates the Noetherianicity of rings in the most general setting for pullbacks.

Theorem 3.1 ([21, Proposition 1.1.7]). *For the conductor square* (□), *the rings R and B are Noetherian and $R \hookrightarrow T$ is finite if and only if A and T are Noetherian rings and $A \hookrightarrow B$ is finite.*

Theorem 1.1 (i) above suggests the following analogous result for conductor squares (□) in which C contains a T-regular element.

Theorem 3.2. *Consider the conductor square* (□) *and the following conditions:*

  (i) *The ring R is Noetherian.*

 (ii) *The rings A, T, and B are Noetherian and the extensions $A \hookrightarrow B$ and $R \hookrightarrow T$ are finite.*

(iii) *The rings A and T are Noetherian and the extension $R \hookrightarrow T$ is finite.*

(iv) *The rings A and T are Noetherian and the extension $A \hookrightarrow B$ is finite.*

The implications (iv) ⇔ (iii) ⇔ (ii) ⇒ (i) *always hold. If the conductor square* (□) *is regular, then the conditions* (i)–(iv) *are equivalent.*

Proof. The implication (ii) ⇒ (iii) is trivial, and the equivalence (iv) ⇒ (iii) is from Lemma 2.1 (v).

(iii) ⇒ (ii) Since $A \hookrightarrow B$ is finite, Lemma 2.1 (v) asserts that the map $R \hookrightarrow T$ is finite. Also, the fact that $A \hookrightarrow B$ is finite and A is Noetherian implies that B is Noetherian.

(ii) ⇒ (i) Since $R \hookrightarrow T$ is finite and T is Noetherian, Eakin's Theorem [18, Theorem 2] implies that R is Noetherian.

(i) ⇒ (iii) Assume that the conductor square (□) is regular. Since R is Noetherian, the ideal C is finitely generated over R and A is Noetherian. Since (□) is regular, Proposition 2.5 (ii) says that C contains an R-submodule that is isomorphic to T. Hence, T is a submodule of a finitely generated module over the Noetherian ring R and so, it too is a finitely generated R-module. It follows that the extension $R \hookrightarrow T$ is finite, which in turn ensures that T is Noetherian.   □

The next three examples show why we need to assume that C is regular as an ideal of T in the implications (i) ⇒ (n) of Theorem 3.2.

Example 3.3. Let F be a field, and let S be a commutative F-algebra. Consider the rings $R = F \times F$ and $T = F \times S$ with the common ideal $C = F \times 0$. The quotient rings are $A = R/C \cong F$ and $B = T/C \cong S$; under these isomorphisms, the induced map $A \to B$ is the same as the map $F \to S$ giving S its F-algebra structure. In particular, the ring R is Noetherian, but the rings T and B need not be Noetherian. (They are Noetherian if and only if S is Noetherian.) Also, the maps $R \to T$ and $A \to B$ are not necessarily finite. (They are finite if and only if S is finite over F.)

Since pathologies are often easy to construct using products, we present the next examples which do not decompose as products.

Example 3.4. Let F be a field. Consider the rings $R = F[X,Y]/(XY,Y^2)$ and $S = F[\![X,Y]\!]/(XY,Y^2)$ with the natural inclusion $R \to S$. The ideal $C = (Y)R = (Y)S$ is isomorphic to F as an R-module and as an S-module since $XY = 0 = Y^2$. For quotients, we have $A = R/C \cong F[X]$ and $B = T/C \cong F[\![X]\!]$; under these isomorphisms, the induced map $A \to B$ is the same as the natural inclusion $F[X] \to F[\![X]\!]$. The ring $F[\![X]\!]$ is not finitely generated as an $F[X]$-module.[1] It follows that T is not finitely generated as an R-module.

   Of course, in the previous example, the rings T and B are Noetherian. This is not the case in the next example.

Example 3.5. Let F be a field. Consider the rings $R = F[X,Y]/(XY,Y^2)$ and $S = F[X,Y,Z_1,Z_2,\ldots]/(XY,Y^2,YZ_1,YZ_2,\ldots)$ with the natural inclusion $R \to S$. The ideal $C = (Y)R = (Y)S$ is isomorphic to F as an R-module and as an S-module since $XY = 0 = Y^2 = Z_iY$. For quotients, we have $A = R/C \cong F[X]$ and $B = T/C \cong F[X,Z_1,Z_2,\ldots]$; under these isomorphisms, the induced map $A \to B$ is the same as the natural inclusion $F[X] \to F[X,Z_1,Z_2,\ldots]$. The ring $F[X,Z_1,Z_2,\ldots]$ is not Noetherian and is not finitely generated as an $F[X]$-module. It follows that T is not Noetherian and is not finitely generated as an R-module.

4 Pullbacks of Prüfer Rings

In this section we consider the following six extensions of the Prüfer condition to commutative rings with zero-divisors and investigate their behavior in the conductor square ($\square$).

Definition 4.1. A *fractional ideal* of a commutative ring R is an R-submodule of the total quotient ring $Q(R)$, possibly zero and possibly non-finitely generated. An ideal $I \subseteq R$ is *invertible* if there is a fractional ideal K such that $IK = R$.

  (i) R is *semihereditary* if every finitely generated ideal of R is projective.

 (ii) R has *weak global dimension* ≤ 1 if every finitely generated ideal of R is flat.

(iii) R is *arithmetical* if its lattice of ideals is distributive.

 (iv) R is *Gaussian* if for every $f, g \in R[X]$, one has the content ideal equation $c(fg) = c(f)c(g)$.

---

[1] This is well known, but we do not know of a proper reference. To explain this fact, consider the induced ring homomorphism $F[X]_{(X)} \to F[\![X]\!]$. Since $F[X]_{(X)}$ is not complete (with respect to the ideal-adic topology determined by its maximal ideal), we conclude from [22, Theorem B] that $F[\![X]\!]$ is not finitely generated over $F[X]_{(X)}$, so it is not finitely generated over the subring $F[X]$. Alternately, suppose that $F[\![X]\!]$ were finitely generated over $F[X]_{(X)}$. Since $F[\![X]\!]$ is flat over the local ring $F[X]_{(X)}$, it is free, so there is an $F[X]_{(X)}$-module epimorphism $F[\![X]\!] \twoheadrightarrow F[X]_{(X)}$. Since $F[\![X]\!]$ is finitely generated over $F[X]_{(X)}$, it follows that $F[X]_{(X)}$ is complete, a contradiction.

 (v) R is *locally Prüfer* if R_P is a *Prüfer ring* (see condition (vi)) for every prime
       ideal M of R.
 (vi) R is *Prüfer* if every finitely generated regular ideal is invertible.
We say that R satisfies *Prüfer condition* (n) when R satisfies condition (n) from the
above list.

It is worth noting that the definitions above are equivalent when R is a domain.
Also, for non-domains, to verify locally Prüfer, it is not enough to check localizations
at maximal ideals; see [5, Example 2.4].

The following characterizations of Prüfer rings will be quite useful for us. The proof
is straightforward.

Lemma 4.2. *Let R be any commutative ring.*
  (i) *If I is finitely generated and regular then: I is invertible if and only if I is
        projective if and only if I is locally principal.*
 (ii) *If every 2-generated ideal of R is locally principal, then every finitely generated
        ideal of R is locally principal.*
(iii) *If R is local, then R is Prüfer if and only if every 2-generated regular ideal is
        principal.*
(iv) *The ring R is Prüfer if and only if every 2-generated regular ideal is locally
        principal.*

The papers [2, 6] also show that the implications in the next result are strict.

Theorem 4.3 ([2, for $n =$ i, ii, iii, iv] and [6, Theorem 2.2 for $n =$ iv, v, vi]). *For
any commutative ring, we have the following implications for Prüfer condition (n):*
(i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (v) $\Rightarrow$ (vi).

The next result relates the Prüfer condition of a ring with its total quotient ring. It is
crucial for the main theorem of this section.

Theorem 4.4 ([3, Theorems 3.7 and 3.12 for $n =$ i, ii, iii, iv, v, vi] and [6, Theorem
3.4 for $n = 5$]). *Let R be any commutative ring. Then R has Prüfer condition (n) if
and only if R is a Prüfer ring and $Q(R)$ has Prüfer condition (n).*

Use the fact that every overring of a Prüfer ring is again a Prüfer ring (see for exam-
ple [31, Theorem 10.19]) together with Theorem 4.4 to obtain the following.

Lemma 4.5. *Let R be any commutative ring. If R has Prüfer condition (n) and if T is
an overring of R, then T has the same Prüfer condition (n).*

The next result gives more information about overrings in the local case.

Lemma 4.6 ([5, Theorem 3.6]). *Let R be any local commutative ring. If R has Prüfer
condition (n) and if T is an overring of R, then T is a local ring with Prüfer condition
(n). Moreover, $T = R_P$ for some prime ideal P of R.*

The next result shows that all of the Prüfer conditions are in fact well behaved in (□) in the local case. Note that the cases $n = $ v and $n = $ vi are equivalent in the local case.

Theorem 4.7 ([5, Theorem 4.1]). *Consider the regular conductor square* (□). *The commutative ring R is a local ring with Prüfer condition* (n) *if and only if T is a local ring with Prüfer condition* (n), *A is a local Prüfer ring, and B is an overring of A.*

In the next result, we say that B is *locally an overring of A* if for every prime $P \in \operatorname{Spec}(A)$ the localization B_P is an overring of A_P. Note that the cases $n = $ i, ii, ii, iv are from [5, Theorem 4.2], but our proof works equally well for all cases.

Theorem 4.8. *Consider the regular conductor square* (□). *For $n = $ i, ii, ii, iv, v, the ring R has Prüfer condition* (n) *if and only if T has Prüfer condition* (n), *A is locally Prüfer, and B is locally an overring of A.*

Proof. ($\Rightarrow$) Assume that R has Prüfer condition (n). The fact that T has Prüfer condition (n) follows from Proposition 2.5 (i) and Lemma 4.5. Since $n \in \{$i, ii, iii, iv, v$\}$, we conclude that R is locally Prüfer by the implication (n) $\Rightarrow$ (v) in Theorem 4.3. To complete this implication, let $P \in \operatorname{Spec}(A)$, and let $\mathfrak{P}$ be the contraction of P in R along the surjection $R \twoheadrightarrow A$. It follows that the localization (□$_\mathfrak{P}$) is a regular conductor square such that $R_\mathfrak{P}$ is Prüfer. From Theorem 4.7, it follows that $A_P = A_\mathfrak{P}$ is Prüfer and B_P is an overring of A_P. We conclude that A is locally Prüfer and B is locally an overring of A.

($\Leftarrow$) Assume that T has Prüfer condition (n), A is locally Prüfer, and B is locally an overring of A. Since $n \in \{$i, ii, iii, iv, v$\}$, we conclude that T is locally Prüfer by the implication (n) $\Rightarrow$ (v) in Theorem 4.3.

We claim that R is locally Prüfer. To see this, let $\mathfrak{P} \in \operatorname{Spec}(R)$. If $C \nsubseteq \mathfrak{P}$ then, by Lemma 2.1 (ii), there is a prime ideal $\mathfrak{Q} \subset T$ such that $R_\mathfrak{P} \simeq T_\mathfrak{Q}$; since T is locally Prüfer, the ring $R_\mathfrak{P} \simeq T_\mathfrak{Q}$ is Prüfer. Assume that $C \subseteq \mathfrak{P}$. In this case, we have the regular conductor square (□$_\mathfrak{P}$). Since $A_\mathfrak{P}$ is a local Prüfer ring and $B_\mathfrak{P}$ is an overring of $A_\mathfrak{P}$, Lemma 4.6 implies that $B_\mathfrak{P}$ is a local Prüfer ring. Thus, Proposition 2.3 (i) implies that $T_\mathfrak{P}$ is local. Since T is locally Prüfer, the ring $T_\mathfrak{P}$ is Prüfer. An application of Theorem 4.7 to the conductor square (□$_\mathfrak{P}$) implies that $R_\mathfrak{P}$ is Prüfer. This establishes the claim.

The claim implies that R is Prüfer because of the implication (v) $\Rightarrow$ (vi) in Theorem 4.3. The ring T is an overring of R by Proposition 2.5 (i), so we have $Q(R) = Q(T)$. Since T has Prüfer condition (n), we conclude from Theorem 4.4 that $Q(R) = Q(T)$ has Prüfer condition (n). The fact that R is Prüfer then implies that R has Prüfer condition (n) by another application of Theorem 4.4.   □

Question 4.9. Does the conclusion of Theorem 4.8 hold for $n = $ vi?

5 Pullbacks of Coherent Rings

We refer the reader to [27] for more background information on coherent rings, including unspecified terminology.

Definition 5.1. Let R be any commutative ring.

  (i) An R-module M is *coherent* if it is finitely generated and if every finitely generated R-submodule of M is finitely presented.

 (ii) The ring R is *coherent* if it is coherent as an R-module.

It is well known that every Noetherian ring is coherent, as is every Prüfer domain. Moreover, every semihereditary ring is coherent.

To discuss the behavior of coherence in conductor squares, we recall some facts about coherent rings.

Theorem 5.2 ([27, Theorem 4.1.1]). *Let $\phi\colon R \to T$ be any homomorphism of commutative rings making T into a finitely presented R-module. (For instance, this is the case when $T \cong R/I$ where I is a finitely generated ideal of R.) If R is coherent, then so is S. The converse holds when ϕ is injective.*

The next result represents the first progress on the transference of the coherent property for conductor squares outside of the $D + M$ setting. Note that the term "epimorphism" is used in a category-theory sense, as in [27] ; in particular, an epimorphism of commutative rings need not be surjective.

Theorem 5.3 ([27, Theorems 4.1.4 and 5.1.3]). *Given the conductor square* ($\square$)*, suppose that $R \hookrightarrow T$ is a flat epimorphism and that C is flat as an R-module.*

  (i) *If R is coherent, then so is T.*

 (ii) *If A, T are coherent and C is a maximal ideal of T, then R is coherent.*

(iii) *If A is coherent such that wk.gl.dim.$(A) \leq \infty$ and if T is semihereditary, then R is coherent.*

(iv) *If A is Noetherian and T is coherent, then R is coherent.*

To continue our survey of coherence, we need a few more definitions.

Definition 5.4. Let D be any integral domain with quotient field K.

  (i) The *inverse* of a fractional ideal I is the fractional ideal $I^{-1} = (D : I) = \{x \in K \mid xI \subseteq D\}$.

 (ii) A fractional ideal I is *divisorial* if $I = (I^{-1})^{-1}$.

(iii) The *v-closure* of a fractional ideal I is $I_v = (I^{-1})^{-1}$. (This is also called the "v divisorial closure" of I.)

(iv) A fractional ideal I is *v-invertible* if $(II^{-1})_v = D$.

(v) A fractional ideal I is *v-finite* if $I^{-1} = J^{-1}$ for some finitely generated fractional ideal J of D.

(vi) The *t-closure* of a fractional ideal I is $I_t = \bigcup\{J_v \mid J$ is a finitely generated fractional subideal of $I\}$.

(vii) A fractional ideal I is *t-invertible* if $(II^{-1})_t = D$.

We now recall several coherent-like properties studied in [24].

Definition 5.5. An integral domain D is

(i) *quasicoherent* if every finitely generated ideal I of D has the property that I^{-1} is finitely generated.

(ii) a *v-coherent* if every finitely generated ideal I of D has the property that I^{-1} is *v*-finite.

(iii) a *finite conductor domain* if the intersection of any two principal ideals of D is finitely generated.

(iv) a *Prüfer v-multiplication domain* (PVMD) if every finitely generated ideal of D is *t*-invertible.

(v) a *v-domain* if every finitely generated ideal of D is *v*-invertible.

(vi) a *DVF domain* if every divisorial ideal of D is *v*-finite.

(vii) a *Mori domain* if it satisfies the ascending chain condition on divisorial ideals.

We summarize the relations between these conditions (from [24]) next:

$$\text{coherent} \implies \text{quasicoherent} \implies \text{finite conductor}$$
$$\Downarrow$$
$$v\text{-domain} \impliedby \text{PVMD} \implies v\text{-coherent} \impliedby \text{DVF} \impliedby \text{Mori}.$$

The transference of these coherent-like properties in a special case of ($\square$) is well-studied in [24]. We list the main results of that paper in the three theorems that follow.

Theorem 5.6. *Consider the conductor square ($\square$) such that R and T are domains, $Q(A) = B$, and C is a maximal ideal of T.*

(i) *[24, Theorem 3.4] The ring R is v-coherent if and only if A and T are v-coherent and C is a t-ideal of T.*

(ii) *[24, Theorem 4.7] The ring R is (quasi)coherent if and only if A and T are (quasi)coherent and T_C is a valuation domain.*

(iii) [24, Theorem 4.8] *The ring R is a finite conductor domain if and only if A and T are finite conductor domains and T_C is a valuation domain.*

(iv) [24, Theorem 4.20 (1)] *If T is local, then R is a DVF domain if and only if A and T are DVF domains and C is a nonprincipal v-finite divisorial ideal of T.*

Theorem 5.7. *Consider the conductor square $(\square)$ such that R and T are domains, $Q(A) \neq B$, and C is a maximal ideal of T, so B is a field.*

(i) [24, Theorem 3.5] *The ring R is v-coherent if and only if A and T are v-coherent and either C is not a t-ideal of T or C is a v-finite divisorial ideal of T.*

(ii) [24, Theorems 4.9 and 4.11] *The ring R is (quasi)coherent if and only if T is (quasi)coherent, A is a field with $[B : A] < \infty$, and C is a finitely generated ideal of T.*

(iii) [24, Theorem 4.10] *The ring R is a finite conductor domain if and only if T is a finite conductor domain, A is a field with $[B : A] < \infty$, and C is a finitely generated ideal of T.*

(iv) [24, Theorem 4.20(2)] *If T is local, then R is a DVF domain if and only if A and T are DVF domains and either C is not a t-ideal of T or C is a v-finite divisorial ideal of T.*

Theorem 5.8. *Consider the conductor square $(\square)$ where R and T are domains and C is a maximal ideal of T.*

(i) [20, Theorem 4.1] *The ring R is a PVMD if and only if A and T are PVMDs, $Q(A) = B$, and T_C is a valuation domain.*

(ii) [24, Theorem 4.15] *The ring R is a v-domain if and only if A and T are v-domains, $Q(A) = B$, and T_C is a valuation domain.*

(iii) [24, Theorem 4.18] *The ring R is a Mori domain if and only if T is a Mori domain and A is a field.*

The final result of this section characterizes the coherency of R in a regular conductor square $(\square)$.

Theorem 5.9. *Consider the conductor square $(\square)$ and the following conditions:*

(i) *The ring R is coherent and the extension $R \hookrightarrow T$ is finite.*

(ii) *The rings A, T, and B are coherent, B is finitely presented over A, and T is finitely presented over R.*

(iii) *The rings A and T are coherent and T is finitely presented over R.*

(iv) *The rings A and T are coherent and B is finitely presented over A.*

The following hold:

(a) *The implications* (iv) $\Leftarrow$ (iii) $\Leftrightarrow$ (ii) $\Rightarrow$ (i) *always hold.*

(b) *If C is finitely generated over R or over T, then we have* (iv) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (ii) $\Rightarrow$ (i).

(c) *If the conductor square* ($\square$) *is regular and C is finitely generated over R or over T, then the conditions* (i)–(iv) *are equivalent.*

Proof. (a) The implication (ii) $\Rightarrow$ (iii) is trivial, and (iii) $\Rightarrow$ (iv) is from Lemma 2.2 (i). For (iii) $\Rightarrow$ (ii), use Lemma 2.2 (i) to conclude that B is finitely presented over A, and use Theorem 5.2 to show that B is coherent. The implication (ii) $\Rightarrow$ (i) also follows from Theorem 5.2, using the fact that T finitely presented over R implies that T is finitely generated over R, by definition.

(b) Assume that C is finitely generated over R or T. We need to show (iv) $\Rightarrow$ (iii), so assume that A and T are coherent and B is finitely presented over A. Lemma 2.1 (v) implies that T is finitely generated over R, thus C is finitely generated over R and over T by Lemma 2.1 (iv). Since T is coherent and C is finitely generated over T, it follows that C is finitely presented over T, and we conclude that T is finitely presented over R by Lemma 2.2 (ii).

(c) Assume that the conductor square ($\square$) is regular and C is finitely generated over R or over T. We need to prove that (i) $\Rightarrow$ (ii), so we assume that R is coherent and the extension $R \hookrightarrow T$ is finite. Lemma 2.1 (iv) implies that C is finitely generated over R and over T. By Proposition 2.5 (ii), the R-module T is isomorphic to an ideal of R. Since T is a finitely generated over the coherent ring R, we conclude that T is finitely presented over R. Theorem 5.2 implies that T is coherent, and that $A = R/C$ is coherent. $\square$

6 The *n*-generator Property in Pullbacks

This section is devoted to the behavior of the (strong) n-generator property in the conductor square ($\square$). We recall the following definitions.

Definition 6.1. Let R be any commutative ring.

(i) An ideal I of R is *n-generated* if there exist $a_1, \ldots, a_n \in I$ such that $I = (a_1, \ldots, a_n)$.

(ii) An ideal I of R is *strongly n-generated* if for every nonzero $a \in I$, there exist $a_1, \ldots, a_{n-1} \in I$ such that $I = (a, a_1, \ldots, a_{n-1})$. It is also common to say that I is "$(n-1)\frac{1}{2}$-generated."

(iii) The ring R is said to have the *(strong) n-generator property* if every finitely generated ideal is (strongly) n-generated.

We record some familiar examples here.

Example 6.2. (i) A domain has the 1-generator property if and only if it is Bézout, by definition. In particular principal ideal domains have the 1-generator property.

(ii) Every Prüfer domain of finite character has the strong 2-generator property. In particular, Dedekind domains have the strong 2-generator property. See [23, Theorem 2.2 (a)].

(iii) Every integrally closed domain with the 2-generator property is a Prüfer domain by [23, Proposition 1.11].

(iv) It is routine to show that if a commutative ring S has the strong n-generator property ($n \geq 2$), then any proper homomorphic image of S must have the $(n-1)$-generator property.

As best we know, there are no comprehensive theorems in the literature regarding the transference of the n-generator property in the most general setting of ($\square$). For example, the proof of Theorem 1.1 (iv) relies heavily on the fact that T contains a retract field. In the theorem that follows, the retract condition in T is dropped.

Theorem 6.3 ([28, Theorem]). *Suppose that C is a maximal ideal in the conductor square ($\square$) and let $I \nsubseteq C$ be an ideal of R. If IA is an n-generated ideal of A and if IT is an m-generated ideal of T, then I is $\max\{2, n, m\}$-generated.*

In order to study the n-generator property in a conductor square of the type ($\square$) where C is not a prime ideal, we put a strong condition on the ring T making it a PID. In doing so, we are able to give some partial results regarding the transference of the (strong) n-generator property in a conductor square ($\square$) where C is a finite intersection of maximal ideals. The set up for these results is next.

Definition 6.4. Let D be an integral domain that is not a field. Let K be its field of fractions. In the diagram ($\square$) above, we set $T = K[X]$ and $C = F_1 \cdots F_r K[X]$ where $F_1, \ldots, F_r$ are irreducible polynomials over the field K that are pairwise coprime in $K[X]$. Now we have that $B = \prod_{i=1}^r K[\theta_i]$ where, for each index $i \leq r$, the element θ_i is a root of F_i in some extension field of K. If D_i is any subring of $K[\theta_i]$ that contains $D[\theta_i]$, then a conductor square ($\square$) with $A = \prod_{i=1}^r D_i$ yields a ring R between $D[X]$ and $K[X]$ with a non-zero conductor from $K[X]$ into R.

$$
\begin{array}{ccc}
R & \lhook\joinrel\longrightarrow & K[X] \\
\downarrow & & \downarrow \\
\prod_{i=1}^r D_i & \lhook\joinrel\longrightarrow & \prod_{i=1}^r K[\theta_i]
\end{array}
\qquad (\boxtimes)
$$

In this case we will say that *R is defined by a conductor square of the type* ($\boxtimes$). It is worth noting that one can assume without loss of generality in this construction that each F_i is monic with coefficients in D.

Example 6.5. Let D be an integral domain with field of fractions K and let $E = \{e_1, \ldots, e_r\}$ be any finite subset of D. As noted in the introduction, setting $C = (X - e_1) \cdots (X - e_r) K[X]$ and $A = \prod_{i=1}^{r} D$, we find that $R = \mathrm{Int}(E, D) = \{g \in K[X] \mid g(E) \subset D\}$, the ring of integer-valued polynomials on D determined by the subset E, is defined by a conductor square of the type ($\boxtimes$).

More generally, it was observed by Elliot [19, Proposition 6.1] that $\mathrm{Int}(S, D)$ is defined by the conductor square ($\square$) where S is any subset of D, $T = K[X]$, $B = K^S$, the map $T \twoheadrightarrow B$ is evaluation at S, and $A = D^S$.

Next, we generalize some definitions made for the ring $\mathrm{Int}(E, D)$ where E is a finite subset of D. For more information on the various Skolem properties, see [11].

Definition 6.6. Suppose that R is a domain defined by a conductor square of type ($\boxtimes$).

  (i) We call an ideal $U \subseteq R$ *unitary* if $U \cap D \neq 0$. It is straightforward to show that an ideal U is unitary if and only if $UK[X] = K[X]$ if and only if $U \cap K \neq 0$.

 (ii) For each subset $I \subseteq K[X]$ and each element $\theta \in F$ where F is an extension field of K, set $I(\theta) = \{g(\theta) \mid g \in I\} \subseteq F$. Note that in a conductor square of type ($\boxtimes$), the set $I(\theta_i)$ is an ideal of D_i, moreover it is the ideal ID_i.

(iii) We say that the domain R has the *almost strong super Skolem property* if, for every pair of unitary ideals $U, V \subseteq R$ and every index $k \leq r$, one has $U = V$ if and only if $U(\theta_k) = V(\theta_k)$.[2]

The point of the next few results is to remove the Prüfer assumption from several results of [4]. We begin with [4, Theorem 5.4].

Theorem 6.7 ([4, Theorem 5.4]). *Suppose that R is a domain defined by a conductor square of the type ($\boxtimes$). Then R has the almost strong super Skolem property.*

Proof. Let U and V be unitary ideals of R such that $U(\theta_i) = V(\theta_i)$ for $i = 1, \ldots, r$.
Claim 1. $C \subseteq U \cap V$. (Compare to [4, Lemma 5.2].) We show that $C \subseteq U$; the containment $C \subseteq V$ then follows by symmetry. Let $g \in C$. Since U is unitary, there is a non-zero element $d \in U \cap D$. Since d is a non-zero constant in $K[X]$, we have $g/d \in K[X]$. Furthermore, we have $(g/d)(\theta_i) = g(\theta_i)/d = 0$ since d is constant and F_i divides g. By definition, this means that $g/d \in R$, so the condition $d \in U$ implies that $g = d(g/d) \in dR \subseteq U$, as desired.
Claim 2. For any ideal $I \subseteq R$, we have $IA = (I + C)/C = \bigoplus_{i=1}^{r} I(\theta_i)$. (Compare to [4, Lemma 5.3].) By definition, we have $A = \prod_{i=1}^{r} D_i \cong R/C$, hence the equality $IA = (I + C)/C$. Since the map $R \to A$ is given by $f \mapsto (f(\theta_1), \ldots, f(\theta_r))$, the containment $IA \subseteq \bigoplus_{i=1}^{r} I(\theta_i)$ is routine. For the reverse containment, let $x = (f_1(\theta_1), \ldots, f_r(\theta_r)) \in \bigoplus_{i=1}^{r} I(\theta_i)$ with each $f_i \in I$. Let $e_1, \ldots, e_r \in \prod_i D_i$ denote

---

[2] Note that this differs from the terminology used in [4], but is consistent with [11].

the primitive idempotents, and fix liftings $t_1, \ldots, t_r \in R$. By assumption, this implies that $t_i(\theta_j) = \delta_{ij}$, the Kroenecker delta. The element $f = \sum_i t_i f_i$ is in I, since each f_i is in I, and the image of f in $\prod_i D_i$ is $\sum_i e_i f_i(\theta_i) = x$, so we have $x \in IA$, as desired.

To complete the proof of the theorem, note that the assumption $U(\theta_i) = V(\theta_i)$ for $i = 1, \ldots, r$ explains the second equality in the following display

$$U/C = UA = \bigoplus_{i=1}^{r} U(\theta_i) = \bigoplus_{i=1}^{r} V(\theta_i) = VA = V/C.$$

The other equalities are from Claims 1 and 2. It follows that $U = V$, as desired.   □

The almost strong super Skolem property guaranteed by the previous result is key for the proof of the next theorem, which in turn yields the two subsequent results. Compare to [4, Theorems 6.2 and 6.3, and Corollary 6.4].

Theorem 6.8. *Let R be a domain defined by a conductor square of the type* (⊠), *and let $U \subseteq R$ be a unitary ideal.*

(i) *U is principal if and only if there is a non-zero $v \in U \cap K$ such that $U = Rv$ if and only if there is a non-zero $v \in U \cap K$ such that $U(\theta_k) = D_k v$ for each $k \leq r$.*

(ii) *U is strongly 2-generated if and only if $U(\theta_k)$ is principal for each $k \leq r$.*

(iii) *For $n \geq 2$, the ideal U is strongly $(n + 1)$-generated if and only if U is n-generated if and only if $U(\theta_k)$ is n-generated for all $k \leq r$.*

Proof. (i) If there is a non-zero $v \in U \cap K$ such that $U = Rv$, then U is principal and $U(\theta_k) = D_k v$ for each $k \leq r$. If U is principal and unitary, write $U = Rv$ for some $v \in U$. The unitary condition implies that $K[X] = UK[X] = vK[X]$, and it follows that v is a constant in $K[X]$, so $v \in K \cap U$.

Assume that there is a non-zero $v \in K \cap U$ such that $U(\theta_k) = D_k v$ for $k = 1, \ldots, r$. Set $V = Rv$, and observe that V is necessarily unitary since $v \in V \cap K$. For each index $k \leq r$, we have $V(\theta_k) = D_k v = U(\theta_k)$. Theorem 6.7 implies that $U = V = Rv$.

(ii) ($\Rightarrow$) If U is strongly 2-generated, then its homomorphic image $U(\theta_k)$ is principal in the proper quotient D_k by Example 6.2 (iv).

($\Leftarrow$) Choose any non-zero $f \in U$. Since each $U(\theta_k)$ is principal, we can write $\overline{U} = \prod_{k=1}^{r} D_k d_k$, where each $d_k \in D_k$; moreover, there exist polynomials $r_k \in R$ such that $r_k(\theta_k) = d_k$. Now, form the polynomial $g = \sum_{k=1}^{r} r_k e_k$, where each $\overline{e_k} \in \prod_i D_i$ is the primitive idempotent corresponding to D_k, and set $V' = Rf + Rg$.

If V' is unitary then $V'(\theta_k) = D_k f(\theta_k) + D_k d_k = D_k d_k = U(\theta_k)$, and we are done by Theorem 6.7. If not, then we show (as in [13, Theorem 4]) how to find a polynomial $h \in K[X]$ such that $g' = g + h F_1 \cdots F_r$ is relatively prime to f in $K[X]$;

once this is shown, then $g'(\theta_k) = g(\theta_k) = d_k \in D_k$ for each index k, which implies that $g' \in R$ and $V = Rf + Rg'$ is unitary, so again Theorem 6.7 ensures that $U = V$.

Note that the fact that U is unitary implies that $U(\theta_k) \neq 0$ for each k, so $d_k \neq 0$ and it follows that g is relatively prime to $F_1 \cdots F_r$. Write $f = f_1 h$ where f_1 and h are relatively prime, each irreducible factor of f_1 divides g, and each irreducible factor of h does not divide g. To show that f and $g' = g + hF_1 \cdots F_r$ are relatively prime in $K[X]$, we let $p \in K[X]$ be an irreducible factor of f and show that p does not divide g'. Since p divides $f = f_1 h$, there are two cases.

Case 1: $p \mid f_1$. In this case, we have $p \mid g$ and $p \nmid h$ by construction of f_1. Since g is relatively prime to $F_1 \cdots F_r$ and $p \mid g$, we have $p \nmid F_1 \cdots F_r$, so $p \nmid hF_1 \cdots F_r$ and $p \nmid g + hF_1 \cdots F_r = g'$.

Case 2: $p \mid h$. In this case, we have $p \nmid g$ by construction of h. Since $p \mid h$, we have $p \mid hF_1 \cdots F_r$, so $p \nmid g + hF_1 \cdots F_r = g'$.

(iii) Certainly if U is n-generated, then it is strongly $(n + 1)$-generated, and if U is strongly $(n + 1)$-generated, then each of the proper homomorphic images $U(\theta_k)$ is n-generated by Example 6.2 (iv). Thus, we assume that $n \geq 2$ and that each $U(\theta_k)$ is n-generated. It suffices to prove that U is also n-generated. Write $U(\theta_k) = D_k d_{1,k} + \cdots + D_k d_{n,k}$; then for each index $k \leq r$, there exist polynomials $a_{i,k} \in R$ such that $a_{i,k}(\theta_k) = d_{i,k}$. Since U is unitary, we have $U(\theta_k) \neq 0$ for each k, so we have $d_{j,k} \neq 0$ for some j. Reorder the $d_{i,k}$ if necessary to assume that $d_{1,k} \neq 0$ for each k. As in [9, Theorem 3], for each $i \leq n$ put $g_i = a_{i,1} e_1 + \cdots + a_{i,r} e_r$, where $\overline{e_k} \in \prod_i D_i$ is the primitive idempotent corresponding to D_k for all $k \leq r$, and set $V = Rg_1 + \cdots + Rg_n$. Note that $g_1(\theta_k) = d_{i,k} \neq 0$ for all k.

If V is unitary, then the condition $U(\theta_k) = V(\theta_k)$ for each $k \leq r$ implies that $U = V$, by Theorem 6.7. If V is not unitary, then, as above, we can find a polynomial $h \in K[X]$ such that $g_1' = g_1 + hF_1 \cdots F_r$ is relatively prime to g_2 in $K[X]$. It follows that $V' = Rg_1' + Rg_2 + \cdots + Rg_n$ is unitary and that $U(\theta_k) = V'(\theta_k)$ for each index $k \leq r$. Again by Theorem 6.7, we get that $U = V$. $\qquad\square$

As a consequence of the preceding result, we obtain the following theorem and its corollary describing the behavior of the (strong) n-generator property in a conductor square ($\boxtimes$).

Theorem 6.9. *Let R be a domain defined by a conductor square of type ($\boxtimes$).*

  (i) *If $n \geq 2$ and R has the strong n-generator property, then D_k has the $(n - 1)$-generator property for each index k.*

 (ii) *If $n \geq 2$ and D_k has the n-generator property for each index k, then R has the n-generator property.*

(iii) *The ring R has the strong 2-generator property if and only if D_k is Bézout for each index k.*

Proof. Note that every finitely generated ideal in R is isomorphic to a unitary ideal; argue as in [33] or see [7]. Thus, the desired result follows from Example 6.2 (iv) and Theorem 6.8.   □

Corollary 6.10. *If R is a domain defined by a conductor square of type ($\boxtimes$), then the following conditions are equivalent for $n \geq 2$:*

  (i) *For each index k, the ring D_k has the n-generator property.*

 (ii) *R has the n-generator property.*

(iii) *R has the strong $(n + 1)$-generator property.*

We summarize the implications from the preceding results in the next diagram.
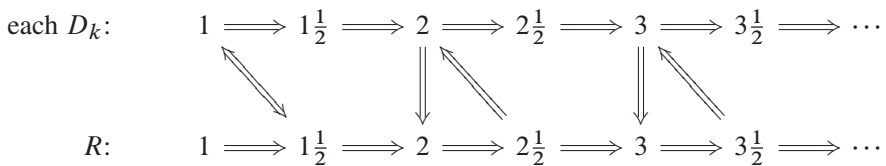
In contrast to the previous results, note that the Prüfer hypothesis in the next corollary is crucial; see Example 6.12.

Corollary 6.11 ([4, Theorem 6.6]). *If R is any Prüfer domain between $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ such that the conductor with respect to $\mathbb{Q}[X]$ is non-zero, then R has the 2-generator property.*

Proof. By [4, Proposition 4.5], the ring R is a Prüfer domain defined by a conductor square of the type ($\boxtimes$). Since R is integrally closed in $Q(R) = K(X)$, it is integrally closed in $K[X]$. It follows from [21, Lemma 1.1.4 (8)] that $\prod_k D_k$ is integrally closed in $\prod_k K[\theta_k]$, that is, that each D_k is integrally closed in its quotient field $K[\theta_k]$. The containment $\mathbb{Z}[\theta_k] \subset D_k$, implies that each D_k contains the integral closure $\mathbb{Z}_k$ of $\mathbb{Z}$ in $\mathbb{Q}[\theta_k]$. The Krull-Akizuki Theorem says that $\mathbb{Z}_k$ is a Dedekind domain. Since D_k is an overring of $\mathbb{Z}_k$, it too is a Dedekind domain by [31, Theorem 6.21] and therefore has the (strong) 2-generator property. Now apply Corollary 6.10.   □

Next, we show that, if $r = 1$ and D_1 is Bézout in the conductor square ($\boxtimes$), then R need not be Bézout, in contrast to the statement of [4, Theorem 6.3 (4)]. In particular, [4, Example 6.8 (1)] incorrectly states that the ring R in the next example is Bézout. Note that Theorem 6.9 (iii) implies that R does have the strong 2-generator property.

Example 6.12. We consider the specific conductor square

$$
\begin{array}{ccc}
R & \lhook\joinrel\longrightarrow & \mathbb{Q}[X] \\
\downarrow & & \downarrow \\
\mathbb{Z}[i] & \lhook\joinrel\longrightarrow & \mathbb{Q}[i]
\end{array}
$$

which has conductor ideal $C = (X^2 + 1)$. It is straightforward to show that $R = \mathbb{Z} + \mathbb{Z}X + (X^2 + 1)\mathbb{Q}[X]$; in other words, a polynomial $f \in \mathbb{Q}[X]$ is in R if and only if the remainder after dividing by $X^2 + 1$ is in $\mathbb{Z}[X]$. The ring $\mathbb{Z}[i]$ is Bézout. To show that R is not Bézout, we show that the ideal $U = (X + 1, X^2 + 1)R$ is not principal.

By way of contradiction, suppose that U is principal. Since the polynomials $X + 1$ and $X^2 + 1$ are relatively prime in $\mathbb{Q}[X]$, the ideal U is unitary. Theorem 6.8 (i) provides a non-zero element $c \in U \cap \mathbb{Q}$ such that $U = cR$. Since $X + 1 \in U = cR$, we have $(X + 1)/c \in R$. Given the explicit description of R, the condition $c \in R$ implies that $c \in \mathbb{Z}$, and the condition $(X + 1)/c \in R$ implies that $c = \pm 1$. We conclude that $1 = \pm c \in U = (X + 1, X^2 + 1)R$, so there are elements $p, q \in R$ such that $1 = (X + 1)p + (X^2 + 1)q$. Rewriting p and q using the explicit description of R, we conclude that there are elements $\tilde{p} \in \mathbb{Z}[X]$ and $\tilde{q} \in \mathbb{Q}[X]$ such that $1 = (X + 1)\tilde{p} + (X^2 + 1)\tilde{q}$. Evaluating at i, we obtain the equation $1 = (i + 1)\tilde{p}(i)$ which implies that $(1 - i)/2 = 1/(1 + i) = \tilde{p}(i) \in \mathbb{Z}[i]$ a contradiction.

7 Factorization in Pullbacks

In this section, we highlight a few examples in the theory of factorization supplied by pullback constructions. First we recall some relevant definitions.

Definition 7.1. Let D be any integral domain.

(i) We denote by $D^{\bullet}$ the set of all nonzero nonunits of D.

(ii) We denote by $\mathcal{A}(D)$ the set of all atoms (irreducible elements) of D.

(iii) We call D an *atomic domain* if for every $a \in D^{\bullet}$, one has a factorization $a = p_1 p_2 \cdots p_n$ where each $p_i \in \mathcal{A}(D)$ and $n \geq 1$.

(iv) We say that D is *ACCP* if it satisfies the ascending chain condition on principal ideals.

(v) We call D a *half factorial domain (HFD)* if for every $a \in D^{\bullet}$, one has a factorization $a = p_1 p_2 \cdots p_n$ where each $p_i \in \mathcal{A}(D)$ and $n \geq 1$. Moreover, if $a = q_1 q_2 \cdots q_n$ is any other such factorization, then $m = n$.

The following implications are straightforward:

$$\text{UFD} \implies \text{HFD} \implies \text{ACCP} \implies \text{Atomic}$$
$$\Uparrow$$
$$\text{Noetherian} \implies \text{Mori}$$

It is worth noting that these factorization properties are *not* well behaved in a conductor square of the type ($\square$). In fact, one of the most basic constructions $\mathbb{Z} + X\mathbb{Q}[X]$ is not even atomic [17, Exercise 9.3.4] while the rings $\mathbb{Z}$ and $\mathbb{Q}[X]$ are UFDs. More generally, if $A \subseteq B$, then $A + XB[X]$ is a UFD if and only if $A = B$ and A is a UFD. In order to investigate the weaker half factorial condition in the $A + XB[X]$ construction, [15] makes the following definitions.

Definition 7.2. Let D be any integral domain.

(i) Two nonzero elements $x, y \in D$ are called *v-coprime* if $xD \cap yD = xyD$.

(ii) A subset $S \subset D$ is called a *splitting multiplicative set* of D if every $d \in D$ is expressible as $d = st$ where $s \in S$ and t is v-coprime to every element of S.

We can now give a characterization of the HFD property in the $A + XB[X]$ construction.

Theorem 7.3 ([15, Corollary 3.5]). *Let $A \subseteq B$ be any pair of integral domains such that B has a "proper" element $b \in B$ (no unit of B multiplies b into A). In the conductor square ($\square$), set $T = B[X]$, $C = XB[X]$, and $R = A + XB[X]$. The following statements are equivalent:*

(i) $S = \{g \in R \mid g(0) \neq 0\}$ *is a splitting set of R.*

(ii) R *is an HFD and $A - \{0\}$ is a splitting set of R.*

(iii) B *is integrally closed and $A - \{0\}$ is a splitting set of R.*

Example 7.4. We use the conductor square ($\square$) to exhibit some examples in the theory of factorization.

(i) [32, Example 26] Though it is true that a domain D is a UFD if and only if $D[X]$ is a UFD, the same cannot be said about HFDs. Indeed, the ring $R = \mathbb{R} + X\mathbb{C}[X]$ is a Noetherian HFD while the polynomial ring $R[t]$ is not an HFD. For example, $X \cdot X \cdot (1 + t^2) = X^2 + X^2 t^2 = (X + iXt)(X - iXt)$ has an irreducible factorization of length 2 and of length 3.

(ii) [32, Example 27] In [14, Theorem 2.2], it is shown that if D is an integral domain such that its polynomial ring $D[X]$ is an HFD, then D must be integrally closed. However, we cannot conclude that D is completely integrally closed. Let A be any UFD and let X, Y be indeterminates. If $R = A + XA[X, Y]$, then R is an HFD and its polynomial ring $R[t]$ is an HFD as well. However, R is neither a

UFD nor completely integrally closed. For example, X, XY, XY^2 are all atoms so that $X \cdot XY^2 = X^2Y^2 = XY \cdot XY$ is not a unique factorization into atoms. Moreover, $Y \notin R$ while $XY^n \in R$ for all $n \geq 1$ so that R is not completely integrally closed.

(iii) [32, Example 25] The integral closure $\overline{D}$ of an atomic integral domain D may not be atomic. Let $\overline{\mathbb{Z}}$ denote the set of all algebraic integers and set $R = \mathbb{Z} + X\overline{\mathbb{Z}}[X]$. Then R satisfies ACCP and is therefore atomic. However, the integral closure $\overline{R} = \overline{\mathbb{Z}}[X]$ of R is not atomic.

We conclude this paper with a result that guarantees that the ring R in the conductor square (⊠) is atomic.

Theorem 7.5 ([8]). *For the conductor square* (⊠), *we set* $C = X(X-1)K[X]$, *so that* $B = K \times K$ *and* $A = D_1 \times D_2$. *Also, set* $S = \{d_1 d_2 \mid d_1 \in D_1, d_2 \in D_2\}$ *and* $\mathfrak{J}_0(R) = R \cap K$. *If the following conditions hold, then the ring* R *defined by the conductor square* (⊠) *is atomic:*

(i) $S = K$.

(ii) *Every nonunit of* $\mathfrak{J}_0(R)$ *is also a nonunit of* D_1 *and* D_2.

(iii) *The* $\mathfrak{J}_0(R)$*-modules* D_1 *and* D_2 *satisfy ACC on their cyclic submodules.*

Bibliography

[1] Anderson, D. F., Dobbs, D. E., Kabbaj, S., Mulay, S. B., Universally catenarian domains of $D + M$ type. Proc Amer Math Soc. 1988;104:378–384.

[2] Bazzoni, S., Glaz, S., Prüfer rings. In: Multiplicative ideal theory in commutative algebra. New York: Springer; 2006. p. 55–72.

[3] ———, Gaussian properties of total rings of quotients. J Algebra. 2007;310:180–193.

[4] Boynton, J., Pullbacks of arithmetical rings. Comm Algebra. 2007;35:2671–2684.

[5] ———, Pullbacks of Prüfer rings. J Algebra. 2008;320:2559–2566.

[6] ———, Prüfer properties and the total quotient ring. Comm Algebra. 2011;39:1624–1630.

[7] Boynton, J., Chapman, S. T., Rings of integer-valued polynomials determined by finite subsets. In preparation.

[8] Boynton, J., Coykendall, J., Another example of an atomic integral domain that is not ACCP. In preparation.

[9] Boynton, J., Klingler, L., The n-generator property in rings of integer-valued polynomials determined by finite sets. Arch Math (Basel). 2006;86:36–42.

[10] Brewer, J. W., Rutter, E. A., $D+M$ constructions with general overrings. Michigan Math J. 1976;23:33–42.

[11] Cahen, P.-J., Chabert, J.-L., Skolem properties and integer-valued polynomials: a survey. Proceedings, Advances in Commutative Ring Theory; 1997, Fez. vol. 205 of Lecture notes in pure and applied mathematics. New York: Dekker; 1999. p. 175–195.

[12] Chapman, S. T., Glaz, S., One hundred problems in commutative ring theory. In: Non-Noetherian commutative ring theory. vol. 520 of Mathematics and its applications. Dordrecht: Kluwer Acad. Publ.; 2000. p. 459–476.

[13] Chapman, S. T., Loper, A., Smith, W. W., The strong two-generator property in rings of integer-valued polynomials determined by finite sets. Arch Math (Basel). 2002;78: 372–377.

[14] Coykendall, J., A characterization of polynomial rings with the half-factorial property. Proceedings, Factorization in Integral Domains; 1996, Iowa City, IA. vol. 189 of Lecture notes in pure and applied mathematics. New York: Dekker; 1997. p. 291–294.

[15] Coykendall, J., Dumitrescu, T., Zafrullah, M., The half-factorial property and domains of the form $A + XB[X]$. Houston J Math. 2006;32:33–46 [electronic].

[16] Dobbs, D. E., Papick, I. J., When is $D + M$ coherent?. Proc Amer Math Soc. 1976;56: 51–54.

[17] Dummit, D. S., Foote, R. M., Abstract algebra. Englewood Cliffs, NJ: Prentice Hall Inc.; 1991.

[18] Eakin Jr, P. M., The converse to a well known theorem on Noetherian rings. Math Ann. 1968;177:278–282.

[19] Elliott, J., Some new approaches to integer-valued polynomial rings. In: Commutative algebra and its applications. Berlin: Walter de Gruyter; 2009. p. 223–237.

[20] Fontana, M., Gabelli, S., On the class group and the local class group of a pullback. J Algebra. 1996;181:803–835.

[21] Fontana, M., Huckaba, J. A., Papick, I. J., Prüfer domains. vol. 203 of Monographs and textbooks in pure and applied mathematics. New York: Marcel Dekker Inc.; 1997.

[22] Frankild, A. J., Sather-Wagstaff, S., Detecting completeness from Ext-vanishing. Proc Amer Math Soc. 2008;136:2303–2312.

[23] Fuchs, L., Salce, L., Modules over non-Noetherian domains. vol. 84 of Mathematical surveys and monographs. Providence, RI: American Mathematical Society; 2001.

[24] Gabelli, S., Houston, E., Coherentlike conditions in pullbacks. Michigan Math J. 1997; 44:99–123.

[25] _____ , Ideal theory in pullbacks. In: Non-Noetherian commutative ring theory. vol. 520 of Mathematics and its applications. Dordrecht: Kluwer Acad. Publ.; 2000. p. 199–227.

[26] Gilmer, R. W., Multiplicative ideal theory. vol. 12 of Queen's papers in pure and applied mathematics. Kingston, ON: Queen's University; 1968.

[27] Glaz, S., Commutative coherent rings. vol. 1371 of Lecture notes in mathematics. Berlin: Springer-Verlag; 1989.

[28] Houston, E., Generating ideals in pullbacks. J Commut Algebra. 2009;1:275–281.

[29] Kabbaj, S., On the dimension theory of polynomial rings over pullbacks. In: Multiplicative ideal theory in commutative algebra. New York: Springer; 2006. p. 263–277.

[30] Krull, W., Beiträge zur Arithmetik kommutativer Integritätsbereiche. II. v-Ideale und vollständig abgeschlossene Integritätsbereiche. Math Z. 1936;41:665–679.

[31] Larsen, M. D., McCarthy, P. J., Multiplicative theory of ideals. vol. 43 of Pure and applied mathematics. New York: Academic Press; 1971.

[32] Lucas, T. G., Examples built with $D + M$, $A + XB[X]$ and other pullback constructions. In: Non-Noetherian commutative ring theory. vol. 520 of Mathematics and its applications. Dordrecht: Kluwer Acad. Publ.; 2000. p. 341–368.

[33] McQuillan, D. L., Rings of integer-valued polynomials determined by finite sets. Proc R Ir Acad Sect A. 1985;85:177–184.

[34] Rotman, J. J., An introduction to homological algebra. vol. 85 of Pure and applied mathematics. New York: Academic Press Inc. [Harcourt Brace Jovanovich Publishers]; 1979.

[35] Seidenberg, A., On the dimension theory of rings. II. Pacific J Math. 1954;4:603–614.

Author Information

Jason G. Boynton, Department of Mathematics, North Dakota State University, Fargo, ND, USA.
E-mail: jason.boynton@ndsu.edu

Sean Sather-Wagstaff, Department of Mathematics, North Dakota State University, Fargo, ND, USA.
E-mail: sean.sather-wagstaff@ndsu.edu

Noetherian Rings without Finite Normalization

Bruce Olberding

Abstract. A number of examples and constructions of local Noetherian domains without finite normalization have been exhibited over the last seventy-five years. We discuss some of these examples, as well as the theory behind them.

1 Introduction

The publication of Emmy Noether's seminal works of 1921 and 1927 on ideal decompositions led to a number of fundamental properties of Noetherian rings being swiftly established. Within five years of the second of these articles, Ore remarked in a survey on ideal theory, perhaps a bit optimistically: "The theory itself to a large extent is still in an evolutionary stage and has not reached the harmonious form it will probably assume later on. Only for domains in which the finite chain condition [i.e., ascending chain condition] holds does it seem to have arrived at some degree of perfection" [47, page 728]. Five years later, in a review of Krull's *Idealtheorie*, he would refer to "the maze of material accumulated in recent years in the field of abstract ideal theory" [48, page 460]. In these two articles, Noether introduced the ascending chain condition to axiomatize the ideal theory of finitely generated algebras over a field and orders in algebraic number fields. The importance of local rings, as well as their completions, was quickly realized and emphasized by Krull [21] and Chevalley [7]. Shortly thereafter, in 1946, Cohen provided a structure theory for complete local rings: Every such ring is the homomorphic image of a power series ring over a field or a rank one discrete valuation ring [9]. Thus, locally and at the limit, Noetherian rings behave like the rings arising from the geometric and arithmetic contexts which Noether sought to capture with the axiom of the ascending chain condition.

However, non-complete local Noetherian rings prove to be more elusive and capable of betraying the geometric and arithmetic intuition in which the theory is rooted, and over the ninety years since the introduction of the ascending chain condition into commutative ideal theory, there has developed along with the axiomatic theory a large bestiary of examples that behave in one fundamental way or another differently than the "standard" rings that motivate and drive the subject. Thus the need for additional hypotheses such as "excellence" to capture, for example, geometric features like desin-

gularization [27]. Similarly, there are a number of penetrating variations on excellence, such as G-rings, Japanese rings, Nagata rings and geometric rings. Miles Reid comments on the delicacy of this part of the theory: "Grothendieck (in [15, IV$_2$, 7.8]) has developed the theory of 'excellent rings' (following Akizuki, Zariski and Nagata), that assembles everything you might ever need as a list of extra axioms, but it seems that this will always remain an obscure appendix in the final chapter of commutative algebra textbooks: 'Le lecteur notera que le résultats les plus delicates du §7 ne serviront qu'assez peu dans la suite' " [54, page 136].

Nevertheless, regardless of whether one views these issues as foundational or obscure, there do exist Noetherian rings at a far remove from excellence. Unlike complete local rings, these rings behave in essential ways differently than rings in arithmetic and geometric applications. Such rings earn the appellation "bad" in Nagata's famous appendix to his 1962 monograph, *Local rings.* As early as 1935, bad Noetherian rings were known: in that year Akizuki and Schmidt each published examples of bad one-dimensional local Noetherian domains. What made their examples bad was the failure to have *finite normalization*; that is, the integral closure of the ring in its total quotient ring is not a finitely generated module over the base ring. We discuss the examples of Akizuki and Schmidt in Section 3.

In what follows we survey examples and constructions of Noetherian rings that are bad in the sense that they fail to have finite normalization. Finite normalization is, as we recall in Section 2, closely related to the absence of nontrivial nilpotents in the completion, and thus there is a parallel emphasis on the completion of the rings in the constructions we discuss.

The designation "bad," as well as the technical ingenuity behind some of the examples, reinforce a notion that these examples are esoteric and hard to produce.[1] In Sections 3, 4 and 5, we review, beginning with the early discoveries of Akizuki and Schmidt, examples of one-dimensional local Noetherian domains without finite normalization, and we also look to more recent constructions, including in Section 5 a geometric example. While the theory behind the constructions is often involved, the constructions themselves are often conceptually straightforward, and show that there is a certain inevitability to the examples: one encounters them with standard operations such as a finite extension of a DVR, as the kernel of a differential, or as an intersection of an image of the completion of a local domain with its quotient field. From this point of view, the examples are not so exotic, and one of the motivations behind this survey is to describe how Noetherian domains without finite normalization occur *between* (Section 3), *above* (Sections 4 and 5) and *below* (Section 6) naturally occurring Noetherian rings.

---

[1] Miles Reid: "The catch-phrase 'counterexamples due to Akizuki, Nagata, Zariski, etc., are too difficult to treat here' when discussing questions such as Krull dimension and chain conditions for prime ideals, and finiteness of normalization is a time-honoured tradition in commutative algebra textbooks...This does little to stimulate enthusiasm for the subject, and only discourages the reader in an already obscure literature" [54, page 136].

In Section 3 we consider examples of one-dimensional local Noetherian rings without finite normalization that occur in an immediate extension of rank one discrete valuation rings (DVRs), and in Corollary 3.11 we give a simple field-theoretic criterion for when a such an example can be sandwiched into an immediate extension of DVRs. Well-known examples due to Akizuki, Schmidt, Nagata, and Ferrand and Raynaud, all fit into this framework.

Section 4 also focuses exclusively on one-dimensional examples. However, the emphasis here is on when such examples can be found birationally dominating a given local Noetherian domain of dimension possibly larger than 1. The examples in this section occur in a particularly transparent way, either as a kernel of a certain exterior differential or cut out of the quotient field of a local Noetherian domain by an image of its completion. The latter construction leads to the striking theorem of Heinzer, Rotthaus and Sally that every local Noetherian domain of Krull dimension greater than one which is essentially of finite type over a field is birationally dominated by a one-dimensional local Noetherian domain without finite normalization (see Theorem 4.3).

Section 5 is devoted to a geometric example, due to Reguera, of a one-dimensional Noetherian domain without finite normalization. This example stands out from the rest in that it has a direct geometric interpretation: it is the local ring of a point, not on a curve, but on the space of arcs associated to the curve.

Section 6 discusses mainly a technique from [43] for locating Noetherian domains without finite normalization as subintegral extensions of "known" Noetherian domains. This technique produces such Noetherian rings in any Krull dimension, and affords a good deal of control over the traits of the examples it yields. The tradeoff however is that strong demands are made on the quotient field of the domain in order to guarantee existence of these well-behaved subrings.

The literature on bad Noetherian rings is diverse and scattered, since these rings often arise as counterexamples on frontiers of various topics. What follows is an attempt to organize and point out a few central ideas in some of these examples. The focus remains narrowly on local Noetherian domains without finite normalization, and does not touch in any detail on other classes of bad Noetherian rings. For more on other sorts of nonstandard Noetherian rings, see [29] and its references.

Terminology and notation. All rings are commutative and have an identity. A *quasilocal* ring is a not-necessarily-Noetherian ring with a unique maximal ideal; in general our focus is on the Noetherian case, and for this we follow tradition and refer to a quasilocal Noetherian ring as a *local Noetherian ring*. The completion of a local Noetherian ring R with maximal ideal $\mathfrak{m}$ in its $\mathfrak{m}$-adic topology is denoted $\widehat{R}$. A *rank one discrete valuation ring* (DVR) is a local principal ideal domain. The integral closure of a ring R in its total ring of quotients is denoted $\overline{R}$. The ring $\overline{R}$ is also referred to more succinctly as the *normalization* of R. The ring R has *finite normalization* if $\overline{R}$ is a finitely generated R-module; R is *normal* if $R = \overline{R}$. An *overring* of a domain R is a ring between R and its quotient field.

2 Normalization and Completion

In this section we sketch some of the history regarding the relationship between normalization and completion of a local Noetherian ring. Krull proved in 1938 that when a local Noetherian domain R has Krull dimension 1, then R has finite normalization if and only if the completion of R in its $\mathfrak{m}$-adic topology has no nonzero nilpotent elements; that is, R is *analytically unramified* [21]. Ten years later, Zariski noted that when a local domain R has finite normalization, then R is analytically unramified if and only if its normalization is analytically unramifed [64, page 360]. Thus, granted finite normalization, whether R is analytically unramified depends entirely on the analytic ramification of the normalization $\overline{R}$. Motivated by this, as well as Krull's theorem above, Zariski proved that if the local ring of a point on an irreducible variety is normal, then the completion of this local ring is a domain; i.e., the local ring is *analytically irreducible* [64, page 352]. Two years later, in 1950, he reached a stronger conclusion: Such a normal local domain is *analytically normal*, meaning that its completion is a normal local domain [65, Théorème 2]. That the local rings of points on a normal variety are analytically normal can be viewed as a version of Zariski's Main Theorem; see [33, pages 207–214], [40] and [66].

In the article of 1948, Zariski asked then whether every normal Noetherian local domain is analytically irreducible [64, page 360]. (Nagata later answered this question in the negative, as we mention in Section 3.) Zariski identified two conditions on a normal local Noetherian domain R that are sufficient but not necessary for R to be analytically irreducible [64, page 360]:

  (i) for each prime ideal P of R, R/P is analytically unramified, and

  (ii) if P_1 and P_2 are distinct associated prime ideals of $\widehat{R}$, then $(P_1 + P_2) \cap R \neq 0$.

Statement (ii) implies the fiber of the prime ideal $\{0\}$ under the mapping $\operatorname{Spec}(\widehat{R}) \to \operatorname{Spec}(R)$ is connected. For if the fiber of $\{0\}$ is not connected, then there exist ideals I and J of $\widehat{R}$ such that $(I + J) \cap R \neq 0$ and I and J each are intersections of minimal prime ideals of $\widehat{R}$. But then if $P_1 \supseteq I$ and $P_2 \supseteq J$ are minimal, hence associated, prime ideals of $\widehat{R}$, $(P_1 + P_2) \cap R \neq 0$.

A geometric version of condition (i) winds through the literature under different guises: In his 1962 monograph, *Local rings*, Nagata defines a Noetherian ring R to be *pseudo-geometric* if for each prime ideal P of R and each finite extension field L of the quotient field $\kappa(P)$ of R/P, the integral closure of R/P in L is finite over R/P (it is the persistence of (i) across finite extensions that earns the adjective "geometric" here) [36, page 131]. Grothendieck later replaced the terminology of pseudo-geometric rings with that of *anneaux universellement japonais*; Bourbaki and Matsumura, whom we follow, in turn refer to pseudo-geometric rings as *Nagata rings*.

In any case, Nagata proves that a local Noetherian Nagata domain is analytically unramified [36, (36.4), page 131], and that a ring essentially of finite type over a Nagata

ring is also a Nagata ring [36, (36.5), page 132]. Consequently, since fields and the ring of integers are Nagata rings, we arrive at the fundamental fact:

> *A finitely generated algebra over a field or the ring of integers has finite normalization.*

This answered in a strong way an earlier question of Zariski: Is the local ring of a point of an irreducible algebraic variety analytically unramified? (Chevallay had provided the first positive answer to Zariski's specific question about local rings of points on varieties [8, Lemma 9 on page 9 and Theorem 1 on page 11], and Zariski himself also later gave another proof of Chevallay's theorem in [64, page 356].)

In summary, a local Noetherian Nagata domain is analytically unramified. Nagata also proved a partial converse in an article of 1958: If R is a reduced local Noetherian ring and R is analytically unramified, then R has finite normalization [35, Proposition 1, page 414]. Of course, Nagata rings demand something quite a bit stronger than simply finite normalization. Indeed, Nagata gave an example in 1955 of a normal local Noetherian domain that is analytically ramified [34, page 111]; thus a local domain having finite normalization need not be a Nagata ring or analytically unramified.

Finally in 1961, Rees made precise the connection between analytic ramification and normalization:

Theorem 2.1 (Rees [51, Theorems 1.2 and 1.5]). *Let R be a reduced local Noetherian ring, and let F be its total ring of quotients. Then R is analytically unramified if and only if for all $x_1, \ldots, x_n \in F$, the ring $R[x_1, \ldots, x_n]$ has finite normalization.*

In light of the connection between analytic ramification and normalization, one source of local Noetherian domains without finite normalization are those local domains (or possibly overrings of such domains) whose completions have nilpotent elements. There is a rich and extensive literature on realizing complete local rings as the completion of local Noetherian rings having specified properties. In 1981, Larfeldt and Lech gave one such method: Let K be a field, let $X_1, \ldots, X_n$ be indeterminates for K and let I be an ideal of $K[X_1, \ldots, X_n]$ that is primary for $(X_1, \ldots, X_n)$. Set $A = K[X_1, \ldots, X_n]/I$. Then using a notion of flat couples, it is shown that there exists a one-dimensional local Noetherian domain R such that $\widehat{R} = A[[T]]$, where T is an indeterminate for A [22, page 201]. In a later article, Lech proved a much more general existence theorem:

Theorem 2.2 (Lech [23, Theorem 1]). *A complete local ring R with maximal ideal $\mathfrak{m}$ is the completion of a local Noetherian domain if and only if*

(i) $\mathfrak{m} = (0)$ *or* $\mathfrak{m} \notin \operatorname{Ass}(R)$*, and*

(ii) *no nonzero integer of R is a zero-divisor.*

Lech's article initiates a deep sequence of papers characterizing the completions of local UFDs (Heitmann [19, Theorems 1 and 8]), reduced local rings (Lee, Leer,

Pilch and Yasufuku [24, Theorem 1]) and excellent local domains containing the ring of integers (Loepp [28, Theorem 9]). These results all demand remarkably little of a complete local ring in order to realize it as the completion of a specific sort of local Noetherian domain. That the completions of more abstract local Noetherian domains could behave so differently from those arising in algebraic geometry and algebraic number theory occasions Eisenbud's remark, "This is one of the ways in which the Noetherian property is 'too general'" [12, page 193].

In any case, the construction of Lech guarantees the existence of many examples of one-dimensional local Noetherian domains without finite normalization: If R is a one-dimensional complete local Cohen–Macaulay ring that is not reduced, its prime subring is a domain and R is torsion-free over its prime subring, then there exists a one-dimensional local Noetherian domain whose completion is R, and hence this ring does not have finite normalization.

3 Examples between DVRs

As discussed in Section 2, a one-dimensional local Noetherian domain has finite normalization if and only if it is analytically ramified. In this section we give an overview of some examples of one-dimensional analytically ramified local Noetherian domains, as well as some of the general theory regarding the existence of such examples. This section concerns one-dimensional local rings sandwiched into an immediate extension of discrete rank one valuation rings (DVRs), while the next section deals with the existence of one-dimensional analytically ramified local rings birationally dominating a local Noetherian domain.

An extension $U \subseteq V$ of DVRs is *immediate* if U and V have the same value group and residue field; equivalently, with $\mathfrak{M}$ the maximal ideal of U, $\mathfrak{M}V \neq V$ and $V = U + \mathfrak{M}V$. It is easy to see that an extension $U \subseteq V$ of DVRs is immediate if and only if the inclusion $U \subseteq V$ lifts to an isomorphism of U-algebras $\widehat{U} \to \widehat{V}$. Thus for a DVR U, the extension $U \subseteq \widehat{U}$ is immediate. We use the following lemma to explain why some classical examples due to Akizuki, Schmidt and Nagata, all of which occur within an immediate extension of DVRs, fail to have finite normalization.

Lemma 3.1. *If $U \subseteq R \subsetneq V$ is an extension of rings such that $U \subseteq V$ is an immediate extension of DVRs, then V/R is a divisible R-module, and hence V is not a finite R-module.*

Proof. Let $0 \neq r \in R$. To see that $V = R + rV$, use the fact that V is a DVR to find nonnegative integers i and j such that $r^i V = \mathfrak{M}^j V$, where $\mathfrak{M}$ is the maximal ideal of U. Since $U \subseteq V$ is an immediate extension, $V = U + \mathfrak{M}^j V = U + r^i V \subseteq R + rV$, proving that $V = R + rV$ and that $D := V/R$ is a divisible R-module. Since $D \neq 0$, there exists a maximal ideal M of R such that $D_M \neq 0$. But since D is divisible,

$D_M = MD_M$, so that by Nakayama's Lemma, D is not a finite R-module, and hence V is not a finite R-module. $\qquad\square$

We now outline without proof the 1935 example of Akizuki. With the exception of our use of Lemma 3.1, we follow Reid [53, Section 9.5] and [54], where commentary and a complete justification for the example can be found.

Example 3.2 (Akizuki [2]). Let U be a DVR with maximal ideal $\mathfrak{M} = tU$ and quotient field K such that there exists $z = \sum_{i=0}^{\infty} u_i t^{e_i} \in \widehat{U}$ (with each u_i a unit in U) that is transcendental over K and $e_i \geq 2e_{i-1} + 2$ for all $i \geq 1$, where $e_0 = 0$. For $i \geq 0$, let $z_i = u_i + u_{i+1}t^{e_{i+1}-e_i} + u_{i+2}t^{e_{i+2}-e_i} + \cdots$. Let R be the localization of $U[t(z_0 - u_0), \{(z_i - u_i)^2\}_{i=0}^{\infty}]$ at the maximal ideal generated by t and $t(z_0 - u_0)$. Calculations show that R is a one-dimensional local Noetherian domain with quotient field $K(z)$ and normalization $V = K(z) \cap \widehat{U}$ properly containing R (for details, see [53, 54]). Thus since $U \subseteq V$ is an immediate extension of DVRs, Lemma 3.1 shows that R does not have finite normalization, a fact which can also be proved by a direct argument [53, 54].

More can be said about this example: Since the maximal ideal M of R is generated by 2 elements and $M^2 = tM$ [53, Exercise 9.5, page 148], it follows that R has multiplicity 2, and hence every ideal of R can be generated by 2 elements [57, Theorem 1.1, page 49]. We discuss rings for which every ideal can be generated by 2 elements later in this section.

Another example, this one due to Schmidt, appeared in the same year as Akizuki's example. Unlike Akizuki's example, Schmidt's example requires positive characteristic, but this in turn makes the justification for the example easier. We give this example next, but presented and justified differently than the original. For another approach, one that makes explicit the valuation theory in the example, see Zariski [63, pages 23–25].

Example 3.3 (Schmidt [58]). Let k be a field of characteristic $p > 0$, let X be an indeterminate for k, and let $z \in Xk[[X]]$ such that z is transcendental over $k(X)$. (Such an element z must exist; see [67, page 220].) Then $k[X, z] \subseteq k[[X]]$. Let $U = k(X, z^p) \cap k[[X]]$, and consider the ring $R = U[z] \subseteq k(X, z)$. Then U is a DVR with maximal ideal generated by X, and R has quotient field $k(X, z)$. Since z is integral over U, R is a finite extension of U, so R is a one-dimensional Noetherian domain. Let $V = k(X, z) \cap k[[X]]$. Then V is a DVR with maximal ideal generated by X. Moreover, V is integral over R, since $V^p \subseteq U$. Thus R is a local ring with normalization V. Since R is a finite U-module and $U \subsetneq V$, Lemma 3.1 implies that $R \neq V$, so again by Lemma 3.1, R does not have finite normalization.

The next example is from Nagata's appendix, "Bad Noetherian domains" [36]. Nagata considers the ring $A = k^p[[X_1, \ldots, X_n]][k]$, where k is a field of characteristic

$p > 0$ such that $[k : k^p] = \infty$ and $X_1, \ldots, X_n$ are indeterminates for k. He proves that A is a regular local ring and a proper subring of its completion $k[[X_1, \ldots, X_n]]$ [36, (E3.1), page 206]. By varying the choices of n and $z \in k[[X_1, \ldots, X_n]]$ appropriately, he fashions the ring $A[z]$ such that it is (depending on the choice of n and z): (i) a one-dimensional analytically ramified local Noetherian domain; (ii) a two-dimensional local Noetherian domain without finite normalization having a non-Noetherian ring between itself and its normalization; (iii) a three-dimensional local Noetherian domain without finite normalization and whose normalization is not Noetherian; (iv) a normal local Noetherian domain which is analytically ramified; and (e) a subring of a one-dimensional Noetherian domain without finite normalization but such that each localization at a prime ideal has finite normalization [36, Examples 3–6 and 8, pages 205–212]. While all these examples are relevant here, we mention only how the choice is made in case (i), since it fits into the present discussion of one-dimensional rings. We differ from Nagata's original justification of the example in that we rely on Lemma 3.1; see also Reid [53, pages 136–137] for a general approach to the example.

Example 3.4 (Nagata [36, Example 3, page 205]). With notation and assumptions as above, let $U = k^p[[X]][k]$, so that U is a DVR. (Thus in the notation above, $U = A$ with $n = 1$.) Since $[k : k^p] = \infty$, there exist countably many distinct p-independent elements $\alpha_1, \alpha_2, \ldots$ of k. Set $z = \sum_{i=0}^{\infty} \alpha_i X^i \in k[[X]]$. Then since z is integral over U, the ring $R = U[z]$ is a one-dimensional Noetherian domain. Also, since the DVR $V = U(z) \cap k[[X]]$ is integral over R (indeed, $V^p \subseteq R$), it follows that V is the normalization of R, and hence R is a local ring. The choice of coefficients of z forces $z \notin U$, so $U \subsetneq R \subseteq V$. Also, $R \neq V$, since otherwise V/U is a finite U-module, contrary to Lemma 3.1. Thus $U \subsetneq R \subsetneq V$, and another application of Lemma 3.1 shows that R does not have finite normalization.

In all of the above examples, the one-dimensional analytically ramified local Noetherian domain R has the property that the inclusion $R \to V$ lifts to a surjection $\widehat{R} \to \widehat{V}$. (This follows from the fact that since V/R is a divisible R-module, $V = R + M^i V$, where M is the maximal ideal of R, for all $i > 0$.) Since $\widehat{V}$ is a domain and R is not a DVR, the kernel P of this mapping is a nonzero prime ideal. Moreover, since the integral closure of R is a local ring, the ring $\widehat{R}$ has a unique height 1 prime ideal P [30, Theorem 7.9, page 77], which therefore, since $\widehat{R}$ has dimension 1, must be nilpotent. In summary: *If $U \subseteq R \subsetneq V$ is an extension of rings such that $U \subseteq V$ is an immediate extension of DVRs, V is the normalization of R and R is a Noetherian ring (all these requirements are satisfied by the examples of Akizuki, Schmidt and Nagata), then there is a nonzero nilpotent prime ideal P of $\widehat{R}$ such that $\widehat{R}/P \cong \widehat{V}$.* In [4], Bennett proves a converse for positive characteristic:

Theorem 3.5 (Bennett [4, Theorem 1, page 133]). *Let R be a one-dimensional local Noetherian domain of characteristic $p > 0$. If there is a nilpotent prime ideal P of $\widehat{R}$*

*such that $\widehat{R}/P$ is a DVR, then there is a DVR U such that $U \subseteq R \subseteq \widehat{U}$ and $R^q \subseteq U$
for some $q = p^e$.*

A one-dimensional analytically ramified local Noetherian domain can always be
modified by finitely many quadratic transformations to produce a ring R whose com-
pletion has a nilpotent prime ideal with residue ring a DVR [4, Section 1]. Bennett
refers to the extension $U \subseteq R \subseteq \widehat{U}$ in the theorem, with R purely inseparable over U,
as a *presentation* of R. The positive characteristic examples of Nagata and Schimdt
occur within such a presentation. As discussed above, a presentation $U \subseteq R \subseteq \widehat{U}$
forces the existence of a prime ideal P of $\widehat{R}$ such that $\widehat{R}/P$ is a DVR, and if also R
has a local normalization, then P is a nilpotent prime ideal of $\widehat{R}$. Turning this around,
Bennett considers when a complete local ring having a nonzero nilpotent prime ideal
with residue ring a DVR arises from a presentation of an analytically ramified local
ring:

Theorem 3.6 (Bennett [4, Theorem 6.0.4]). *Let V be a complete DVR of positive char-
acteristic, and let C be a one-dimensional local Noetherian ring that is a flat finite
V-algebra with nilpotent ideal P such that $C/P \cong V$. Then there exists a local
Noetherian domain R and a DVR U such that $\widehat{U} = V$, $U \subseteq R \subseteq V$ and $\widehat{R} \cong C$.*

Since V is a DVR, the assertion here that C is flat means only that the nonzero
elements of V are nonzerodivisors on C. The idea behind the construction, which
Bennett terms "quasi-algebrization," is to begin with a suitable choice for the DVR
U, select carefully a finite U-subalgebra S of $V = \widehat{U}$, and then perform an infinite
sequence of operations on S to produce R, all the while staying in the quotient field of
S. The quotient field of R is then finite over that of U, but R is not finite over U.

Bennett's article was partly inspired by examples of Ferrand and Raynaud, who in
1970 introduced a method based on derivations to construct analytically ramified local
Noetherian domains [13]. We will have more to say about their method in Section 6,
but we mention here one of the examples produced with their construction, an example
which occurs in an immediate extension of DVRs. In that sense it fits within the se-
quence of examples considered so far; however, it does not fit directly within Bennett's
framework because it has characteristic 0.

The example of Ferrand and Raynaud uses the notion of idealization of a module.
When A is a ring and L is an A-module, we denote by $A \star L$ the *Nagata idealization*
(or, *trivialization*) of L. This ring is defined as a set by

$$A \star L = \{(a, \ell) : a \in A, \ell \in L\},$$

where for all $a_1, a_2 \in A$ and $\ell_1, \ell_2 \in L$, addition and multiplication in the ring are
defined by:

$$(a_1, \ell_1) + (a_2, \ell_2) = (a_1 + a_2, \ell_1 + \ell_2)$$

$$(a_1, \ell_1)(a_2, \ell_2) = (a_1 a_2, a_1 \ell_2 + a_2 \ell_1).$$

The completion of the local ring in the following proposition is the Nagata idealization of a module; the completions considered later in this section also have this form.

Proposition 3.7 (Ferrand and Raynaud [13, Proposition 3.1]). *Let $\mathbb{C}\{X\}$ be the ring of convergent power series with complex coefficients, and let F be the quotient field of $\mathbb{C}\{X\}$. Then for each $e \in \mathbb{N}$ there exists a subring R of $\mathbb{C}\{X\}$ such that the following statements hold for R.*

(i) *R is a Noetherian domain with quotient field F, embedding dimension $e + 1$ and normalization $\mathbb{C}\{X\}$.*

(ii) *$\widehat{R} \cong \mathbb{C}[[X]] \star J$, for some free $\mathbb{C}[[X]]$-module J of rank e.*

(iii) *If $e > 1$, then R does not have a canonical ideal and the generic formal fiber of R is not Gorenstein.*

The ring R is sandwiched into the immediate extension $\mathbb{C}[X]_{(X)} \subseteq \mathbb{C}\{X\}$. It arises as $D^{-1}(K)$, where $D : \mathbb{C}\{X\} \to L$ is a well-chosen derivation, L is a $\mathbb{C}((X))$-vector space and K is a finite rank free $\mathbb{C}[[X]]$-submodule of L. In the terminology of Section 6, R is a "strongly twisted" subring of $\mathbb{C}\{X\}$. It also can be deduced from (ii) that the multiplicity and embedding dimension of R agree.

Goodearl and Lenagan generalize this idea to incorporate higher-order differentials, and in so doing permit multiplicity and embedding dimension to differ. The rings they construct with this method are *differentially simple*, meaning there is a derivation D from the ring to itself such that no proper nonzero ideal is invariant under D.

Theorem 3.8 (Goodearl–Lenagan [14, Proposition 6 and Example D]). *For any pair of positive integers m and t, there exists a one-dimensional analytically ramified local Noetherian domain R containing the field of rational numbers such that R has embedding dimension $m + 1$, multiplicity $m + t$ and is differentially simple.*

The issue of differential simplicity is relevant to our themes here because Posner showed in 1960 that a differentiably simple ring of characteristic zero finitely generated over its field of constants ("constants" here being the constants for the relevant derivation; the ring of all such constants forms a field in a differentiably simple ring) is normal [49, Theorem 1[2]], and he asked implicitly in a subsequent paper whether a differentiably simple ring of characteristic zero must be normal [50, page 1421]. This question is made more compelling by the 1966 observation of Seidenberg that if a Noetherian domain R contains the rational numbers, then the conductor $(R :_R \overline{R})$ of the normalization of R into itself is invariant under the derivation [59, page 169]. Thus if R is a differentially simple local Noetherian domain containing the rational numbers, then either R is normal or R does not have finite normalization, and hence arises the question of whether the latter case can occur.

---

[2] There is a mistake in the proof of the first lemma of Posner's article which is corrected in [59].

Moreover, Vasconcelos showed that if R is a one-dimensional analytically unramified local Noetherian ring containing the rational numbers and having a derivation D such that $D(x) = 1$ for some nonunit x of R, then R is a DVR, and he asked whether this remains true if R is assumed to be reduced but analytically ramified [62, page 230]. Lequain answered Vasconcelos' question in the negative by modifying Akizuki's construction, Example 3.2, to produce a one-dimensional analytically ramified local Noetherian domain R having a nonunit x such that $D(x) = 1$ for a derviation $D : R \to R$ [25, Theorem 2.1 and Example 2.2]. Since R is local and one-dimensional, the condition $D(x) = 1$ then forces R to be differentially simple with respect to D. Another construction in mixed characteristic given later by de Souza Doering and Lequain produced similar examples, but of arbitrary large embedding dimension and multiplicity [10, Proposition 1]. However, as noted in [14, page 479], the calculations to justify these examples are "long and technical." The construction of Goodearl and Lenagan, in addition to showing every possible pair $2 \leq m \leq e$ can occur as embedding dimension and multiplicity, respectively, of such an example, has the advantage of being computationally simpler than the previous examples, as well as having an obvious choice for the derivation to decide the differential simplicity of the ring, namely the derivation that defines the ring as a pullback.

Proposition 3.7, which is the point of departure for the construction of Goodearl and Lenagan, can be viewed as a particular instance of a more general method of extracting analytically ramified local rings as subrings of rings possessing a special sort of derivation. As discussed in Section 6, this method can be applied to produce rings of any Krull dimension. But in dimension 1, some consequences of the method can be described without mention of the notion of what is termed in Section 6 a "strongly twisted" subring. So in keeping with the focus on one-dimensional rings, we discuss some of these consequences now and postpone till Section 6 an explanation of the method behind the results.

In dimension 1, the method of strongly twisted subrings produces stable domains. An ideal I of a domain R is *stable* if it is projective over $\mathrm{End}_R(I)$, its ring of endomorphisms. The terminology here is due to Lipman [26]; see the survey [41] for background and an explanation of the terminology. In this section we are interested exclusively in the case in which R is a quasilocal ring, and in this situation stable ideals are simply ideals having a principal reduction of reduction number ≤ 1; that is, an ideal I of a quasilocal domain R is stable if and only if $I^2 = iI$ for some $i \in I$ (see [26] and [42, Lemma 3.1]). The domain R is *stable* provided every nonzero ideal is stable.

Bass proved that the class of stable domains includes the 2-*generator domains*, those domains for which every ideal can be generated by 2 elements [3]. A local Noetherian domain with finite normalization is a 2-generator ring if and only if it is a stable domain; see Drozd and Kiričenko [11] or Sally and Vasconcelos [55, Theorem 2.4]. The latter authors noted that a stable Noetherian domain must have Krull dimension 1 [56], and they proved that a stable local Noetherian domain of embedding dimension

2 must be a 2-generator ring [56, Lemma 3.2]. Using the method of Ferrand and Raynaud they also gave an example in characteristic 2 of a local Noetherian stable domain that does not have the 2-generator property, and hence does not have finite normalization [56, Example 5.4]. Heinzer, Lantz and Shah modified this example to show that every embedding dimension > 1 was possible for a local Noetherian stable domain without finite normalization [17, (3.12)]. (It is easy to see that for a local Noetherian stable domain, since its maximal ideal has reduction number 1, the embedding dimension and multiplicity of the ring agree.) A consequence of Theorem 3.13 below is that examples of large embedding dimension exist in any characteristic.

Thus analytically *unramified* local Noetherian stable domains are simply 2-generator rings, but the class of analytically *ramified* local Noetherian stable domains properly includes the class of 2-generator rings, and whether an analytically ramified local Noetherian stable domain R is a 2-generator ring is conditioned on whether its embedding dimension is ≤ 2. The embedding dimension of R reflects how far away R is from its normalization:

Theorem 3.9 ([44, Theorem 4.2]). *Let R be a quasilocal domain with normalization $\overline{R}$ and quotient field F, and let $n > 1$. Then R is an analytically ramified local Noetherian stable domain of embedding dimension n if and only if $\overline{R}$ is a DVR and $\overline{R}/R \cong \bigoplus_{i=1}^{n-1} F/\overline{R}$ as R-modules.*

More characterizations in this same spirit can be found in [44]. The case $n = 1$ implies that the analytically ramified local 2-generator domains are precisely those quasilocal domains R for which $\overline{R}$ is a DVR and $\overline{R}/R \cong F/\overline{R}$ as R-modules [44, Corollary 4.5]. It follows that when R is an analytically ramified local 2-generator domain, then $R \subseteq \overline{R}$ is what is termed in [16] a J-*extension*, meaning that every proper R-subalgebra of $\overline{R}$ is a finitely generated R-module. It is in fact the unique J-extension of R in its quotient field [16, Proposition 3.1]. More generally, when R is an analytically ramified local Noetherian domain, then the J-extensions $R \subseteq S$, where S is an overring of R, are in one-to-one correspondence with the minimal prime ideals of the total quotient ring of $\widehat{R}$ [16, Theorem 2.1]. An analytically ramified local Noetherian domain, even a Gorenstein one, may have more than one J-extension in its quotient field [16, Example 3.8].

Analytically ramified local Noetherian stable domains arise from immediate extensions of DVRs, as we see in the next theorem, which uses the notion of the exterior differential of a ring extension. Given an A-linear derivation $D : S \rightarrow L$, with L an S-module, there exists a universal module through which D must factor. More precisely, for an extension $R \subseteq S$ of rings, there exists an S-module $\Omega_{S/R}$, and an R-linear derivation $d_{S/R} : S \rightarrow \Omega_{S/R}$, such that for every derivation $D : S \rightarrow L$, there exists a unique S-module homomorphism $\alpha : \Omega_{S/R} \rightarrow L$ with $D = \alpha \circ d_{S/R}$; see for example [12, 20]. The S-module $\Omega_{S/R}$ is the *module of Kähler differentials* of the ring extension $R \subseteq S$, and the derivation $d_{S/R} : S \rightarrow \Omega_{S/R}$ is the *exterior*

differential of the extension $R \subseteq S$. If L is a torsion-free S-module, then a submodule K of L is *full* if L/K is a torsion S-module.

Theorem 3.10 ([45, Theorems 4.1 and 4.4]). *Let $U \subseteq V$ be an immediate extension of DVRs with quotient fields Q and F, respectively. Suppose K is a full V-submodule of $\Omega_{F/Q}$ such that $n := \dim_{V/\mathfrak{M}} K/\mathfrak{M}K$ is positive, where $\mathfrak{M}$ is the maximal ideal of V. Then $R = V \cap d_{F/Q}^{-1}(K)$ is an analytically ramified quasilocal stable domain with normalization V. Every quasilocal stable domain containing U and having normalization V must arise this way for a unique choice of K, and satisfy the following properties.*

(i) *R is a Noetherian domain (with embedding dimension $n + 1$) if and only if n is finite.*

(ii) *If R is a Noetherian domain, then $\widehat{R} \cong \widehat{V} \star J$, where J is a free $\widehat{V}$-module of rank n.*

With some basic facts about the module of Kähler differentials, the theorem yields a criterion for when an analytically ramified local Noetherian domain can be sandwiched into an immediate extension of DVRs.

Corollary 3.11 ([45, Corollary 4.2]). *Let $U \subseteq V$ be an immediate extension of DVRs having quotient fields Q and F, respectively. Then there exists an analytically ramified local Noetherian domain containing U and having normalization V if and only if either (i) F has characteristic 0 and is not algebraic over Q, or (ii) F has characteristic $p > 0$ and $F \neq Q[F^p]$.*

Proof. The proof depends on the fact that statements (i) or (ii) hold precisely when $\Omega_{F/Q} \neq 0$ [20, Proposition 5.7]. Suppose that R is an analytically ramified local Noetherian domain containing U and having normalization V. Then there exists an analytically ramified local ring between R and V that has normalization V and is a stable ring (see Theorem 4.2 below). Thus by Theorem 3.10, $\Omega_{F/Q} \neq 0$, as claimed. Conversely, if $\Omega_{F/Q} \neq 0$, then since $\Omega_{F/Q}$ is an F-vector space, we may choose any proper full S-submodule K of $\Omega_{F/Q}$ such that $\dim_{V/\mathfrak{M}} K/\mathfrak{M}K$ is finite and apply Theorem 3.10 to obtain the ring in the corollary. $\square$

Remark 3.12. In positive characteristic, *every* analytically ramified local Noetherian stable domain must arise as in Theorem 3.10. For if R is an analytically ramified local Noetherian stable domain, then there exists a prime ideal P of $\widehat{R}$ such that $P^2 = 0$ and $\widehat{R}/P$ is a DVR [44, Corollary 3.5]. Thus when R has positive characteristic, there exists by Theorem 3.5 a DVR U such that $U \subseteq R \subseteq \widehat{U}$. With F the quotient field of R, we have that $U \subseteq V := \widehat{U} \cap F$ is an immediate extension, and so we are in the setting of the theorem. See also [45, Theorem 6.4].

Corollary 3.11 helps explain why the examples of Akizuki, Schmidt and Nagata given earlier in this section are couched as they are.

- *Akizuki's example*. The ring in this example is sandwiched into an immediate extension of DVRs $U \subseteq V$ with quotient fields K and $K(z)$, respectively, where z is transcendental over K. Thus $\Omega_{K(z)/K}$ has dimension 1 as a $K(z)$-vector space, and as in the proof of Corollary 3.11, there exists an analytically ramified local Noetherian stable domain containing U and having normalization V. As discussed after Akizuki's example, the ring produced in the example is a 2-generator ring, so in fact Theorem 3.10 captures this same ring from another point of view, as a pullback of a derivation.

- *Schmidt's example*. This ring is sandwiched into a characteristic p immediate extension $U \subseteq V$, where U and V have quotient fields $Q := k(X, z^p)$ and $F := k(X, z)$, respectively, and X and z are transcendental over k. Since $F \neq Q[F^p]$, Corollary 3.11 shows there is an analytically ramified local Noetherian domain containing U and having normalization V.

- *Nagata's example*. This example involves an immediate extension $U \subseteq V$ of DVRs in characteristic $p > 0$, where (in the notation of the example) the quotient field of U is $Q = k^p((X))[k]$ and the quotient field of V is $F = k^p((X))[k](z)$. Now $z \in F$ but $z \notin Q[F^p] = Q$, so by Corollary 3.11, there must be an analytically ramified local Noetherian stable domain containing U and having normalization V.

Theorem 3.10, along with technicalities involving separability and valuation theory, leads to an existence theorem in the setting of function fields which shows that analytically ramified local Noetherian stable domains of arbitrarily large embedding dimension exist is every characteristic (compare to the discussion preceding Theorem 3.9). By a DVR *in* F/k we mean a DVR that is a k-algebra having quotient field F. A *divisorial valuation ring* in F/K is a DVR V in F/k such that $\mathrm{trdeg}_k V/\mathfrak{M} = \mathrm{trdeg}_k F - 1$, where $\mathfrak{M}$ is the maximal ideal of V.

Theorem 3.13 ([45, Theorem 7.3]). *Let F/k be a finitely generated field extension, and let V be a DVR in F/k with maximal ideal $\mathfrak{M}$ such that $V/\mathfrak{M}$ is a finitely generated extension of k. Then the following statements are equivalent.*

  (i) *V is the normalization of an analytically ramified local Noetherian domain containing k.*

 (ii) *V is the normalization of an analytically ramified Noetherian stable ring containing k and having embedding dimension $d = \mathrm{trdeg}_k F - \mathrm{trdeg}_k V/\mathfrak{M}$.*

(iii) *V is not a divisorial valuation ring in F/k.*

If F/k is a finitely generated field extension of transcendence degree $d > 1$, then there exists a DVR V in F/k with maximal ideal $\mathfrak{M}$ such that $V/\mathfrak{M}$ is a finite algebraic extension of k (see Theorem 4.3). Thus by Theorem 3.13, V is the normalization of

an analytically ramified Noetherian stable ring containing k and having embedding dimension d.

At the other extreme from function fields are those local Noetherian domains whose normalizations are complete DVRs. The following theorem is obtained by sandwiching local Noetherian domains into an immediate extension of DVRs.

Theorem 3.14 ([45, Theorem 7.6]). *Let V be a complete DVR with residue field k.*

(i) *If V has characteristic $p \neq 0$ and k is perfect, then there does not exist an analytically ramified local Noetherian domain containing k whose normalization is V.*

(ii) *If either* (a) $V = \widehat{\mathbb{Z}}_p$, (b) *$V$ and k have characteristic 0, or* (c) *V has characteristic $p \neq 0$ and $[k : k^p]$ is uncountable, then for every $d > 1$ there exists an analytically ramified local Noetherian stable domain of embedding dimension d whose normalization is V. There also exists a non-Noetherian stable domain whose normalization is V.*

If R is an analytically ramified local Noetherian domain of dimension 1 whose normalization is a DVR, then by Theorem 4.2 below, there exists an analytically ramified 2-generator overring of R having the same normalization as R. Using Matlis' theory of Q-rings, such rings which have normalization a complete DVR are classified in [45]. (An integral domain R with quotient field Q is a Q-*ring* if $\operatorname{Ext}_R^1(Q, R) \cong Q$; see [31].)

Theorem 3.15 ([45, Theorem 8.4]). *A one-dimensional quasilocal domain R with quotient field Q is an analytically ramified local 2-generator ring whose normalization $\overline{R}$ is a complete DVR if and only if $\widehat{R}$ has rank 2 as a torsion-free R-module, $\overline{R}/R$ is a nonzero divisible R-module and there are no other proper nonzero divisible R-submodules of Q/R.*

4 Examples Birationally Dominating a Local Ring

The analytically ramified local Noetherian domains considered in the last section are sandwiched into an immediate extension of DVRs. We depart now from this approach, and while the analytically ramified rings we next consider have normalization a DVR, we do not need that they have a DVR subring which anchors an immediate extension. (Although by Theorem 3.5, in positive characteristic such a DVR is always present modulo an adjustment by finitely many quadratic transformations.) To frame this next sequence of results, we require some terminology: If $B \subseteq R$ is an extension of quasilocal domains, then R *dominates* B if the maximal ideal of B is a subset of the maximal ideal of R. The ring R *birationally dominates* B if R dominates B and has the same quotient field as B. When B is a quasilocal domain with maximal ideal $\mathfrak{m}$, we say the quasilocal ring R *finitely dominates* B if R birationally dominates B and $R/\mathfrak{m}R$ is a

finite B-module. When also $R/\mathfrak{m}R$ is a nonzero cyclic B-module, we say R *tightly dominates* B; i.e., the quasilocal ring R tightly dominates B if R birationally dominates B and $R = B + \mathfrak{m}R$. Thus R tightly dominates the subring B if and only if $\mathfrak{m}R$ is the maximal ideal of R and B and R share the same residue field and quotient field.

Tightly dominating DVRs arise from analytic arcs. For example, if k is a field and $X_1, \ldots, X_n$ are indeterminates for k, then the ring $A = k[X_1, \ldots, X_n]$ embeds into $k[[X_1]]$ as a $k[X_1]$-algebra in such a way that the images of $X_2, \ldots, X_n$ are in $X_1 k[[X_1]]$ (see [67, page 220]). Identifying A with its image in $k[[X_1]]$, the DVR that is the intersection of $k[[X_1]]$ with the quotient field of A tightly dominates A. More generally, if A is a local Noetherian domain, then there exists a DVR V that tightly dominates A if and only if there is a prime ideal P of $\widehat{A}$ such that $P \cap A = 0$ and $\widehat{A}/P$ is a DVR [44, Corollary 5.5].

If A is a local Noetherian domain and P is a prime ideal of $\widehat{A}$ such that $P \cap A = 0$ and $\dim(\widehat{A}/P) = 1$ (i.e., the dimension of the generic formal fiber of A is $\dim(A) - 1$), then there is a finitely generated birational extension of A that is tightly dominated by a DVR. For example, if a local domain A of dimension d is essentially of finite type over a field, then A is birationally dominated by a DVR whose residue field is finite over the residue field of A (see Theorem 4.3), so A has a finitely generated birational extension of dimension d that is essentially of finite type over k and tightly dominated by this DVR. Thus blowing up at an ideal of A produces a ring that is tightly dominated by a DVR. As the next theorem shows, in such a situation it is conceptually easy to locate analytically ramified local Noetherian domains. Recall from Section 3 that $d_{V/A}$ is the exterior differential of the ring extension V/A.

Theorem 4.1 ([45, Theorems 5.1 and 5.3 and Corollary 5.4]). *Let $U \subseteq A \subsetneq V$ be an extension of local Noetherian domains, where $U \subseteq V$ is an immediate extension of DVRs with quotient fields Q and F, respectively, and V birationally dominates A. The ring $R = \operatorname{Ker} d_{V/A}$ is an analytically ramified local Noetherian stable ring that tightly dominates A; R has normalization V; R has maximal ideal $\mathfrak{m}R$ extended from the maximal ideal $\mathfrak{m}$ of A; and R is contained in every stable ring between A and V. If also A is essentially of finite type over U with Krull dimension $d > 1$ and P is the kernel of $\widehat{A} \to \widehat{V}$, then*

$$\operatorname{emb.dim} R = 1 + \dim_F \Omega_{F/Q} = 1 + \operatorname{emb.dim} \widehat{A}_P.$$

Moreover, if F is separable over Q, then $\operatorname{emb.dim} R = d$ and the ring $\widehat{A}_P$ is a regular local ring.

Thus in the context of the theorem, when A is essentially of finite type over U, then the embedding dimension of R is a measure of the regularity of a corresponding prime ideal in the generic formal fiber. If U is an excellent DVR, then A is excellent, and hence the generic formal fiber of A is regular. Therefore, in this case, $\operatorname{emb.dim} R = d$. This occurs, for example, in the following circumstance. Let k be a field, and let A be

a local domain of Krull dimension $d > 1$ that is essentially of finite type over k. Then A is finitely dominated by a DVR (see Theorem 4.3). If in fact A is tightly dominated by a DVR V, then, choosing $t \in A$ such that tV is the maximal ideal of V, we have that $U := k[t]_{(t)} \subseteq V$ is an immediate extension of DVRs, and A is essentially of finite type over U. Therefore, the theorem is applicable to $U \subseteq A \subsetneq V$, and since A is excellent, we conclude also that emb.dim $R = d$.

There is also a version of the theorem for dimension 1, but in this case the base ring A must necessarily be analytically ramified, since otherwise every overring of A has finite normalization. More precisely, let A be an analytically ramified local Noetherian domain whose normalization $\overline{A}$ is a DVR that tightly dominates A. Then $R = \operatorname{Ker} d_{\overline{A}/A}$ is an analytically ramified local Noetherian stable domain such that every stable overring of A contains R; this is established in the proof of [44, Theorem 5.11]. The assumption here that $\overline{A}$ is a DVR that tightly dominates A is equivalent to the assertion that $\overline{A}/A$ is a divisible A-module. Divisible submodules of $\overline{A}/A$ play an important role in Matlis' approach to one-dimensional analytically ramified Cohen–Macaulay rings in the monograph [30], where the subtleties of the analytically ramified case are dealt with in some detail. These ideas also lead in [44, Theorem 5.11] to another proof of the following theorem of Matlis.

Theorem 4.2 (Matlis [30, Theorem 14.16]). *Every one-dimensional analytically ramified local Noetherian domain is finitely dominated by an analytically ramified local 2-generator ring R.*

If R is a one-dimensional analytically *unramified* local ring, then every overring of R is analytically unramified. But in higher dimensions, there is much more room between a Noetherian domain A and its quotient field for pathological behavior, and even though A may be a natural enough Noetherian ring, say, a polynomial ring over a field, there can exist analytically ramified local Noetherian overrings of A. This is a consequence of the following theorem, which shows that under mild hypotheses, such analytically ramified overrings must exist. The equivalence of statements (ii), (iv) and (v) can be deduced from Heinzer, Rotthaus and Sally [18, Corollaries 1.27 and 2.4]. That the other statements are equivalent to these three, as well as the assertion about the case in which A is excellent, is proved in [44, Corollary 5.13]. The final assertion of the theorem is due to Matsumura, who proved that (v) holds for a local domain of dimension $d > 1$ that is essentially of finite type over a field [32, Theorem 2].

Theorem 4.3. *Let A be a local Noetherian domain with Krull dimension $d > 1$. Then the following statements are equivalent.*

(i) *A is finitely dominated by an analytically ramified local Noetherian stable ring.*

(ii) *A is finitely dominated by an analytically ramified one-dimensional local Noetherian ring.*

(iii) *A is tightly dominated by an analytically ramified one-dimensional local Noetherian ring.*

(iv) *A is finitely dominated by a DVR.*

(v) *The dimension of the generic formal fiber of A is $d - 1$.*

If also A is excellent, then the stable ring in (i) *can be chosen to have embedding dimension d but no bigger. Moreover, these five equivalent conditions are satisfied when A is essentially of finite type over a field and has dimension $d > 1$.*

The ring in (ii) is obtained using a theorem, stated below, of Heinzer, Rotthaus and Sally, which involves intersecting a homomorphic image of the completion of a local domain with the quotient field of the domain. This is a third source of one-dimensional analytically ramified local rings (the other two being immediate extensions of DVRs and kernels of exterior differentials). To formalize this idea, let A be a local Noetherian domain, and suppose that I is an ideal of $\widehat{A}$ such that every associated prime P of I satisfies $A \cap P \neq 0$. Then the canonical mapping $A \rightarrow \widehat{A}/I$ is an embedding, and we can identify A with its image in $\widehat{A}/I$. Under this identification, since the associated primes of I contract to 0 in A, it follows that the nonzero elements of A are nonzerodivisors in $\widehat{A}/I$. Therefore, the quotient field F of A can be viewed as a subring of the total quotient ring of $\widehat{A}/I$, and hence we may consider the ring $R = F \cap (\widehat{A}/I)$.

Theorem 4.4 (Heinzer–Rotthaus–Sally [18, Corollary 1.27]). *Let A be a local Noetherian domain with quotient field F, and let I be a ideal of $\widehat{A}$ such that $\dim(\widehat{A}/I) = 1$ and every associated prime P of I satisfies $A \cap P \neq 0$. Then $R = \widehat{A}/I \cap F$ is a one-dimensional local Noetherian domain with $\widehat{R} \cong \widehat{A}/I$, and if I is properly contained in its radical, then R is analytically ramified.*

Thus if A has dimension $d > 1$ and the generic formal fiber of A has dimension $d-1$ (as is the case in the context of Theorem 4.3), then we may choose a prime ideal P of $\widehat{A}$ such that $\widehat{A}/P$ has dimension 1. For any P-primary ideal I of $\widehat{A}$ properly contained in P, the theorem shows that $R = \widehat{A}/I \cap F$ is a one-dimensional analytically ramified local Noetherian ring. If also $P^2 \subseteq I$, then R is a stable domain [44, Theorem 5.3].

Moreover, if the generic formal fiber of A has n distinct prime ideals $P_1, \ldots, P_n$ of dimension 1, then choosing $I = Q_1 \cap \cdots \cap Q_n$, where each Q_i is P_i-primary and at least one Q_i is not prime, yields a one-dimensional analytically ramified local domain whose normalization has n maximal ideals. Such an example can be realized for example whenever A is a countable local Noetherian domain of Krull dimension > 1. For in this case, there exists for each $n > 0$, n distinct prime ideals of dimension 1 in the generic formal fiber of A [18, Proposition 4.10]. Lech's construction in Theorem 2.2 is another way to produce one-dimensional analytically ramified local Noetherian domains with normalization not a local ring.

5 A Geometric Example

As discussed in Section 2, the local rings of points of varieties are analytically un-
ramified, and hence one does not encounter local Noetherian domains without finite
normalization in a direct way in geometric contexts. However, Reguera has recently
shown that local rings of certain points in the the space of arcs of an irreducible curve
are analytically ramified. The space of arcs of a variety, introduced by Nash in [37]
to study the geometry of the singular locus of a variety, encodes information about the
exceptional divisors of desingularizations of the variety. This space, which is in fact a
scheme, is somewhat mysterious, since it need not be of finite type over a field, or even
Noetherian. We discuss in a very limited way the space of arcs of an affine scheme in
order to give some context for the example of Reguera.

Let X be a separated scheme of finite type over a perfect field k, and let K/k be a
field extension. A *K-arc on X over k* is a k-morphism $\mathrm{Spec}\, K[[T]] \to X$. Associated
to X is a scheme X_∞, the *space of K-arcs of X over k*, whose K-rational points
are the K-arcs on X. The scheme X_∞ is constructed as a direct limit of spaces of
"truncated arcs," but we omit this description here, and give instead an interpretation
of X_∞ in the case where X is affine; see [52] for the more general version.

If X is the affine space $\mathrm{Spec}\, k[X_1, \ldots, X_m]/I$, with I an ideal of $k[X_1, \ldots, X_m]$,
then X_∞ can described as follows. For each $i \geq 0$, let $\underline{X}_i = (X_{1,i}, \ldots, X_{m,i})$ be an
m-tuple of indeterminates for k. For each $f \in I$, we have

$$ f\left(\sum_{i=0}^{\infty} X_{1,i} T^i, \ldots, \sum_{i=0}^{\infty} X_{m,i} T^i \right) = \sum_{i=0}^{\infty} F_i T^i, $$

for some $F_i \in k[\underline{X}_0, \ldots, \underline{X}_i, \ldots]$. Then X_∞ is the affine scheme $X_\infty = \mathrm{Spec}\, A$,
where

$$ A = k[\underline{X}_0, \ldots, \underline{X}_i, \ldots]/(\{F_i\}_{i \geq 0, f \in I}). $$

The space X_∞ parameterizes the arcs of X in the following way. For P a prime ideal
of A, let $\kappa(P)$ denote the residue field of P, and let $\phi_P : A \to \kappa(P)$ be the canonical
homomorphism. Then corresponding to P is the $\kappa(P)$-arc $\alpha_P : \mathrm{Spec}\, \kappa(P)[[T]] \to X$
induced by the ring homomorphism

$$ \alpha_P^{\#} : k[X_1, \ldots, X_m]/I \to \kappa(P)[[T]] : X_t + I \mapsto \sum_{i=0}^{\infty} \phi_P(X_{t,i}) T^i. $$

Thus there is a morphism of schemes $j : X_\infty \to X$ which sends $P \in X_\infty$ to the
image under α_P of the closed point of $\mathrm{Spec}\, \kappa(P)[[T]]$; i.e., j sends P to the *center* of
the arc α_P on X.

Reguera considers the structure of the ring A, as well as $A/N(A)$, with $N(A)$ the
nilradical of A, and shows that for the cusp $f(X, Y) = X^3 - Y^2$, there is a localization
A_P of A at a height one prime ideal P such that $B = A_P/N(A_P)$ is a one-dimensional

analytically ramified local Noetherian domain of embedding dimension 2. This example is abstracted into a more general result, which we state below in Theorem 5.2. We first sketch the example, and refer to [52, Corollary 5.6] for the extensive theory and calculations which justify the example.

Example 5.1 (Reguera [52]). Let X and Y be indeterminates for $\mathbb{C}$, let $f(X, Y) = X^3 - Y^2$ and let C be the affine curve $\operatorname{Spec} \mathbb{C}[X, Y]/(f)$. Then $C_\infty = \operatorname{Spec} A$, where

$$A = \mathbb{C}[X_0, Y_0, X_1, Y_1, \ldots]/(F_0, F_1, \ldots)$$

and as above,

$$\left(\sum_{i=0}^\infty X_i T^i\right)^3 - \left(\sum_{i=0}^\infty Y_i T^i\right)^2 = \sum_{i=0}^\infty F_i T^i.$$

In particular, $F_0 = X_0^3 - Y_0^2$ and $F_1 = 3X_0^2 X_1 - 2Y_0 Y_1$. Let

$$P = \sqrt{(X_0, X_1, Y_0, Y_1, Y_2)A}.$$

Then P is a prime ideal of A [52, Example 3.16]. The ring A_P is not a Noetherian ring, but $A_P/N(A_P)$ is a one-dimensional analytically ramified Noetherian domain of embedding dimension 2 [52, Corollary 5.6].

The prime ideal P in the example also has geometric significance: it is the generic point of the closed subset of C_∞ consisting of the arcs on C centered at the origin [52, Corollary 5.6]. The ideas behind the example yield a more general result:

Theorem 5.2 (Reguera [52, Corollary 5.7]). *Let C be an irreducible formal curve of multiplicity $e \geq 2$ over a field k of characteristic 0, and let P be the generic point of the irreducible closed subset consisting of the arcs centered at a singular point of C. Then for $B = \mathcal{O}_{C_\infty, P}$, the ring $B/N(B)$ is a one-dimensional analytically ramified local Noetherian domain of embedding dimension e.*

6 Strongly Twisted Subrings of Local Noetherian Domains

Let S be a ring, and let L be an S-module. When $D : S \to L$ is a derivation, then for each S-submodule K of L, the pullback $D^{-1}(K)$ is a subring of S. This simple observation is used in a sophisticated way by Ferrand and Raynaud in their 1970 article to construct analytically ramified local Noetherian domains of dimension 1 and 2. (A third example in dimension 3 was also constructed, but it was produced from the two-dimensional example rather than directly from a derivation.) The ring in Theorem 3.7 is the one-dimensional example. In that case $S = \mathbb{C}\{X\}$, L is a finite dimensional vector space over the field $\mathbb{C}((X))$, and K is a free module over $\mathbb{C}[[X]]$ of the same rank as the dimension of L. The ring R in the theorem is then $R = D^{-1}(K)$, and the fact that R works as advertised in the theorem is the real content of the con-

struction. That the ring R is Noetherian is subtle and sensitive to the setting here, and in general, because the derivation is not an R-module map, the connection between module-theoretic properties of K and ideal-theoretic properties of R is opaque. Ferrand and Raynaud's approach to this difficulty is to single out in a technical lemma what specifically makes their example work [13, Lemme 2.1]. Because of its length we do not reproduce their lemma here, but ultimately it asserts that $\widehat{R} \cong \widehat{S} \star \widehat{K}$ (where $\star$ represents Nagata idealization, as discussed in Section 3). To do so it demands much of S, K and L, and even the resulting pullback R; e.g., it requires a priori that R is a Noetherian ring, which presents significant challenges to applying the lemma. In any case, the example in Theorem 3.7 just meets the requirements of their lemma.

Remarkably, however, Ferrand and Raynaud find a two-dimensional UFD S that also satisfies the criteria of the lemma, and as a consequence they produce a two-dimensional local Noetherian domain R whose completion fails to be analytically unramified in a dramatic way, in that it has embedded primes. In this case $S = \mathbb{C}\{X, Y\}$, L is a vector space over the quotient field of S, and K is a V-submodule of L, where V is a DVR tightly dominating S. The derivation $D : S \to K$ is carefully chosen to force $R = D^{-1}(K) \cap S$ to be a Noetherian ring [13, Proposition 3.3]. The method of Ferrand and Raynaud was abstracted and improved upon by Goodearl and Lenagan in 1989 to obtain more examples in dimensions 1 and 2 (see also Section 3). A good bit of the method of Goodearl and Lenagan can be fit into the larger framework of twisted subrings discussed below. However, as discussed in Section 2, Goodearl and Lenagan also extended their method in dimension 1 to higher order derivations, and as a consequence were able to construct one-dimensional analytically ramified local Noetherian domains whose multiplicity and embedding dimension differ. By contrast in dimension 1 the method of strongly twisted subrings as outlined below and demonstrated in Section 3 produces stable domains, and multiplicity and embedding dimension coincide for such rings.

Goodearl and Lenagan also abstracted the method of Ferrand and Raynaud to dimension 2, and provided a wider class of examples of two-dimensional local Noetherian domains whose completions have an embedded prime. Their method produces the following example. Let k be a field, let X be an analytic indeterminate for k and let $y, z \in Xk[[X]]$ be algebraically independent over $k(X)$. Let $U = k(X, z) \cap k[[X]]$, let S be the localization of $U[y]$ at the maximal ideal (X, y), and let $d : S \to k((X))$ be the restriction of the partial derivative $\partial/\partial z$ on $k(X, y, z)$ to S. Then $R = d^{-1}(k[[X]] \cap k(X, y, z))$ is a two-dimensional analytically ramified local Noetherian domain with normalization S [14, page 494]. This example is an instance of something more general:

Proposition 6.1 (Goodearl–Lenagan [14, page 494]). *If X, Y, Z are indeterminates for the field k, then there exists a two-dimensional analytically ramified local Noetherian domain R containing $k[X, Y, Z]$ with quotient field $k(X, Y, Z)$ whose normalization is a regular local ring.*

In [43], derivations are used to construct large classes of Noetherian domains without finite normalization. The method allows for strong control over the constructed ring, and as with the methods discussed above, realizes the ring as a subring of a "standard" Noetherian domain S. The method can be arranged to produce rings of any Krull dimension, but the only way of which I am aware to use the method to produce rings of dimension > 1 is with rather specific assumptions on the quotient field of S, as evidenced by Theorem 6.3. In dimension 1, the method is much easier to implement. Ultimately the technical reason for this is that immediate extensions of DVRs are more easily found in nature than are examples of the higher dimensional analogue of "strongly analytic" extensions. Strongly analytic extensions are discussed later in this section.

More formally, we begin with a domain S having quotient field F and a derivation D from F to a torsion-free divisible S-module L. As in the method of Ferrand and Raynaud, we choose a submodule K of L and define $R = S \cap D^{-1}(K)$. The ring R then is the object of interest. To obtain control over the ideal-theoretic traits of R, the derivation D needs to be somewhat special:

Definition 6.2. Let S be a domain with quotient field F, and let R be a subring of S. Let K be a torsion-free S-module, and let FK denote the divisible hull $F \otimes_S K$ of K. We say that R *is strongly twisted by* K if there is a derivation $D : F \to FK$ such that:

(i) $R = S \cap D^{-1}(K)$,

(ii) $D(F)$ generates FK as an F-vector space, and

(iii) $S \subseteq \operatorname{Ker} D + sS$ for all $0 \neq s \in S$.

The derivation D *strongly twists R by* K.

The reason for the adverb "strongly" here is that there is a weaker notion of a subring twisted along a multiplicatively closed subset of S; we discuss this later in the section. Parsing the above definition shows that the real demand on D occurs in (iii). This is a strong property, and it is what makes the requirements of the definition a challenge to satisfy. By contrast, (i) asserts nothing, since we may simply define R to be $S \cap D^{-1}(K)$. (Recall from our earlier discussion that $D^{-1}(K)$ is always a ring.) The criterion (ii) can also easily be arranged: If $D(F)$ falls short of generating all of FK, then, setting L to be the F-subspace of FK generated by $D(F)$, we may replace K with $L \cap K$, and doing so will not change R.

It also follows from the definition that if there is *some* nonzero torsion-free module K such that the subring R of S is strongly twisted by K, then there are *many* strongly twisted subrings of S. Indeed, it is easy to see that for every torsion-free S-module J with $\operatorname{rank}(J) \leq \operatorname{rank}(K)$, there exists a subring of S that is strongly twisted by J [43, Lemma 3.1]. Thus the issue for finding strongly twisted subrings of the Noetherian domain S is whether there exists a derivation fulfilling the requirements of the definition. When S is a DVR with quotient field F, then the existence of the derivation depends entirely on whether there is a DVR subring U of S with quotient field Q

such that $U \subseteq S$ is an immediate extension and $\Omega_{F/Q} \neq 0$; see Theorem 3.10 and Corollary 3.11. But when S has dimension > 1, then the only way I know to satisfy the requirements of the definition is via the following theorem, which guarantees the existence of a strongly twisted subring when the quotient field of S is sufficiently large and of positive characteristic.

Theorem 6.3 ([43, Lemma 3.4 and Theorem 3.5]). *Let F/k be a field extension such that k has positive characteristic and at most countably many elements. Suppose that the cardinality of F and the dimension of the F-vector space $\Omega_{F/k}$ are the same (which is the case if F/k is a separably generated extension of infinite transcendence degree). If S is a k-subalgebra of F with quotient field F and K is a nonzero torsion-free S module of at most countable rank, then there exists a subring R of S that is strongly twisted by K.*

The proof of the theorem reduces to proving that under the hypotheses on S and its quotient field, there exists a subring A of S such that the A-module S/A is torsion-free and divisible and the extension $A \subseteq S$ has trivial generic fibers; i.e., $P \cap A \neq 0$ for all nonzero prime ideals P of S. In [43], such an extension is termed a *strongly analytic extension*. It is the condition of having trivial generic fibers where positive characteristic is needed, so as to arrange S to be a purely inseparable extension of A. Strongly analytic extensions of DVRs are exactly the immediate extensions, but in higher dimensions, the only strongly analytic extensions of Noetherian rings I am aware of are those constructed in the proof of the theorem.

Strongly analytic extensions provide an alternative, derivation-free way to view strongly twisted subrings: A subring R of the domain S is strongly twisted by an S-module if and only if there is a subring A of R such that $A \subseteq S$ is a strongly analytic extension, R and S share the same quotient field and the extension $R \subseteq S$ is *quadratic*, meaning that every R-submodule between R and S is a ring [43, Corollary 2.6].

Theorem 6.3 assures the existence of easy-to-locate strongly twisted subrings. For example, if k is a field of positive characteristic that is a separably generated extension of infinite transcendence degree over a countable subfield, and $X_1, \ldots, X_n$ are indeterminates for k, then every ring S between $k[X_1, \ldots, X_n]$ and $k(X_1, \ldots, X_n)$ has strongly twisted subrings; in fact, for each such ring S, there exists for each nonzero torsion-free S-module of at most countable rank a subring of S that is strongly twisted by K.

Granted existence, the next theorems deal with the properties of strongly twisted subrings, and we see that these are determined by the choice of K and S. Although we are mainly interested in the Noetherian case, a few general facts can be stated for strongly twisted subrings of a not-necessarily-Noetherian domain. The extension $R \subseteq S$, where R is a strongly twisted subring of S, proves to be a particularly strong sort of integral extension. It is, first of all, a quadratic extension, as defined above; that is, for all $s, t \in S$, it is the case that $st \in sR + tR + R$. A quadratic extension

is clearly an integral extension. In our context these quadratic extensions are also *subintegral*, in the sense of Swan [60]: In addition to the extension $R \subseteq S$ being integral, the contraction mapping $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is a bijection and the induced maps on residue field extensions are isomorphisms (so for every prime ideal P of S, $S_P = R_{P \cap R} + PS_P$). This is included in the following theorem, which collects together a number of observations from [43].

Theorem 6.4 ([43, Lemma 4.1 and Theorems 4.2 and 4.4]). *Let S be a domain with quotient field F, let K be a nonzero torsion-free S-module and let $FK = F \otimes_R K$. Suppose that R is a subring of S that is strongly twisted by K, and let D be the derivation that twists R. Then:*

(i) *R and S share the same quotient field.*

(ii) *The extension $R \subseteq S$ is subintegral and quadratic.*

(iii) *The derivation D induces an isomorphism of R-modules $S/R \to FK/K$.*

(iv) *Every ring T between R and S must be of the form $T = S \cap D^{-1}(L)$ for some unique S-module L with $K \subseteq L \subseteq FK$.*

(v) *Given an S-submodule L with $K \subseteq L \subseteq FK$, there is an intermediate ring $R \subseteq T \subseteq S$ such that T is strongly twisted by L.*

(vi) *The ring S is a finite R-module only when $R = S$.*

Whether a strongly twisted subring R of a Noetherian ring S is Noetherian is determined by the module K. This is the content of the next theorem, which relies on the following idea. When R is a subring of S strongly twisted by K and D is the derivation that twists R, then there is an embedding $R \to S \star K : r \mapsto (r, D(r))$. This mapping is faithfully flat, and for each $0 \neq a \in S \cap \mathrm{Ker}\, D$, it induces an isomorphism $R/aR \to S/aS \star K/aK$ [43, Theorem 4.6]. Thus the mapping $R \to S \star K$ is "locally" an isomorphism, a fact which is behind many of the results mentioned in this section. In this way, a strongly twisted subring of S is a kind of inversion of idealization: Rather than ramify S with K to produce $S \star K$, we use K to excavate a subring R of S which behaves in small enough neighborhoods like $S \star K$.

Theorem 6.5 ([43, Theorem 5.2]). *Let S be a domain, let K be a torsion-free S-module, and suppose that R is a subring of S strongly twisted by K. Let D be the derivation that strongly twists R. Then R is a Noetherian domain if and only if S is a Noetherian domain and for each $0 \neq a \in S \cap \mathrm{Ker}\, D$, K/aK is a finite S-module.*

Thus if S is a Noetherian domain and K is a finitely generated S-module, then R is a Noetherian domain. We will outline this case in Theorem 6.7. However, the theorem leaves just enough room for other, more subtle, choices of K; one such case is treated in Theorem 6.9. So we elaborate shortly on the structural relationship between R, S and K in two cases that depend on the choice of K. But both cases will force R to be Noetherian, so we consider first in Theorem 6.6 the general situation in which R

is Noetherian, or, equivalently, by Theorem 6.5, the case in which K/aK is a finite S-module for all $0 \neq a \in S \cap \operatorname{Ker} D$.

To state Theorem 6.6, we recall the following standard notions. Let I be an ideal of a ring A. Then an ideal $J \subseteq I$ is a reduction of I if there exists $n > 0$ such that $I^{n+1} = JI^n$. The smallest number n for which such an equation holds for J and I is the *reduction number* of I with respect to J. The ideal J is a *minimal reduction* of I if J itself has no proper reduction. If I is an ideal of a local Noetherian ring, then minimal reductions must exist [61, Theorem 8.3.5]. The minimum of the reduction numbers of the minimal reductions of the ideal I of A is denoted $r_A(I)$. The *analytic spread* of an ideal I in a local Noetherian ring $(A, \mathfrak{m})$, denoted $\ell_A(I)$, which is useful in detecting minimal reductions (see for example [6] or [61]), is defined to be the Krull dimension of the *fiber cone* of I with respect to A, where for an ideal I and an A-module L, the *fiber cone* of I with respect to L is:

$$\mathcal{F}_{I,L} := L[It]/\mathfrak{m}L[It] \cong \bigoplus_{n=0}^{\infty} I^n L/\mathfrak{m}I^n L.$$

In addition to facts about reductions of ideals in strongly twisted subrings, Theorem 6.6 calculates the local cohomology of such rings: If A is a local ring and I is an ideal of A, then H_I^i is the right derived functor of the I-torsion function Γ_I defined for each A-module L by $\Gamma_I(L) = \{\ell \in L : I^k \ell = 0 \text{ for some } k > 0\}$. If I is an ideal of the local Noetherian ring A and L is an A-module, then $\operatorname{depth}_I(L)$ is the greatest integer i such that for all $j < i$, $H_I^j(L) = 0$. When L is a finite A-module, then $\operatorname{depth}_I(L)$ is the length of a maximal regular sequence on L [5, Theorem 6.27].

The underlying theme of the next theorem, as well as Theorems 6.7 and 6.9, is that various properties of nonzero ideals I of a strongly twisted subring R of S which are contracted from S are determined by IS and K. We use "contracted" here in the basic sense: The ideal I of R is *contracted* from S if there is an ideal J of S such that $I = J \cap R$; equivalently, $I = IS \cap R$. Since $R \subseteq S$ is by Theorem 6.4 an integral extension, every integrally closed ideal of R is contracted from an ideal of S. In particular, every prime ideal of R is contracted from an ideal of S. Statement (vii) of the theorem can be found in [43, Corollary 4.3]; (viii) in [43, Corollary 4.7]; and the remaining statements are collected from [46, Sections 3 and 4].

Theorem 6.6. *Let S be a local Noetherian domain with maximal ideal N and quotient field F, and let K be a nonzero torsion-free S-module. Suppose that R is a Noetherian subring of S that is strongly twisted by K. Then statements* (i)–(vi) *of Theorem* 6.4 *hold for R, as do all of the following statements.*

(vii) *R is a local ring; R and S have the same residue field; and $N = MS$, where M is the maximal ideal of R.*

(viii) *There is an isomorphism of rings: $\widehat{R} \cong \widehat{S} \star \widehat{K}$, where $\widehat{R}$ is the completion of R in the M-adic topology and $\widehat{S}$ and $\widehat{K}$ denote the completions of S and K, respectively, in the N-adic topology.*

(ix) *For each nonzero ideal I of R contracted from S, there is an isomorphism of rings:*

$$\mathcal{F}_{I,R} \cong \mathcal{F}_{IS,S} \star \mathcal{F}_{IS,K}.$$

(x) *For each nonzero ideal I of R contracted from S, $\ell_R(I) = \ell_S(IS)$.*

(xi) *Suppose R (equivalently, S) has infinite residue field. If I is a nonzero ideal of R contracted from S, then $r_S(IS) \le r_R(I) \le r_S(IS) + 1$.*

(xii) *If I is a nonzero ideal of R, then there is an isomorphism of R-modules:*

$$H_I^i(R) \cong H_{IS}^i(S) \oplus H_{IS}^i(K).$$

(xiii) *If I is an ideal of R, then $\mathrm{depth}_I(R) = \min\{\mathrm{depth}_{IS}(S), \mathrm{depth}_{IS}(K)\}$.*

Examples show the bound on $r_R(I)$ in (xi) cannot be improved [46, Section 3]. Note also that (xi) implies that if I is an ideal of R contracted from a principal ideal of S, then $I^2 = iI$ for some $i \in I$. Thus, in the terminology of Section 3, I is a stable ideal of R. Therefore, if S is a DVR, then R is a stable domain. This is one reason for the the emphasis on stable domains in Section 3, since the existence results in that section which involve stable domains rely on the method of strongly twisted subrings to produce these rings. More generally, strongly twisted subrings of Dedekind domains must be stable domains [43, Theorem 7.1].

We specialize next to the case where K is a finitely generated S-module. Since by Theorem 6.5, a subring R of a Noetherian domain S strongly twisted by a finitely generated S-module K is Noetherian, all the properties listed in Theorem 6.6 hold for R. But the fact that K is finitely generated allows for the stronger conclusions of the next theorem, which utilizes the following standard terminology. When $(A, \mathfrak{m})$ is a local Noetherian ring and L is a finitely generated A-module, then $\mu(L)$ denotes the minimal number of generators needed to generate L; that is $\mu(L)$ is the dimension of $A/\mathfrak{m}$-vector space $L/\mathfrak{m}L$. The *embedding dimension* of A, denoted emb.dim A, is $\mu(\mathfrak{m})$. When J is an $\mathfrak{m}$-primary ideal of A, the *Hilbert function* of the module L with respect to J, denoted $H_{J,L}$, is given then by

$$H_{J,L}(n) = \text{ length } J^n L / J^{n+1} L,$$

with the convention $J^0 = A$. For large enough n, the Hilbert function $H_{J,L}$ agrees with a polynomial having rational coefficients [12, Proposition 12.2 and Exercise 12.6]. The leading coefficient of this polynomial is of the form $e/(d-1)!$ for some positive integer e, which is designated the *multiplicity* of J on L. We write $e(J, L)$ for e to emphasize the dependence on J and L. The *multiplicity of the local ring A* is denoted $e(A)$, and is defined by $e(A) = e(\mathfrak{m}, A)$. Statements (xiv)–(xvii) of the next theorem can be found in [46, Section 6]; (xviii)–(xxiii) can be deduced from the preceding statements and [43, Theorem 7.2]; (xxiv) is proved in [43, Corollary 7.3]; (xxv) follows from [43, Proposition 5.3].

Theorem 6.7. *Let S be a local Noetherian domain with maximal ideal N and quotient field F, and let K be a nonzero finitely generated torsion-free S-module. Suppose that R is a subring of S strongly twisted by K. Then R is a local Noetherian domain and statements* (i)–(vi) *of Theorem 6.4 and statements* (vii)–(xiii) *of Theorem 6.6 hold for R, as do all of the following statements.*

(xiv) *If I is a nonzero ideal of R contracted from S, then $\mu_R(I) = \mu_S(IS) + \mu_S(K)$.*

(xv) emb.dim $R = $ emb.dim $S + \mu_S(K)$.

(xvi) *If I and J are ideals of R contracted from S, with J an M-primary ideal, then:*
$$e(I, J) = e(IS, S) \cdot (1 + \text{rank}(K)).$$

(xvii) *The multiplicity of R is $e(R) = e(S) \cdot (1 + \text{rank}(K))$.*

(xviii) *R is a Cohen–Macaulay ring if and only if S is a Cohen–Macaulay ring and K is a maximal Cohen–Macaulay S-module.*

(xix) *R is a Gorenstein ring if and only if S is a Cohen–Macaulay ring that admits a canonical module ω_S and $K \cong \omega_S$. Moreover, if R is a Gorenstein ring, then $e(R) = 2e(S)$.*

(xx) *R is a complete intersection if and only if S is a complete intersection and $K \cong S$.*

(xxi) *R is a hypersurface if and only if S is a regular local ring and $K \cong S$.*

(xxii) *If R is a hypersurface, then R has minimal multiplicty, and in fact, $e(R) = 2$ and emb.dim $R = d + 1$, where d is the dimension of S.*

(xxiii) *If S is a regular local ring, and K is a finitely generated free S-module, then R is a Cohen–Macaulay ring of minimal multiplicity.*

(xxiv) *The Cohen–Macaulay rings properly between R and S are in one-to-one correspondence (see Theorem* 6.4 (vii) *and* (viii)*) with the maximal Cohen–Macaulay modules properly between K and FK.*

(xxv) *If S has Krull dimension > 1, then there exists a non-Noetherian ring between R and S.*

The following example illustrates the theorem with a simple choice of S and K.

Example 6.8. Let k be a field of postive characteristic that is a separably generated extension of infinite transcendence degree over a countable subfield. Let $X_1, \ldots, X_d$ be indeterminates for K, and define $S = k[X_1, \ldots, X_d]_{(X_1,\ldots,X_d)}$. Let K be a free S-module of rank $n > 0$. Then by Theorems 6.3, 6.4 and 6.6, there is a local Noetherian subring R of S strongly twisted by K such that every nonzero integrally closed ideal of R, in particular every prime ideal of R, needs at least $n + 1$ generators. Moreover, $R \subseteq S$ is a quadratic subintegral extension, and R and S both share the same quotient

field. The embedding dimension of R is $d + n$, its multiplicity is $1 + n$ and R is a Cohen–Macaulay ring. If n is chosen to be 1, then R is a hypersurface.

One of Nagata's bad Noetherian rings is a two-dimensional local Noetherian domain R that has a non-Noetherian domain between R and its normalization [36, Example 4, page 206]. Theorem 6.7(xxv) provides another source of such examples; e.g., set $d = 2$ in Example 6.8.

Next we consider a case in which K is not finitely generated yet still produces a strongly twisted subring that is Noetherian. Though not finitely generated, the module K has the property that K/sK is finitely generated for all $0 \neq s \in S$, which in turn guarantees by Theorem 6.5 that R is a Noetherian ring. In addition to being an S-module, K is also a V-module, where V is a DVR that finitely dominates S. Such DVRs are the subject of Theorem 4.3, and we recall from that theorem that if S is essentially of finite type over a field, then such a DVR must exist. This assures that there are plenty of natural choices for S and K to which the construction can be applied. That the ring R in the theorem is Noetherian follows from Theorem 6.5; for an explicit argument see [43, Example 5.4]. Statements (xiv) and (xvi) can be found in [46, Section 7]; (xv) and (xvii) follow from (xiv) and (xvi), respectively; (xviii) is in [43, Proposition 6.4]; (xix) follows from (xviii); (xx) and (xxi) follow from (xix); (xxii) is proved in [45, Proposition 6.6]; (xxiii) can be found in [46, Section 7]; (xxiv) follows from (xxiii); and (xxv) is in [43, Proposition 5.6].

Theorem 6.9. *Let S be a local Noetherian domain with maximal ideal N and quotient field F, and such that there exists a DVR V that finitely dominates S. Let $m = \dim_{S/N} V/NV$, let K be a nonzero torsion-free finite rank V-module with $K \neq FK$, and let $r_K = \dim_{V/\mathfrak{M}} K/\mathfrak{M}K$, where $\mathfrak{M}$ is the maximal ideal of V. Suppose that R is a subring of S that is strongly twisted by K. Then R is a local Noetherian domain and statements* (i)–(vi) *of Theorem* 6.4 *and statements* (vii)–(xiii) *of Theorem* 6.6 *hold for R, as do all of the following statements.*

(xiv) *For each nonzero ideal I of R contracted from S, $\mu_R(I) = \mu_S(IS) + m \cdot r_K$, and if K is a free V-module, then $r_K = \text{rank}(K)$.*

(xv) *emb.dim R = emb.dim $S + m \cdot r_K$.*

(xvi) *If I and J are ideals of R contracted from S and J is M-primary, then:*

$$e(J, I) = e(JS, S) + \begin{cases} r_K \cdot \text{length } V/JV & \text{if } S \text{ has Krull dimension } 1 \\ 0 & \text{if } S \text{ has Krull dimension} > 1. \end{cases}$$

(xvii) *The multiplicity of the local ring R is*

$$e(R) = e(S) + \begin{cases} m \cdot r_K & \text{if } S \text{ has Krull dimension } 1 \\ 0 & \text{if } S \text{ has Krull dimension} > 1. \end{cases}$$

(xviii) *For each nonmaximal prime ideal P of R, $R_P = S_{P'}$, where P' is the unique prime ideal of S lying over R.*

 (xix) *For each i less than the Krull dimension of S, Serre's regularity condition R_i holds for S if and only if it holds for R.*

  (xx) *If S is integrally closed and has Krull dimension > 1, then for each height 1 prime ideal P of R, R_P is a DVR.*

 (xxi) *If S is a regular local ring, then R has an isolated singularity.*

(xxii) *The maximal ideal M of R is the associated prime of a nonzero principal ideal.*

(xxiii) *The local cohomology modules for a nonzero ideal I of R are given by*

$$H_I^i(R) \cong \begin{cases} 0 & \text{if } i = 0 \\ H_{IS}^1(S) \oplus FK/K & \text{if } i = 1 \\ H_{IS}^i(S) & \text{if } i > 1. \end{cases}$$

(xxiv) $\mathrm{depth}_M(R) = 1$.

 (xxv) *If V tightly dominates R, then every intermediate ring T, $R \subseteq T \subsetneq S$, is a local Noetherian ring that is strongly twisted by some V-module L with $K \subseteq L \subsetneq FK$.*

Here is a simple example:

Example 6.10. Let k be a field of positive characteristic, and suppose that k is separably generated and of infinite transcendence degree over a countable subfield. Let $S = k[X_1, \ldots, X_d]_{(X_1, \ldots, X_d)}$, where $d > 1$. Then by Theorem 4.3, there exists a DVR V that meets the requirements of Theorem 6.9. Let K be a torsion-free V-module of finite rank $n > 0$. Then by Theorem 6.3, there exists a local Noetherian subring R of S strongly twisted by K and satisfying all the statements of Theorems 6.4, 6.6 and 6.9. Moreover, as discussed at the beginning of Section 4, the DVR V can be chosen to tightly dominate S, so that $m = 1$ in Theorem 6.9.

Nagata constructs an example of a local Noetherian domain of multiplicity 1 that is not a regular local ring [36, Example 2, page 203]. Example 6.10, with $K = S$, is another such example when the DVR V is chosen so that it tightly dominates S.

Abyhankar constructs in [1] for each pair of integers $n > d > 1$ a local ring of embedding dimension n, Krull dimension d and multiplicty 2. Example 6.10 accomplishes something similar, but with multiplicity 1 and all the rings R occur in subintegral extensions $R \subseteq S$, with S fixed: Choose V to be a DVR tightly dominating S and for $n > d$, choose K to be a free V-module of rank $n - d$.

We conclude with a note on generality. To simplify the presentation, we have restricted everything to strongly twisted subrings, but there is a weaker notion of twisted subring for which suitable variations on many of the preceding ideas apply. Let S be

a ring, let K be an S-module, and let C be a multiplicatively closed subset of nonzerodivisors of S that are also nonzerodivisors on K. Then a subring R of S is *twisted by K along C* if there is a C-linear derivation $D : S_C \to K_C$ such that:

(i) $R = S \cap D^{-1}(K)$,

(ii) $D(S_C)$ generates K_C as an S_C-module, and

(iii) $S \subseteq \operatorname{Ker} D + cS$ for all $c \in C$.

A strongly twisted subring of a domain S is twisted along $C = S \setminus \{0\}$, but the converse need not be true; more precisely, being twisted along $C = S \setminus \{0\}$ is not sufficient to guarantee condition (iii) in the definition of strongly twisted subring.

Relativized versions of many of the properties discussed in this section hold for a subring R of S twisted along C. Instead of working with nonzero ideals of R contracted from S, one usually must restrict to ideals of R contracted from S *and* meeting C. For example, when S is Noetherian and K is a finitely generated S-module, then it is in general possible to conclude only that every ideal of R meeting C is finitely generated. Thus Noetherianness of R is no longer guaranteed; instead, there is a filter of ideals which behave like ideals in a Noetherian ring. However, in the special circumstance when S is a two-dimensional local UFD finitely dominated by a DVR V, then a subring R of S twisted by a torsion-free finite rank V-module along any multiplicatively closed subset containing a nonunit of S is Noetherian [43, Theorem 5.7]. This is an abstract version of the example of Ferrand and Raynaud of a two-dimensional local Noetherian domain whose completion has embedded primes [13, Proposition 3.1].

Bibliography

[1] Abhyankar, S., Local rings of high embedding dimension. Amer J Math. 1967;89:1073–1077.

[2] Akizuki, Y., Einige Bemerkungen über primäre Integritätsbereiche mit Teilerkettensatz. Proc Phys Math Soc Japan. 1935;17:327–336.

[3] Bass, H., On the ubiquity of Gorenstein rings. Math Z. 1963;82:8–28.

[4] Bennett, B., On the structure of non-excellent curve singularities in characteristic p. Publ Math Inst Hautes Études Sci. 1973;42:129–170.

[5] Brodmann, M. P., Sharp, R. Y., Local cohomology: an algebraic introduction with geometric applications. vol. 60 of Cambridge studies in advanced mathematics. Cambridge: Cambridge University Press. 1998.

[6] Bruns, W., Herzog, J., Cohen–Macaulay rings. vol. 39 of Cambridge studies in advanced mathematics. Cambridge: Cambridge University Press; 1993.

[7] Chevalley, C., On the theory of local rings. Ann of Math. 1943;44:690–708.

[8] Chevalley, C., Intersections of algebraic and algebroid varieties. Trans Amer Math Soc. 1945;57:1–85.

[9] Cohen, I. S., On the structure and ideal theory of complete local rings. Trans Amer Math Soc. 1946;59:54–106.

[10] de Souza Doering, A., Lequain, Y., Maximally differential prime ideals. J Algebra. 1986; 101:403–417.

[11] Drozd, J. A., Kiričenko, V. V., On quasi-Bass orders. Izv Math USSR. 1972;6:323–365.

[12] Eisenbud, D., Commutative algebra. With a view toward algebraic geometry. vol. 150 of Graduate texts in mathematics. New York: Springer-Verlag; 1995.

[13] Ferrand, D., Raynaud, M., Fibres formelles d'un anneau local noethérien. Ann Sci Éc Norm Supér (4). 1970;3:295–311.

[14] Goodearl, K. R., Lenagan, T. H., Constructing bad Noetherian local domains using derivations. J Algebra. 1989;123(2):478–495.

[15] Grothendieck, A., Dieudonné, J., Élèments de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné): IV. Étude locale des schémas et des morphismes de schémas, Seconde partie. Publ. Math. Inst. Hautes Études Sci. 1965;24:5–231.

[16] Heinzer, W., Lantz, D., Jónsson extensions of one-dimensional semilocal domains. J Algebra. 1988;117:179–197.

[17] Heinzer, W., Lantz, D., Shah, K., The Ratliff–Rush ideals in a Noetherian ring. Comm Algebra. 1992;20:491–522.

[18] Heinzer, W., Rotthaus, C., Sally, J., Formal fibers and birational extensions. Nagoya Math J. 1993;131:1–38.

[19] Heitmann, R., Characterization of completions of unique factorization domains. Trans Amer Math Soc. 1993;337:379–387.

[20] Kunz, E., Kähler differentials. Advanced lectures in mathematics. Braunschweig: Friedr. Vieweg & Sohn; 1986.

[21] Krull, W., Dimensionstheorie in Stellenringen. J. Reine Angew Math. 1938;179:204–226.

[22] Larfeldt, T., Lech, C., Analytic ramifications and flat couples of local rings. Acta Math. 1981;146(3):-4, 201–208.

[23] Lech, C., A method for constructing bad noetherian local rings. vol. 1183 of Lecture notes in mathematics. 1986. 241–247.

[24] Lee, D., Leer, L., Pilch, S., Yasufuku, Y., Characterization of completions of reduced local rings. Proc Amer Math Soc. 2001;129(11):3193–3200

[25] Lequain, Y., Differential simplicity and complete integral closure. Pacific J Math. 1971; 36:741–751.

[26] Lipman, J., Stable ideals and Arf rings. Amer J Math. 1971;93:649–685.

[27] Lipman, J., Desingularization of two-dimensional schemes. Ann of Math (2). 1978; 107(1):151–207.

[28] Loepp, S., Characterization of completions of excellent domains of characteristic zero. J Algebra. 2003;265(1):221–228.

[29] Loepp, S., Rottaus, C., Sword, S., A class of local Noetherian domains. J Commut Algebra. 2009;1:647–678.

[30] Matlis, E. 1-dimensional Cohen–Macaulay rings. vol. 327 of Lecture notes in mathematics. Springer-Verlag; 1973.

[31] Matlis, E., The theory of Q-rings. Trans Amer Math Soc. 1974;187(1):147–181.

[32] Matsumura, H., On the dimension of formal fibres of a local ring. In: Algebraic geometry and commutative algebra in honor of Masayoshi Nagata, Vol. I. Tokyo: Kinokuniya; 1988. p. 261–266.

[33] Mumford, D., The red book of varieties and schemes. 2nd, expanded ed [includes the Michigan lectures (1974) on curves and their Jacobians, with contributions by Arbarello E]. vol. 1358 of Lecture notes in mathematics. Berlin: Springer-Verlag; 1999.

[34] Nagata, M., An example of normal local ring which is analytically ramified. Nagoya Math J. 1955;9:111–113.

[35] Nagata, M., A general theory of algebraic geometry over Dedekind domains. II. Separably generated extensions and regular local rings. Amer J Math. 1958;80:382–420.

[36] Nagata, M., Local rings. vol. 13 of Interscience tracts in pure and applied mathematics. New York-London: John Wiley & Sons; 1962.

[37] Nash, J., Arc structure of singularities. Duke Math J. 1995;81:207–212.

[38] Noether, E., Idealtheorie in Ringbereichen. Math Ann. 1921;83:24–66.

[39] Noether, E., Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. Math Ann. 1927;96:26–61.

[40] Nowak, K., A simple algebraic proof of Zariski's main theorem on birational transformations. Univ Iagel Acta Math. 1996;33:115-118.

[41] Olberding, B., Stability of ideals and its applications. Proceedings, Ideal Theoretic Methods in Commutative Algebra; 1999, Columbia, MO. vol. 220 of Lecture notes in pure and applied mathematics. Dekker, New York; 2001. p. 319–341.

[42] Olberding, B., On the structure of stable domains. Comm Algebra. 2002;30(2):877–895.

[43] Olberding, B., A counterpart to Nagata idealization. Submitted.

[44] Olberding, B., Generic formal fibers and analytically ramified stable rings. Submitted.

[45] Olberding, B., One-dimensional bad Noetherian domains. Submitted.

[46] Olberding, B., On invariants of contracted ideals in subintegral extensions of Noetherian domains. Preprint.

[47] Ore, O., Abstract ideal theory. Bull Amer Math Soc. 1933;39(10):728–745.

[48] Ore, O., Review: W. Krull, Idealtheorie. Bull Amer Math Soc. 1937;43(7):460–461.

[49] Posner, E., Integral closure of differential rings. Pacific J Math. 1960;10(4):1393–1396.

[50] Posner, E., Integral closure of rings of solutions of linear differential equations. Pacific J Math. 1962;12(4):1417–1422.

[51] Rees, D., A note on analytically unramified local rings. J Lond Math Soc. 1961;36:24–28.

[52] Reguera, A., Towards the singular locus of the space of arcs. Amer J Math. 2009;131: 313–350.

[53] Reid, M., Akizuki's counterexample. arXiv:alg-geom/9503017v1.

[54] Reid, M., Undergraduate commutative algebra. vol. 29 of London Mathematical Society student texts. Cambridge: Cambridge University Press; 1995.

[55] Sally, J., Vasconcelos, W., Stable rings and a problem of Bass. Bull Amer Math Soc. 1973;79:575–576.

[56] Sally, J., Vasconcelos, W., Stable rings. J Pure Appl Algebra. 1974;4:319-336.

[57] Sally, J., Numbers of generators of ideals in local rings. New York-Basel: Marcel Dekker, Inc.; 1978.

[58] Schmidt, F. K., Über die Erhaltung der Kettensätze der Idealtheorie bei beliebigen endlichen Körpererweiterungen. Math Z. 1936;41:443–450.

[59] Seidenberg, A., Derivations and integral closure. Pacific J Math. 1966;16:167–173.

[60] Swan, R. G., On seminormality. J Algebra 1980;67:210–229.

[61] Swanson, I., Huneke, C., Integral closure of ideals, rings, and modules. vol. 336 of London Mathematical Society lecture note series. Cambridge: Cambridge University Press; 2006.

[62] Vasconcelos, W., Derivations of commutative Noetherian rings. Math Z. 1969;112:229–233.

[63] Zariski, O., The concept of a simple point of an abstract algebraic variety. Trans Amer Math Soc. 1947;62:1–52.

[64] Zariski, O., Analytical irreducibility of normal varieties. Ann of Math (2). 1948;49:352–361.

[65] Zariski, O., Sur la normalité analytique des variétés normales. Ann Inst Fourier. 1950;2: 161–164.

[66] Zariski, O., Theory and applications of holomorphic functions on algebraic varieties over arbitrary ground fields. Memoires of the American Mathematical Society. 1951.

[67] Zariski, O., Samuel, P., Commutative Algebra Vol. 2. Princeton: Van Nostrand; 1958.

Author Information

Bruce Olberding, Department of Mathematical Sciences, New Mexico State University, Las Cruces, NM, USA.
E-mail: olberdin@nmsu.edu

Krull Dimension of Polynomial and Power Series Rings

John J. Watkins

Abstract. We present here a fundamental theorem due to J. W. Brewer, W. J. Heinzer, P. R. Montgomery, and E. A. Rutter, on the height (or codimension) of prime ideals in polynomial rings, and use this theorem to give elementary proofs of several well known results concerning Krull dimension for polynomial rings.

Keywords. Prime Ideals, Krull Dimension, Polynomial Rings, Power Series Rings.

2010 Mathematics Subject Classification. 13C15.

1 Introduction

> *When we say that space has*
> *three dimensions, what do we mean?*
>
> Henri Poincaré (1854–1912)

As the above quotation from the great French mathematician Henri Poincaré indicates, the notion of n-dimensional space was merely an intuitive one as late as the nineteenth century. From the ancient Greeks we have inherited the idea that lines and curves are made up of points, and that in turn surfaces are bounded by curves and that volumes are bounded by surfaces. It is all well and good to say that of course n-dimensional Euclidean space has dimension n, and that any set of points in a Euclidean space has dimension n if n parameters are needed to describe the set, but what does that mean?

The notion of dimension is of obvious importance in geometry, and Poincaré was not the only nineteenth century mathematician to recognize just how elusive this concept is. Georg Cantor used his revolutionary idea of one-to-one correspondence to show that all n-dimensional spaces have the same number of points as a line, and hence are indistinguishable as sets; or, as he put it in a letter to Dedekind in 1877:

> The distinction between domains of different dimensions must be sought
> for in quite another way than by the characteristic number of independent
> coordinates.

And, by the 1890s, the truly remarkable space filling curves produced by Peano and Hilbert made it completely clear just how elusive the notion of dimension is. This extremely unsettling situation was resolved in 1912 by L. E. J. Brouwer who finally

provided us with a precise topological definition of dimension. In 1912, Brouwer also proved the famous 'Brouwer fixed point theorem' which states that every continuous function from a convex compact set in a Euclidean space (e.g., a closed ball) to itself has a fixed point.

Because of the link between algebra and geometry, it then became natural to look for an algebraic analogue of the topological notion of dimension. This algebraic analogue was first introduced in ring theory by Wolfgang Krull in 1937. Krull's definition is now so commonly viewed as the 'correct' definition that the standard terminology for it, *Krull dimension*, is often shortened to simply *dimension*.

Definition 1.1. Let R be a commutative ring with 1. The *Krull dimension* of R is the supremum of the lengths of chains of prime ideals in R. We write $\dim R$ for the dimension of R. The *length* of a chain of distinct prime ideals

$$P_0 \subset P_1 \subset P_2 \subset \cdots \subset P_n$$

is said to be n.

Note that this corresponds to the dimension of a vector space over a field being the length of the longest chain of proper subspaces. Similarly, in algebraic geometry the dimension of an algebraic variety X over an algebraically closed field k is the supremum of the lengths of chains $Z_0 \subset Z_1 \subset Z_2 \subset \cdots \subset Z_n$ of irreducible closed subsets of X, and by Hilbert's Nullstellensatz such a chain corresponds exactly to a chain $I(Z_0) \supset I(Z_1) \supset I(Z_2) \supset \cdots \supset I(Z_n)$ of prime ideals.

Let's look at several examples. If K is a field, then $\dim K = 0$ (since the ideal $P_0 = (0)$ is the only proper ideal in K); conversely, if R is an integral domain, and $\dim R = 0$, then R is a field. On the other hand, if R is a principal ideal domain that is not a field, then any nonzero prime ideal is of the form (p) where p is irreducible, and so (p) is maximal; hence, the longest chains of prime ideals in R look like $(0) \subset (p)$ and $\dim R = 1$. Thus, both $\mathbb{Z}$, the ring of integers, and $K[x]$, the polynomial ring over a field K, have dimension 1.

Note that, in particular, for a field K,

$$\dim K[x] = \dim K + 1.$$

This is a special case of an extremely important result about the dimension of the polynomial ring $K[x_1, x_2, \ldots, x_n]$ in n indeterminates over a field K. The chain of ideals

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, x_2, \ldots, x_n)$$

is a chain of distinct prime ideals of length n in this ring. In fact, it turns out that there are no longer chains of prime ideals in this ring. In other words, the polynomial ring $K[x_1, x_2, \ldots, x_n]$ has dimension n; that is,

$$\dim K[x_1, x_2, \ldots, x_n] = \dim K + n.$$

Proofs of this classical theorem are typically rather involved and can be given only after the Hilbert basis theorem and Krull's principal ideal theorem have been proven (see [5] and [9]). This approach has the unfortunate consequence of giving the impression that this fundamentally important result about the dimension of polynomial rings is as deep as these two enormously famous theorems. At the 1972 Conference on Commutative Algebra held at the University of Kansas, J.W. Brewer, W.J. Heinzer, P.R. Montgomery, and E.A. Rutter presented an elementary proof of this and other classical results concerning the Krull dimension of polynomial rings [3]. Their approach in this truly remarkable paper is very much in the same extraordinarily elegant style as Irving Kaplansky in [8].

2 A Key Property of $R[x]$

Let R be a commutative ring with 1. A very useful and easily proven basic fact concerning localizations of the polynomial ring $R[x]$ is that if T is a multiplicative system of R, then

$$(R[x])_T \cong R_T[x].$$

For example, if R is an integral domain, then we can let T be the multiplicative system of all nonzero elements of R. In this case, then, $(R[x])_T$ is just $K[x]$, where K is the quotient field of R. So, the process of localization yields a one-to-one order-preserving correspondence between the prime ideals in $K[x]$ and the prime ideals of $R[x]$ which are disjoint from T. But, a prime ideal Q in $R[x]$ is disjoint from T if and only if $Q \cap R = (0)$. Thus, we conclude that there is a one-to-one order-preserving correspondence between the prime ideals in $K[x]$ and the prime ideals of $R[x]$ whose intersection with R is (0).

An immediate consequence of this is the following very elementary theorem from [8], which is of fundamental importance in the study of chains of prime ideals in polynomial rings. The theorem says simply that it is impossible to have a chain of three distinct prime ideals in a polynomial ring $R[x]$ whose intersections with R are all equal.

Theorem 2.1. *Let R be a ring, and let $Q_1 \supset Q_2 \supset Q_3$ be a chain of three distinct prime ideals in $R[x]$. Then, $Q_1 \cap R \neq Q_3 \cap R$.*

Proof. We switch to the ring $(R/Q_3)[x]$, the ring of polynomials over the integral domain R/Q_3. In the ring $(R/Q_3)[x]$ we have a chain of distinct prime ideals, namely

$$Q_1/Q_3 \supset Q_2/Q_3 \supset Q_3/Q_3 = (0).$$

Assume, by way of contradiction, that $Q_1 \cap R = Q_3 \cap R$. This means that all three ideals Q_1/Q_3, Q_2/Q_3, and Q_3/Q_3 have intersection (0) with R/Q_3.

Since R/Q_3 is an integral domain, we can let L be the quotient field of R/Q_3, and so, by virtue of the one-to-one correspondence discussed above, these three ideals

whose intersection with R/Q_3 is (0) correspond to a chain of three distinct prime ideals in $L[x]$. But, this is clearly impossible because, as we saw earlier, $\dim L[x] = 1$. This completes the proof of the theorem. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Theorem 2.1 allows us to give upper and lower bounds on the dimension of a polynomial ring $R[x]$ in terms of the dimension of R. For the lower bound, we will use the basic fact that an ideal P is a prime ideal of R if and only if $P[x]$ is a prime ideal of $R[x]$.

Theorem 2.2. *Let R be a commutative ring with 1, and let $\dim R = n$. Then,*

$$n + 1 \leq \dim R[x] \leq 2n + 1.$$

Proof. Let

$$Q_0 \subset Q_1 \subset Q_2 \subset \cdots \subset Q_m$$

be a chain of distinct prime ideals in $R[x]$. Then, by Theorem 2.1,

$$Q_0 \cap R \subset Q_2 \cap R \subset Q_4 \cap R \subset \cdots \subset Q_{2\lfloor \frac{m}{2} \rfloor} \cap R$$

is a chain of length $\lfloor \frac{m}{2} \rfloor$ of distinct prime ideals in R. Therefore, we see that $\lfloor \frac{m}{2} \rfloor \leq n$. It follows that $m \leq 2n + 1$. Thus, $\dim R[x] \leq 2n + 1$, as desired.

Now, for the lower bound, let

$$P_0 \subset P_1 \subset P_2 \subset \cdots \subset P_n$$

be a chain of length n of distinct prime ideals in R. Then,

$$P_0[x] \subset P_1[x] \subset P_2[x] \subset \cdots \subset P_n[x] \subset P_n[x] + (x)$$

is a chain of length $n+1$ of distinct prime ideals in $R[x]$. Therefore, $\dim R[x] \geq n+1$, as desired. This completes the proof of the theorem. $\qquad\qquad\qquad\qquad\square$

Theorem 2.2 is best possible in the following sense: for any integer $n \geq 0$ and any integer m such that $n + 1 \leq m \leq 2n + 1$, there is a ring R of dimension n such that the dimension of $R[x]$ is m. In other words, in the absence of additional conditions on the ring R, Theorem 2.2 says all that can be said about the dimension of $R[x]$.

3 The Main Theorem

We now turn to the major result in [3]. We begin with a definition of the *height* of a prime ideal.

Definition 3.1. Let R be a commutative ring with 1, and let P be a prime ideal of R. The *height* of P – written $\mathrm{ht}(P)$ – is the supremum of the lengths of chains of prime ideals in R *descending* from P. Thus, if P has height k, there is a chain of distinct prime ideals

$$P = P_0 \supset P_1 \supset P_2 \supset \cdots \supset P_k,$$

but none longer.

For example, minimal prime ideals have height 0; whereas, maximal ideals in the ring of integers $\mathbb{Z}$ or in a polynomial ring $K[x]$ over a field K all have height 1. The height of a prime P is also sometimes referred to as the *codimension* of P, or, in an older terminology, as the *rank* of P.

Next, we prove a useful intermediate result from [3] concerning the height of a prime ideal in a polynomial ring. We have already observed that if P is a prime ideal of a ring R, then $P[x]$ is a prime ideal of $R[x]$. Moreover, it is easy to see that $P[x] \cap R = P$. What can be said about the height of a larger prime ideal Q of $R[x]$ whose intersection with R also equals P?

Theorem 3.2. *Let $x, x_2, \ldots, x_n$ be n indeterminates, and let R be a commutative ring with 1. Let Q be a prime ideal of $R[x]$, and let the ideal P of R be the prime ideal $P = Q \cap R$.*

If $Q \supset P[x]$ – that is, if Q and $P[x]$ are distinct primes of $R[x]$ – then,

$$\mathrm{ht}(Q) = \mathrm{ht}(P[x]) + 1,$$

and, for $n > 1$,

$$\mathrm{ht}(Q[x_2, \ldots, x_n]) = \mathrm{ht}(P[x, x_2, \ldots, x_n]) + 1.$$

Proof. Not surprisingly, the proof depends almost entirely upon Theorem 2.1. If $\mathrm{ht}(P) = \infty$, then both results are obvious. So, we assume that $\mathrm{ht}(P)$ is finite, and use induction on $\mathrm{ht}(P)$ to prove the first result.

First, we suppose that $\mathrm{ht}(P) = 0$. It follows that $\mathrm{ht}(P[x]) = 0$, for, if not, we have

$$Q \supset P[x] \supset Q_1$$

for some prime ideal Q_1 of $R[x]$. But, then, by Theorem 2.1, $Q \cap R \neq Q_1 \cap R$. Therefore, $Q_1 \cap R$ is a prime ideal properly contained in P, contradicting that $\mathrm{ht}(P) = 0$. Hence, $\mathrm{ht}(P[x]) = 0$.

Similarly, and still assuming that $\mathrm{ht}(P) = 0$, we can see that $\mathrm{ht}(Q) = 1$. This is true because if Q_2 is a prime ideal such that $Q_2 \subset Q$, then the prime ideal $Q_2 \cap R$ must be P since $\mathrm{ht}(P) = 0$ and $Q_2 \cap R \subseteq Q \cap R = P$. So, a chain of length 2 of distinct prime ideals $Q \supset Q_1 \supset Q_2$ is impossible, by Theorem 2.1. Thus, $\mathrm{ht}(Q) = 1$, and in this case, $\mathrm{ht}(Q) = \mathrm{ht}(P[x]) + 1$, as desired.

Now, let $\text{ht}(P) = m$, for some integer $m > 0$, and assume that the first result holds for all $0 \leq k < m$. We claim that, for any prime Q_1 such that $Q_1 \subset Q$, $\text{ht}(Q_1) \leq \text{ht}(P[x])$. In order to prove this claim, let $P_1 = Q_1 \cap R$. Thus, $P_1 \subseteq P$. If $P_1 = P$, then $P[x] \subseteq Q_1$ forces $Q_1 = P[x]$, since otherwise we have a chain $P[x] \subset Q_1 \subset Q$ of three distinct prime ideals whose intersections with R are all equal, contrary to Theorem 2.1; and so, trivially, we conclude that $\text{ht}(Q_1) = \text{ht}(P[x])$. This means that $\text{ht}(Q_1) \leq \text{ht}(P[x])$, as claimed. On the other hand, if $P_1 \subset P$, then either $Q_1 = P_1[x]$, or $Q_1 \supset P_1[x]$. In the first case, of course,

$$\text{ht}(Q_1) = \text{ht}(P_1[x]) < \text{ht}(P[x]);$$

and, in the latter case, we can use induction (since $\text{ht}(P_1) < m$) to get

$$\text{ht}(Q_1) = \text{ht}(P_1[x]) + 1 \leq \text{ht}(P[x]).$$

Thus, the claim is verified.

It follows immediately from this claim that a chain of distinct primes in $R[x]$ descending from Q can be no longer than $\text{ht}(P[x]) + 1$, that is, $\text{ht}(Q) \leq \text{ht}(P[x]) + 1$. And, since $Q \supset P[x]$, it has been obvious all along that $\text{ht}(Q) \geq \text{ht}(P[x]) + 1$. Thus, $\text{ht}(Q) = \text{ht}(P[x]) + 1$. This completes the verification of the first result of the theorem.

Next, turning to the second result of the theorem, we temporarily will consider the ring $R[x, x_2, \ldots, x_n]$ as $R[x][x_2, \ldots, x_n]$ (this allows us to still think of having $Q \subset R[x]$ and $P = Q \cap R$). Then, we can see that

$$Q[x_2, \ldots, x_n] \cap R[x_2, \ldots, x_n] = (Q \cap R)[x_2, \ldots, x_n] = P[x_2, \ldots, x_n].$$

Now, considering the ring $R[x, x_2, \ldots, x_n]$ as $R[x_2, \ldots, x_n][x]$, we can apply the first result of the theorem – which we just proved – since $Q[x_2, \ldots, x_n]$ is a prime ideal of $R[x_2, \ldots, x_n][x]$, and

$$Q[x_2, \ldots, x_n] \supset P[x_2, \ldots, x_n][x],$$

since $Q \supset P[x]$.

Therefore, by the first result of the theorem, we have

$$\text{ht}(Q[x_2, \ldots, x_n]) = \text{ht}(P[x_2, \ldots, x_n][x]) + 1,$$

which is the second result since $P[x_2, \ldots, x_n][x] = P[x, x_2, \ldots, x_n]$. This completes the proof of the theorem. □

We now use Theorem 3.2 to prove the main theorem in [3]:

Theorem 3.3. *Let R be a commutative ring with* 1. *Let Q be a prime ideal of the ring $R[x_1, x_2, \ldots, x_n]$, and let the ideal P of R be the prime ideal $P = Q \cap R$. Then,*

$$\text{ht}(Q) = \text{ht}(P[x_1, \ldots, x_n]) + \text{ht}(Q/P[x_1, \ldots, x_n])$$
$$\leq \text{ht}(P[x_1, \ldots, x_n]) + n.$$

Proof. We give a proof by induction on n. First, we do the case $n = 1$. If $Q = P[x_1]$, then we are done, since $\mathrm{ht}(Q) = \mathrm{ht}(P[x_1])$. If $Q \supset P[x_1]$, then $\mathrm{ht}(Q) = \mathrm{ht}(P[x_1]) + 1$, by Theorem 3.2. But, $\mathrm{ht}(Q/P[x_1]) = 1$, by Theorem 2.1, and so, it is true that

$$\mathrm{ht}(Q) = \mathrm{ht}(P[x_1]) + \mathrm{ht}(Q/P[x_1]) \leq \mathrm{ht}(P[x_1]) + 1,$$

as desired.

Now, we let $n > 1$, and assume that the theorem is true for all $1 \leq k < n$. Let $Q_1 = Q \cap R[x_1]$. Consider first the case where $Q_1 = P[x_1]$. This case follows immediately using induction in the ring $R[x_1][x_2, \ldots, x_n]$ where $k = n - 1$, and we have

$$\begin{aligned}
\mathrm{ht}(Q) &= \mathrm{ht}(P[x_1][x_2, \ldots, x_n]) + \mathrm{ht}(Q/P[x_1][x_2, \ldots, x_n]) \\
&\leq \mathrm{ht}(P[x_1][x_2, \ldots, x_n]) + n - 1,
\end{aligned}$$

and $\mathrm{ht}(Q) \leq \mathrm{ht}(P[x_1, x_2, \ldots, x_n]) + n$, as desired.

Next, consider the case where $Q_1 \supset P[x_1]$. In this case, the first thing to observe is that, by Theorem 3.2,

$$\mathrm{ht}(Q_1[x_2, \ldots, x_n]) = \mathrm{ht}(P[x_1, \ldots, x_n]) + 1.$$

Therefore, again using induction in the ring $R[x_1][x_2, \ldots, x_n]$ where $k = n - 1$, we get

$$\begin{aligned}
\mathrm{ht}(Q) &= \mathrm{ht}(Q_1[x_2, \ldots, x_n]) + \mathrm{ht}(Q/Q_1[x_2, \ldots, x_n]) \\
&\leq \mathrm{ht}(Q_1[x_2, \ldots, x_n]) + n - 1 \\
&= \mathrm{ht}(P[x_1, \ldots, x_n]) + 1 + n - 1 \\
&= \mathrm{ht}(P[x_1, \ldots, x_n]) + n.
\end{aligned}$$

Thus, we have shown, as desired, that $\mathrm{ht}(Q) \leq \mathrm{ht}(P[x_1, \ldots, x_n]) + n$.

In order to complete the proof, we still need to show that, in this case,

$$\mathrm{ht}(Q) = \mathrm{ht}(P[x_1, \ldots, x_n]) + \mathrm{ht}(Q/P[x_1, \ldots, x_n]).$$

To do this, we first observe that, since $Q_1 \supset P[x_1]$,

$$\mathrm{ht}(Q/P[x_1, \ldots, x_n]) \geq \mathrm{ht}(Q/Q_1[x_2, \ldots, x_n]) + 1;$$

this trivial fact will be used very shortly. We now simply repeat the same argument we used previously; so, once again, by induction we get

$$\begin{aligned}
\mathrm{ht}(Q) &= \mathrm{ht}(Q_1[x_2, \ldots, x_n]) + \mathrm{ht}(Q/Q_1[x_2, \ldots, x_n]) \\
&= \mathrm{ht}(P[x_1, \ldots, x_n]) + 1 + \mathrm{ht}(Q/Q_1[x_2, \ldots, x_n]) \\
&\leq \mathrm{ht}(P[x_1, \ldots, x_n]) + \mathrm{ht}(Q/P[x_1, \ldots, x_n]).
\end{aligned}$$

But, then, since it is obvious that

$$\mathrm{ht}(Q) \geq \mathrm{ht}(P[x_1,\ldots,x_n]) + \mathrm{ht}(Q/P[x_1,\ldots,x_n]),$$

it follows that

$$\mathrm{ht}(Q) = \mathrm{ht}(P[x_1,\ldots,x_n]) + \mathrm{ht}(Q/P[x_1,\ldots,x_n]),$$

as desired. This completes the proof of the theorem.   □

Theorem 3.3 is a rather remarkable theorem. Its proof depends upon nothing more than the elementary Theorem 2.1, and yet it is powerful enough to prove many of the classical results in dimension theory. As the authors of [3] point out, this theorem "is of no greater depth than the fact that there cannot exist in $R[X_1]$ a chain of three distinct prime ideals having the same contraction to R. This fact in turn is really no deeper than the fact that $K[X_1]$ is a PID if K is a field. Thus, we obtain an elementary proof of the next result."

Theorem 3.4. *Let K be a field. Then,*

$$\dim K[x_1,\ldots,x_n] = n.$$

Proof. Since $K[x_1,\ldots,x_n]/(x_1,\ldots,x_i) \cong K[x_{i+1},\ldots,x_n]$, for each $1 < i < n$, and since $K[x_{i+1},\ldots,x_n]$ is an integral domain for each $0 \leq i < n$, we see that

$$(0) \subset (x_1) \subset (x_1,x_2) \subset \cdots \subset (x_1,x_2,\ldots,x_n)$$

is a chain of distinct prime ideals of length n in this ring; hence, $\dim K[x_1,\ldots,x_n] \geq n$.
    Now, suppose that Q is a prime ideal of the ring $K[x_1,x_2,\ldots,x_n]$. Then, $Q \cap K = (0)$. (Otherwise, since K is a field, $Q \cap K = K$, and then $1 \in Q$.) So, by Theorem 3.3, $\mathrm{ht}(Q) \leq 0 + n$. Therefore, $\dim K[x_1,\ldots,x_n] \leq n$.
    Hence, $\dim K[x_1,\ldots,x_n] = n$. This completes the proof of the theorem.   □

A recent proof of this classical result has also been given in [4] where the authors provide a characterization of the Krull dimension of a ring in terms of elements in the ring rather than in terms of prime ideals.

4 Additional Applications

Since $\dim K = 0$, for a field K, the result in Theorem 3.4 has the form

$$\dim R[x_1,\ldots,x_n] = n + \dim R.$$

Theorem 3.3 can be used to prove that there are rings other than fields where this same relationship holds between the dimension of a ring and the dimensions of the

polynomial rings. We now turn to the task of showing that two classes of rings behave in this same way with respect to the dimensions of their polynomial rings, namely, Noetherian rings and semi-hereditary rings.

In order to prove this result for Noetherian rings, we need two fundamental results in commutative ring theory, each of which we state without proof. The first is Krull's hugely influential *principal ideal theorem* of 1928; see [8, page 110] for a proof.

Theorem 4.1. *Let R be a Noetherian ring. Let $I = (a_1, \ldots, a_k)$ be a proper ideal of R generated by k elements. Let P be a prime ideal of R that is minimal over I. Then, $\mathrm{ht}(P) \leq k$.*

The second is a useful converse to Krull's principal ideal theorem; see [8, page 112] for a proof (Kaplansky mentions that this theorem "is not at all of the same depth as the principal ideal theorem. In fact, the proof really used just the ascending chain condition on radical ideals . . . ").

Theorem 4.2. *Let R be a commutative Noetherian ring with 1, and let P be a prime ideal of R. Let $\mathrm{ht}(P) = n$. Then, there are elements $a_1, \ldots, a_n$ such that P is minimal over $(a_1, \ldots, a_n)$.*

We can now use these two results, together with Theorem 3.3, to give a classical result on the relationship between the dimension of a Noetherian ring and the dimensions of its polynomial rings.

Theorem 4.3. *Let R be a commutative Noetherian ring with 1. Then,*

$$\dim R[x_1, \ldots, x_n] = n + \dim R.$$

Proof. First, we observe that the general fact that

$$\dim R[x_1, \ldots, x_n] \geq n + \dim R$$

follows immediately from the lower bound in Theorem 2.2.

Next, we remark that $R[x_1, \ldots, x_n]$ is Noetherian, and also, then, for any multiplicative system T, so too is the localization $R[x_1, \ldots, x_n]_T$.

Now, let Q be a maximal ideal in the ring $R[x_1, \ldots, x_n]$, and let $P = Q \cap R$. Consider the multiplicative system $R \setminus P$. There is a one-to-one correspondence between prime ideals in the localization $R[x_1, \ldots, x_n]_{R \setminus P}$ and prime ideals in $R[x_1, \ldots, x_n]$ disjoint from $R \setminus P$. But, since $Q \cap R = P$, any chain of prime ideals descending from Q will be disjoint from $R \setminus P$; therefore, by virtue of this one-to-one correpondence,

$$\mathrm{ht}(Q) = \mathrm{ht}(Q(R[x_1, \ldots, x_n])_{R \setminus P}).$$

Thus, we can, without loss, assume that R is a local ring, and that P is its unique maximal ideal.

We will also need to show that $\text{ht}(P[x_1, \ldots, x_n]) = \text{ht}(P)$. It is for this purpose that we need Krull's principal ideal theorem. Let $\text{ht}(P) = k$.

Since any chain of length k of distinct primes in R

$$P = P_0 \supset P_1 \supset P_2 \supset \cdots \supset P_k$$

can immediately be 'lifted' to a chain of length k of distinct primes in $R[x_1, \ldots, x_n]$:

$$P[x_1, \ldots, x_n] = P_0[x_1, \ldots, x_n] \supset P_1[x_1, \ldots, x_n]$$
$$\supset P_2[x_1, \ldots, x_n] \supset \cdots \supset P_k[x_1, \ldots, x_n],$$

we conclude that $\text{ht}(P[x_1, \ldots, x_n]) \geq \text{ht}(P)$.

Now, by Theorem 4.2, there is an ideal $I = (a_1, \ldots, a_k)$ of R such that P is minimal over I. So, then, $P[x_1, \ldots, x_n]$ is minimal over $I[x_1, \ldots, x_n]$. But, in the ring $R[x_1, \ldots, x_n]$, the ideal $I[x_1, \ldots, x_n]$ is also generated by the k elements $a_1, \ldots, a_k$. Therefore, by Theorem 4.1 – that is, by Krull's principal ideal theorem – we conclude that $\text{ht}(P[x_1, \ldots, x_n]) \leq k$. Thus, $\text{ht}(P[x_1, \ldots, x_n]) \leq \text{ht}(P)$, and we have shown that

$$\text{ht}(P[x_1, \ldots, x_n]) = \text{ht}(P),$$

as desired.

Finally, then, we can apply Theorem 3.3 – and, using the fact that R is a local ring with unique maximal ideal P, so that $\text{ht}(P) = \dim R$ – to get

$$\text{ht}(Q) \leq n + \text{ht}(P[x_1, \ldots, x_n])$$
$$= n + \text{ht}(P)$$
$$= n + \dim R.$$

Since Q is an arbitrary maximal ideal in $R[x_1, \ldots, x_n]$, it follows immediately that $\dim R[x_1, \ldots, x_n] \leq n + \dim R$. Therefore,

$$\dim R[x_1, \ldots, x_n] = n + \dim R.$$

This completes the proof of the theorem. $\square$

Next, we use Theorem 3.3 to give a similar result on the relationship between the dimension of a semihereditary ring and the dimensions of its polynomial rings. Recall that a ring is semihereditary if its finitely generated ideals are projective.

Theorem 4.4. *Let R be a commutative semihereditary ring with* 1. *Then,*

$$\dim R[x_1, \ldots, x_n] = n + \dim R.$$

Proof. As in the proof of Theorem 4.3 it suffices to prove that

$$\dim R[x_1, \ldots, x_n] \leq n + \dim R.$$

Moreover, we can once again, without loss, assume that R is a local ring, and that P is its unique maximal ideal. In this case, then, since R is semihereditary, R_P is a valuation domain (see [6, page 113]).

So, to complete the proof, all we need to do is show that if V is a valuation domain with maximal ideal M, then $\mathrm{ht}(M[x_1, \ldots, x_n]) = \mathrm{ht}(M)$, since the remainder of the proof then follows from Theorem 3.3 exactly as in the proof of Theorem 4.3. Of course, as before, it is clear that $\mathrm{ht}(M[x_1, \ldots, x_n]) \geq \mathrm{ht}(M)$.

Let Q be a nonzero prime ideal of $V[x_1, \ldots, x_n]$ such that $Q \subset M[x_1, \ldots, x_n]$. Let $f \neq 0 \in Q$. Then, since V is a valuation domain its ideals are totally ordered, and in particular, its principal ideals are totally ordered, so we can write $f = ag$ where $a \in V$ and $g \in V[x_1, \ldots, x_n]$ is such that some coefficient of g is a unit in V. Thus, $g \notin M[x_1, \ldots, x_n]$; and so, $g \notin Q$. But, $ag = f \in Q$, and Q is prime, so we conclude that $a \in Q$. Therefore, $a \in Q \cap V$, and $f = ag \in (Q \cap V)[x_1, \ldots, x_n]$. Hence, $Q \subseteq (Q \cap V)[x_1, \ldots, x_n]$. On the other hand, it is clear that $Q \supseteq (Q \cap V)[x_1, \ldots, x_n]$, and so, $Q = (Q \cap V)[x_1, \ldots, x_n]$. It follows that $\mathrm{ht}(M[x_1, \ldots, x_n]) \leq \mathrm{ht}(M)$. Therefore, $\mathrm{ht}(M[x_1, \ldots, x_n]) = \mathrm{ht}(M)$, as desired. This completes the proof of the theorem. □

The next two results from [3] concern Hilbert rings. A commutative ring R with 1 is a Hilbert ring if every prime ideal of R is an intersection of maximal ideals. The fact that for a field K, the polynomial ring $K[x_1, \ldots, x_n]$ is a Hilbert ring provides a very natural approach to Hilbert's Nullstellensatz (see [8, page 19]). The motivating idea behind Hilbert rings, and the one we use in the proofs to follow, is that a ring R is a Hilbert ring if the contraction $Q \cap R$ of any maximal ideal Q in the polynomial ring $R[x]$ is a maximal ideal in R.

Theorem 4.5. *Let R be a commutative ring with 1 such that for some $n \geq 1$ all maximal ideals of $R[x_1, \ldots, x_n]$ have the same height, then R is a Hilbert ring.*

Proof. It is sufficient to prove this for the case $n = 1$ since R is a Hilbert ring if and only if $R[x]$ is a Hilbert ring (see [8, page 18]). Let Q be a maximal ideal of $R[x]$. We must prove that $Q \cap R$ is a maximal ideal of R. Assume, by way of contradiction, that $P = Q \cap R$ is not maximal, and let $P \subset M$, where M is a maximal ideal in R. Note that $M[x]$ is not a maximal ideal of $R[x]$.

Now, by Theorem 3.3, $\mathrm{ht}(Q) \leq \mathrm{ht}(P[x]) + 1 < \mathrm{ht}(M[x]) + 1$, and so, it follows that $\mathrm{ht}(M[x]) \geq \mathrm{ht}(Q)$. But, $M[x]$ is not a maximal ideal, so this contradicts the hypothesis that all maximal ideals of $R[x]$ have the same height. Therefore, $P = Q \cap R$ is a maximal ideal, and R is a Hilbert ring. This completes the proof of the theorem. □

Since the polynomial ring $K[x_1, \ldots, x_n]$ is a Hilbert ring for any field K, we know that whenever Q is a maximal ideal in $R[x_{k+1}]$, where $R = K[x_1, \ldots, x_k]$, then $M = Q \cap R$ is a maximal ideal of R. So, it is easy to use induction together with Theorem 3.4 to show that, for each $n \geq 1$, all maximal ideals of $K[x_1, \ldots, x_n]$ have height n. The next theorem generalizes this idea.

Theorem 4.6. *Let R be a commutative Hilbert ring with 1 such that all maximal ideals of R have the same height. If, for some $n \geq 1$, $\mathrm{ht}(M) = \mathrm{ht}(M[x_1, \ldots, x_n])$ for each maximal ideal M of R, then all maximal ideals of $R[x_1, \ldots, x_n]$ have the same height.*

In particular, then, if R is a Noetherian ring or a semihereditary ring, all maximal ideals of $R[x_1, \ldots, x_n]$ have the same height.

Proof. First, we observe that for an integral domain D with quotient field K there is a one-to-one order preserving correspondence between prime ideals P of $D[x_1, \ldots, x_n]$ with $P \cap D = (0)$ and all prime ideals of $K[x_1, \ldots, x_n]$. Therefore, since all maximal ideals of $K[x_1, \ldots, x_n]$ have height n, if Q is a maximal ideal of $D[x_1, \ldots, x_n]$ with $Q \cap D = (0)$, then $\mathrm{ht}(Q) = n$.

Now, let Q_1 and Q_2 be maximal ideals of $R[x_1, \ldots, x_n]$, and let $M_1 = Q_1 \cap R$ and $M_2 = Q_2 \cap R$. We then apply the above observation to the integral domains $R[x_1, \ldots, x_n]/(M_i[x_1, \ldots, x_n])$, for $i = 1, 2$; thus, $\mathrm{ht}(Q_i/(M_i[x_1, \ldots, x_n])) = n$, and

$$\mathrm{ht}(Q_1) = \mathrm{ht}(M_1[x_1, \ldots, x_n]) + n = \mathrm{ht}(M_1) + n$$
$$= \mathrm{ht}(M_2) + n = \mathrm{ht}(M_2[x_1, \ldots, x_n]) + n = \mathrm{ht}(Q_2).$$

Hence, all maximal ideals of $R[x_1, \ldots, x_n]$ have the same height, as desired.

The last statement in the theorem then follows immediately since, as we saw during the proofs of Theorems 4.3 and 4.4, the condition that $\mathrm{ht}(M) = \mathrm{ht}(M[x_1, \ldots, x_n])$ for each maximal ideal M of R is satisfied if R is Noetherian or semihereditary. This completes the proof of the theorem.   □

In [3] the authors present examples proving that neither of the last two theorems can be strengthened: an example of an integrally closed Hilbert domain D of dimension 1 such that not all maximal ideals of $D[x]$ have the same height; and, an integrally closed Hilbert domain D such that all maximal ideals of $D[x]$ have the same height but this is not true of D. An example is given in [10] of a Hilbert ring of dimension 2 with an uncountable number of maximal ideals of height 1.

As a final application of Theorem 3.3, we present a greatly simplified proof of Jaffard's special chain theorem (see [7, page 35]). A chain

$$Q_0 \subset Q_1 \subset Q_2 \subset \cdots \subset Q_k$$

of distinct prime ideals in a polynomial ring $R[x_1, \ldots, x_n]$ is called a *special chain* if, for each Q_i, the ideal $(Q_i \cap R)[x_1, \ldots, x_n]$ belongs to the chain.

Theorem 4.7. *Let R be a commutative ring with* 1. *If Q is a prime ideal of finite height in $R[x_1, \ldots, x_n]$, then* $\mathrm{ht}(Q)$ *can be realized as the length of a special chain of primes of $R[x_1, \ldots, x_n]$ descending from Q.*

In particular, if R is finite dimensional, then $\dim(R[x_1, \ldots, x_n])$ *can be realized as the length of a special chain of primes of $R[x_1, \ldots, x_n]$.*

Proof. This follows immediately by induction on $\mathrm{ht}(Q)$ by Theorem 3.3. □

5 The Dimension of Power Series Rings

It is worth briefly mentioning in conclusion a result from [2] in which the behavior between the dimension of a ring and the dimension of its power series ring is exactly what we would wish it to be. But first, we look at an example that illustrates just how pathological behavior can be for power series rings.

As in the polynomial ring case, for a prime P of a ring R, the heights of the prime ideals $P[x]$ and $P[[x]]$ are at least as great as the height of the prime P, simply because any chain of primes descending from P can be 'lifted' to chains of the same length descending from $P[x]$ and from $P[[x]]$. One immediate consequence of this is that

$$\text{if } \dim R = \infty, \text{ then } \dim R[x] = \infty \text{ and } \dim R[[x]] = \infty.$$

When the dimension of R is finite, Theorem 2.2 shows that there are strict limitations on the dimension of $R[x]$ in terms of the dimension of R. And, we know that for some classes of rings, such as Noetherian and semihereditary rings, the lower bound is even achievable and we have

$$\dim R[x] = \dim R + 1.$$

However, for power series, the story is very different. It is even possible to have a ring R such that $\dim R = 0$, and yet, $\dim R[[x]] = \infty$. The source of the dramatic difference between the polynomial situation and the power series situation is that in a power series ring $R[[x]]$, the ideal $IR[[x]]$ generated by I, while clearly contained in the ideal $I[[x]]$, may not actually be equal to $I[[x]]$.

Here is an example of this phenomenon. Let $R = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \cdots$ be the ring which is a countably infinite product of the rationals $\mathbb{Q}$. Let I be the ideal of R generated by the countably many elements

$$(1, 0, 0, 0, 0, \ldots), \quad (0, 1, 0, 0, 0, \ldots), \quad (0, 0, 1, 0, 0, \ldots), \quad \ldots;$$

that is, I is the set of elements of R that have finite support. Now, if $f \in IR[[x]]$, then f has finite support; however, here is a power series in $I[[x]]$ that clearly does not have finite support:

$$g = (1, 0, 0, 0, 0, \ldots) + (0, 1, 0, 0, 0, \ldots)x + (0, 0, 1, 0, 0, \ldots)x^2 + \cdots;$$

hence, $g \in I[[x]] \setminus IR[[x]]$. Now, a beautiful theorem in [1] says that if there is an ideal I in a ring R such that $I[[x]] \nsubseteq \sqrt{IR[[x]]}$ then $\dim R[[x]] = \infty$. Thus, since $g \in I[[x]]$, but g does not have finite support, $g \notin \sqrt{IR[[x]]}$; and so, $\dim R[[x]] = \infty$, even though $\dim R = 0$.

On the other hand, if K is a field, then the only nonzero ideals of $K[[x]]$ are $(x), (x^2), (x^3), \ldots$; and so, $(0) \subset (x)$ is the longest possible chain of prime ideals in $K[[x]]$. Thus, $\dim K[[x]] = 1$, and we have

$$\dim K[[x]] = \dim K + 1.$$

Not surprisingly, as we see in the following theorem from [2], Noetherian rings exhibit this same good behavior. Once again, we must rely on Krull's principal ideal theorem.

Theorem 5.1. *Let R be a commutative Noetherian ring with* 1. *Then,*

$$\dim R[[x]] = \dim R + 1.$$

Proof. Let $\dim R = n$, and let

$$P = P_0 \supset P_1 \supset P_2 \supset \cdots \supset P_n$$

be a chain of distinct prime ideals of R of length n. As usual, this chain can 'lifted' to a chain of the same length in $R[[x]]$. But, in this case, we can also add one more prime ideal at the top, and get

$$P + (x) \supset P[[x]] = P_0[[x]] \supset P_1[[x]] \supset P_2[[x]] \supset \cdots \supset P_n[[x]],$$

which is a chain of distinct prime ideals of $R[[x]]$ of length $n + 1$. Thus,

$$\dim R[[x]] \geq \dim R + 1.$$

Note that up to this point in the proof we have not invoked the Noetherian property of the ring R, and so, this inequality holds in general.

Now, let Q be a maximal ideal of $R[[x]]$. Then, $Q = M + (x)$ where M is a maximal ideal of R. Since $\dim R = n$, we have $\mathrm{ht}(M) \leq n$. Therefore, by Theorem 4.2, there are elements $a_1, \ldots, a_n$ in R such that M is minimal over $(a_1, \ldots, a_n)$. But, then, $M + (x)$ is minimal over $(a_1, \ldots, a_n, x)$. So, by Krull's principal ideal theorem, Theorem 4.1, $\mathrm{ht}(M + (x)) \leq n + 1$. Since Q was an arbitrary maximal ideal of $R[[x]]$, it follows that $\dim R[[x]] \leq n + 1$. Hence,

$$\dim R[[x]] = \dim R + 1,$$

as desired. This completes the proof of the theorem. $\square$

Bibliography

[1] Arnold, J. T., On the dimension theory of overrings of an integral domain. Trans Amer Math Soc. 1969;138:313–326.

[2] Brewer, J. W., Power series rings over commutative rings. Marcel Dekker; 1981.

[3] Brewer, J. W, Heinzer, W. J., Montgomery, P. R., Rutter, E. A., Krull dimension of polynomial rings. Proceedings of the Kansas Conference on Commutative Algebra. vol. 311 of Lecture notes in mathematics. Springer-Verlag; 1973. p. 26–45.

[4] Coquand, T., Lombardi, H., A short proof for the Krull dimension of a polynomial ring. Amer Math Monthly. 2005;112:826–829.

[5] Eisenbud, D., Commutative algebra with a view toward algebraic geometry. Springer-Verlag; 1995.

[6] Endo, S., On semi-hereditary rings. J Math Soc Japan. 1961;13:109–119.

[7] Jaffard, P., Theorie de la dimension dans les anneaux de polynomes. Gauthier-Villars; 1960.

[8] Kaplansky, I., Commutative rings. revised ed. Polygonal Publishing House; 1994 [University of Chicago Press; 1974].

[9] Matsumura, H., Commutative ring theory. Cambridge University Press; 1989.

[10] Roberts, L. G., An example of a Hilbert ring with maximal ideals of different heights. Proc Amer Math Soc (2). 1973;37:425–426.

Author Information

John J. Watkins, Department of Mathematics and Computer Science, Colorado College, Colorado Springs, CO, USA.
E-mail: jwatkins@coloradocollege.edu

The Projective Line over the Integers

Ela Celikbas and Christina Eubanks-Turner

Abstract. In this article we survey work that has been done to describe the partially ordered set of prime ideals of the projective line over the integers, denoted by $\mathrm{Proj}(\mathbb{Z}[h,k])$. We consider a conjecture given by Aihua Li and Sylvia Wiegand that would complete a characterization of $\mathrm{Proj}(\mathbb{Z}[h,k]) = \mathrm{Spec}(\mathbb{Z}[x]) \cup \mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$. In this paper we give some previous results and some new results that support the conjecture. In particular we show that a possible axiom for $\mathrm{Proj}(\mathbb{Z}[h,k])$ proposed by Arnavut, Li and Wiegand holds for a large number of previously unknown cases.

Keywords. Prime Ideals, Prime Spectrum, Projective Line, Polynomials, Radical Element.

2010 Mathematics Subject Classification. 13A15, 13B25, 06A11, 06A06.

1 Introduction

Let h and k be indeterminates over the integers $\mathbb{Z}$. The *projective line* $\mathrm{Proj}(\mathbb{Z}[h,k])$ *over the integers* can be viewed as the partially ordered set under inclusion of all prime ideals of $\mathbb{Z}[h,k]$ that are generated by finite sets of homogeneous polynomials in h and k other than those prime ideals that contain both h and k. For x an indeterminate over $\mathbb{Z}$, the prime spectrum of $\mathbb{Z}[x]$ or $\mathrm{Spec}(\mathbb{Z}[x])$, the partially ordered set of prime ideals of $\mathbb{Z}[x]$ under inclusion, is sometimes called the *affine line* over $\mathbb{Z}$. In this paper we let $x = h/k$ and we view $\mathrm{Proj}(\mathbb{Z}[h,k])$ as the union of its affine pieces $\mathrm{Spec}(\mathbb{Z}[x])$ and $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$. In this view of $\mathrm{Proj}(\mathbb{Z}[h,k])$, the intersection of $\mathrm{Spec}(\mathbb{Z}[x])$ with $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$ is identified with $\mathrm{Spec}(\mathbb{Z}[x, \frac{1}{x}])$; cf. Notation 2.7 (ii).

In 1986, Roger Wiegand gave five axioms that characterized the prime spectrum of $\mathbb{Z}[x]$ as a partially ordered set; cf. [7] and Definition 2.4 below. Four of those axioms hold for $\mathrm{Proj}(\mathbb{Z}[h,k])$, but $\mathrm{Proj}(\mathbb{Z}[h,k])$ fails to satisfy the key fifth axiom of $\mathrm{Spec}(\mathbb{Z}[x])$; cf. [5]. So far no one has completed a characterization of $\mathrm{Proj}(\mathbb{Z}[h,k])$, although there have been several related results. In 1994 William Heinzer, David Lantz and Sylvia Wiegand determined those partially ordered sets that occur as the projective line $\mathrm{Proj}(R[h,k])$ when R is a one-dimensional semilocal domain. In 1997, Aihua Li and Sylvia Wiegand described some properties of $\mathrm{Proj}(\mathbb{Z}[h,k])$. In 2002, Meral Arnavut conjectured that a modified form of the key axiom of $\mathrm{Spec}(\mathbb{Z}[x])$ would complete a characterization of $\mathrm{Proj}(\mathbb{Z}[h,k])$; she gave partial results toward her conjecture; cf. [1] and Axiom 4.2 below.

The key axiom for $\mathrm{Spec}(\mathbb{Z}[x])$ stipulates the existence of "radical elements", defined in Definition 2.2, for pairs (S, T) of finite subsets of $\mathrm{Spec}(\mathbb{Z}[x])$, where the elements

of S have height one and those of T have height two. Radical elements often exist for sets S and T in $\text{Proj}(\mathbb{Z}[h,k])$, but not always. We expect that the determination of when radical elements exist would lead to a characterization of $\text{Proj}(\mathbb{Z}[h,k])$.

In this article we continue the investigation of the projective line over the integers. In the process we give further evidence for Arnavut's conjecture. Among our main results are new cases when radical elements exist, such as Theorem 5.5 and Theorem 5.8. In Theorem 5.5, we show the existence of radical elements when every maximal ideal of $T \cap \text{Spec}(\mathbb{Z}[x])$ has form $(x,p)\mathbb{Z}[x]$, where p is a prime integer; each (x,p) corresponds to exactly one maximal ideal of form $(\frac{1}{x},p)\mathbb{Z}[\frac{1}{x}] \in T \cap \text{Spec}(\mathbb{Z}[\frac{1}{x}])$; and vice versa. In Theorem 5.8, we find radical elements for sets of form

$$S = \left\{ (p_1), \ldots, (p_n), (x), \left(\frac{1}{x}\right), (x-a), (x-b) \right\}, \quad \text{and}$$

$$T = \left\{ (x,p_1), \ldots, (x,p_\ell), \left(\frac{1}{x}, p_{\ell+1}\right), \ldots, \left(\frac{1}{x}, p_n\right) \right\},$$

where the p_i are prime integers relatively prime to $a,b \in \mathbb{Z}$, under certain conditions. It is difficult to produce prime ideals that are the correct radical elements. For the proof of Theorem 5.5, we use Hilbert's Irreducibility Theorem to find radical elements. For the proof of Theorem 5.8, we use Euler's theorem. Theorem 5.8 is a special case of the conjecture and answers a question in Arnavut's paper [1].

In Section 2 we restate relevant notation, definitions and previous results of Meral Arnavut, Aihua Li and Sylvia Wiegand from [1], [4], and [5]. In Section 3 we discuss the *coefficient subset* of $\text{Proj}(\mathbb{Z}[h,k])$ from [4]. A coefficient subset of $\text{Proj}(\mathbb{Z}[h,k])$ behaves like the set of all prime ideals of $\text{Proj}(\mathbb{Z}[h,k])$ generated by prime integers. In Section 4 we summarize Meral Arnavut's results towards the conjecture. Our new results are in Section 5; they all support the conjecture.

2 Definitions and Background

First we establish some notation.

Notation 2.1. Let $\mathbb{N}$ be the natural numbers and let $\mathbb{Q}$ be the rationals. Let U be a partially ordered set, sometimes abbreviated *poset*. A *chain* in U is a totally ordered subset of U. Throughout we suppose that U has a unique minimal element u_0 and that every chain in U is finite.

For $u \in U$, *the height of* u, $\text{ht}(u)$, is the length t of a maximal length chain in U of form $u_0 < u_1 < u_2 < \cdots < u_t = u$; *the dimension of* U, $\dim(U)$, is the maximum of $\{\text{ht}(u) \mid u \in U\}$; and we set

$$H_1(U) := \{u \in U \mid \text{ht}(u) = 1\}, \quad \text{and} \quad H_2(U) := \{u \in U \mid \text{ht}(u) = 2\}.$$

For every $u, v \in U$ and $S \subseteq H_1(U)$, define

$$u^\uparrow := \{v \in U \mid u < v\}, \quad v^\downarrow := \{u \in U \mid u < v\}, \quad (u, v)^\uparrow := u^\uparrow \cap v^\uparrow, \quad \text{and}$$

$$S^\uparrow = \{t \in U \mid t \in s^\uparrow, \text{for all } s \in S\}$$

For $U := \mathrm{Spec}(R)$, where R is a Noetherian ring, and $a \in R$, let

$$a^\uparrow := \{P \in \mathrm{Spec}(R) \mid a \in P\} \quad \text{and}$$

$$(a, b)^\uparrow := \{P \in \mathrm{Spec}(R) \mid a \in P \text{ and } b \in P\}.$$

In Definition 2.4, we give the five axioms that Roger Wiegand showed characterize $\mathrm{Spec}(\mathbb{Z}[x])$ as a partially ordered set; cf. [7]. The key axiom is easier to state if we first define "radical element".

Definition 2.2 ([4]). Let U be a partially ordered set of dimension two and let S and T be finite subsets of U such that $\emptyset \neq S \subseteq H_1(U)$ and $T \subseteq H_2(U)$. If $w \in H_1(U)$ satisfies (i) and (ii), then w is called a *radical element* for (S, T):

(i) $w < t$, for every $t \in T$,

(ii) Whenever $m \in U$ is greater than both w and s, for some $s \in S$, then $m \in T$.

(In other words, w is a *radical element* for (S, T) if and only if $\bigcup_{s \in S} (w, s)^\uparrow \subseteq T \subset w^\uparrow$.)

The following picture illustrates the relations between a radical element and the associated sets S and T in a two-dimensional poset:
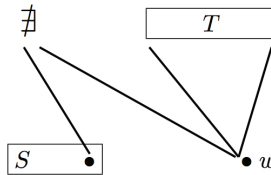
Figure 1. Relations for a radical element w.

For convenience we also introduce the following notation that is used later.

Notation 2.3. A ht(1, 2)-*pair* of a poset U is a pair (S, T) of finite subsets S and T of U such that $\emptyset \neq S \subseteq H_1(U)$ and $T \subseteq H_2(U)$.

Definition 2.4. Let U be a partially ordered set. The following five axioms are called the *Countable Integer Polynomial (CZP) Axioms*:

(P1) U is countable and has a unique minimal element.

(P2) U has dimension two.

(P3) For each element u of height-one, $u^\uparrow$ is infinite.

(P4) For each pair u, v of distinct elements of height-one, $(u, v)^\uparrow$ is finite.

(RW) Every ht(1, 2)-pair of U has at least one radical element in U.

Note: Such a set also satisfies Axiom P3′ below, which follows from Axiom RW.

(P3′) For every height-two element t, the set $t^\downarrow$ is infinite.

   Axiom RW is essential because it distinguishes $\mathrm{Spec}(\mathbb{Z}[x])$ from other similar prime spectra such as $\mathrm{Spec}(\mathbb{Q}[x, y])$; cf. [7]. The following theorem from R. Wiegand shows that the CZP axioms characterize $\mathrm{Spec}(\mathbb{Z}[x])$.

Theorem 2.5 ([7]). *A poset U satisfies the CZP axioms of Definition 2.4 if and only if U is order isomorphic to* $\mathrm{Spec}(\mathbb{Z}[x])$.

Remarks 2.6. The first two remarks are from [4, 5]:

 (i) By Theorem 2.5, every ht(1, 2)-pair of $\mathrm{Spec}(\mathbb{Z}[x])$ has infinitely many radical elements in $\mathrm{Spec}(\mathbb{Z}[x])$.

 (ii) Since $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}]) \cong \mathrm{Spec}(\mathbb{Z}[x])$, every ht(1, 2)-pair of $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$ has infinitely many radical elements in $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$.

(iii) The following discussion shows how the existence of radical elements is important for showing that two posets U and V that both satisfy axioms for $\mathrm{Proj}(\mathbb{Z}[h, k])$ are order isomorphic. Since $\mathrm{Proj}(\mathbb{Z}[h, k])$ is a countable set, we would want to define an order-isomorphism φ at each stage between finite subsets F and G of U and V respectively, and then extend φ to U and V. If u_0 and v_0 are the minimal elements of U and V respectively, S is the set of height-one elements of F, T is the set of height-two elements of F, and φ is an order-isomorphism from $F = \{0\} \cup S \cup T$ in U to $G = \{0\} \cup S' \cup T'$ in V, we would try to extend φ so that a radical element for (S, T) goes to a radical element for (S', T'). This is a simplification of the process; actually a height-one set S, and a height-two set T, might be enlarged first and φ defined on enlarged ht(1, 2)-pair before defining the map φ on a radical element. The process is described more explicitly in Roger Wiegand's paper [6]. If we knew which pairs had radical elements, we could perhaps obtain such an order-isomorphism.

Notation 2.7. As mentioned in the introduction, the projective line over the integers, denoted by $\mathrm{Proj}(\mathbb{Z}[h, k])$, where h and k are indeterminates, has two standard interpretations as a partially ordered set. The first interpretation is from algebraic geometry; the second is more ring-theoretic and is used in this paper.

 (i) $\mathrm{Proj}(\mathbb{Z}[h, k])$ is the set of all prime ideals of $\mathbb{Z}[h, k]$ generated by finite sets of homogeneous polynomials in the variables h and k, but not those prime ideals containing both h and k.

(ii) $\mathrm{Proj}(\mathbb{Z}[h,k]) := \mathrm{Spec}(\mathbb{Z}[x]) \cup \mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$, where $\mathrm{Spec}(\mathbb{Z}[x]) \cap \mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$ is identified with $\mathrm{Spec}(\mathbb{Z}[x, \frac{1}{x}])$. In this identification each prime ideal of the form $p\mathbb{Z}[x]$, where p is a prime integer, is considered the same as $p\mathbb{Z}[\frac{1}{x}]$, and $f(x)\mathbb{Z}[x]$ is identified with $x^{-\deg(f)} f(x)\mathbb{Z}[\frac{1}{x}]$, for every irreducible polynomial $f(x)$ of $\mathbb{Z}[x] \setminus x\mathbb{Z}[x]$ with $\deg(f) > 0$.

In particular, in the second view, if $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is irreducible, and $a_n \neq 0$ and $a_0 \neq 0$, then we identify $(f(x)) \in \mathrm{Spec}(\mathbb{Z}[x])$ with $(\frac{1}{x^n} f(x)) \in \mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$, written $(f(x)) \sim (\frac{1}{x^n} f(x))$, where

$$\frac{1}{x^n} f(x) = a_0 \left(\frac{1}{x}\right)^n + \cdots + a_{n-1}\left(\frac{1}{x}\right) + a_n.$$

Thus $(x^2 + 2x + 3)\mathbb{Z}[x] \sim (1 + \frac{2}{x} + \frac{3}{x^2})\mathbb{Z}[\frac{1}{x}]$. The only elements of $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$ that are not in $\mathrm{Spec}(\mathbb{Z}[x])$ are the height-one prime $\frac{1}{x}\mathbb{Z}[\frac{1}{x}]$ and the height-two maximals $(p, \frac{1}{x})\mathbb{Z}[\frac{1}{x}]$, where p is a prime integer. Similarly $x\mathbb{Z}[x]$ is the only height-one element of $\mathrm{Spec}(\mathbb{Z}[x])$ not in $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$, and $\{(p, x)\mathbb{Z}[x], p$ is a prime integer$\}$ is the set of all the height-two elements that are in $\mathrm{Spec}(\mathbb{Z}[x])$ but not in $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$.

Here is an illustration of $\mathrm{Proj}(\mathbb{Z}[h,k])$ with this interpretation, from [5].
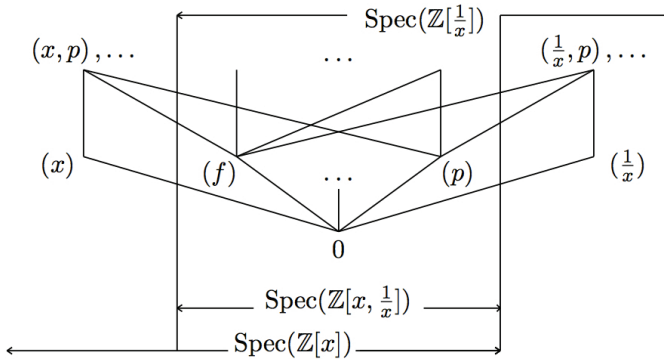
Figure 2. $\mathrm{Proj}(\mathbb{Z}[h,k])$.

The following proposition is useful for finding radical elements. The proof is straightforward and is omitted.

Proposition 2.8 ([1]). *Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, where $a_0, \ldots, a_n \in \mathbb{Z}$ and $a_n \neq 0$, let $l(f)$ denote the leading coefficient a_n of $f(x)$ and let $c(f)$ denote the constant term a_0 of $f(x)$.*

(i) *If p is a prime integer, then*

    (a) $f(x) \in (x, p)\mathbb{Z}[x] \Leftrightarrow p \mid c(f)$;

    (b) $(f(x)) = (\frac{1}{x^n} f(x)) \subseteq (\frac{1}{x}, p)\mathbb{Z}[\frac{1}{x}] \Leftrightarrow p \mid l(f)$.

(ii) *If $f(x)$ is an irreducible element of $\mathbb{Z}[x]$ of positive degree in x, then*

    (a) $l(f) = \pm 1 \iff (f, \frac{1}{x})^\uparrow = \emptyset \iff (f)^\uparrow \subseteq \mathrm{Spec}(\mathbb{Z}[x])$.

    (b) $c(f) = \pm 1 \iff (f, x)^\uparrow = \emptyset \iff (f)^\uparrow \subseteq \mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$.

By the following theorem, some adjustment of the CZP axioms of Definition 2.4 is necessary in order to describe $\mathrm{Proj}(\mathbb{Z}[h, k])$.

Theorem 2.9 ([5]). $\mathrm{Proj}(\mathbb{Z}[h, k])$ *satisfies Axioms* P1–P4 *of Definition* 2.4, *but does not satisfy Axiom* RW *of Definition* 2.4. *Thus* $\mathrm{Proj}(\mathbb{Z}[h, k]) \ncong \mathrm{Spec}(\mathbb{Z}[x])$.

The following example shows that the (RW) axiom fails for $\mathrm{Proj}(\mathbb{Z}[h, k])$:

Example 2.10 ([5]). Let $S = \{(\frac{1}{x}), (2), (5)\}$ and $T = \{(x, 2), (\frac{1}{x}, 2), (\frac{1}{x}, 3)\}$ in $\mathrm{Proj}(\mathbb{Z}[h, k])$. Then the pair (S, T) does not have a radical element in $\mathrm{Proj}(\mathbb{Z}[h, k])$.

Remark 2.11. If there is a radical element w for a ht(1, 2)-pair in $\mathrm{Proj}(\mathbb{Z}[h, k])$, then $w \notin S$. Otherwise, $w^\uparrow \subseteq T$ by Definition 2.2 (i), and this would imply T is infinite by (P3) of Definition 2.4, a contradiction.

Our goal in this paper is to determine answers to Questions 2.12.

Questions 2.12. For which ht(1, 2)-pairs of $\mathrm{Proj}(\mathbb{Z}[h, k])$ do radical elements exist? Which pairs have no radical element?

In what follows we obtain partial answers to these questions.

3 The Coefficient Subset and Radical Elements of $\mathrm{Proj}(\mathbb{Z}[h, k])$

In this section we give some more background and describe various ht(1, 2)-pairs of $\mathrm{Proj}(\mathbb{Z}[h, k])$ in order to obtain partial answers to Question 2.12. In particular the "coefficient" subset C_0 of $\mathrm{Proj}(\mathbb{Z}[h, k])$ of prime ideals generated by prime elements of $\mathbb{Z}$ is relevant. It is more feasible that a ht(1, 2)-pair (S, T) has a radical element if, for every prime element p of $\mathbb{Z}$ with $(p) \in S$, there is a maximal ideal $M \in T$ so that $p \in M$, cf. Proposition 3.5.

First in Proposition 3.1 we observe that some ht(1, 2)-pairs (S, T) inherit infinitely many radical elements in $\mathrm{Proj}(\mathbb{Z}[h, k])$ from $\mathrm{Spec}(\mathbb{Z}[x])$ or $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$. This is because $\mathrm{Spec}(\mathbb{Z}[x])$ and $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$ are CZP, cf. Theorem 2.5.

Proposition 3.1 ([5]). *Every* ht(1, 2)-*pair* (S, T) *of* $\mathrm{Proj}(\mathbb{Z}[h, k])$ *has infinitely many radical elements in case* (i) *or* (ii) *hold:*

  (i) *For every* $s \in S$, $s^\uparrow \subseteq \mathrm{Spec}(\mathbb{Z}[x])$, *and* $T \subseteq \mathrm{Spec}(\mathbb{Z}[x])$.

  (ii) *For every* $s \in S$, $s^\uparrow \subseteq \mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$, *and* $T \subseteq \mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$.

Next we consider subsets of $\mathrm{Proj}(\mathbb{Z}[h,k])$ like the subsets of prime ideals generated by all prime integers of $\mathrm{Proj}(\mathbb{Z}[h,k])$. We consider the existence of radical elements for various $\mathrm{ht}(1,2)$-pairs subject to conditions involving such a "coefficient" subset.

Definition 3.2 ([1]). Let U be a poset of dimension two. A subset C of height-one elements is called a *coefficient subset of U* if

(i) For every $p \in C$, $p^\uparrow$ is infinite.

(ii) For every pair p, q of distinct elements of C, $p \neq q \in C$, $(p,q)^\uparrow = \emptyset$.

(iii) $\bigcup_{p \in C} p^\uparrow = H_2(U)$.

(iv) For every $p \in C$ and $u \in H_1(U) \setminus C$, we have $(p,u)^\uparrow \neq \emptyset$, and $p^\uparrow = \bigcup_{v \in H_1(U) \setminus C} (p,v)^\uparrow$.

Definition 3.3. Let $A \subseteq H_1(U)$, with $(a,b)^\uparrow = \emptyset$ for every $a, b \in A$. A coefficient subset C is said to be *attached to A* if, for every $p \in C$ and every $a \in A$, $|(p,a)^\uparrow| = 1$.

Example 3.4. The set C_0 of all prime ideals of $\mathbb{Z}[x]$ generated by prime integers is a coefficient subset of $\mathrm{Proj}(\mathbb{Z}[h,k])$ attached to $\{(x), (\frac{1}{x})\}$. It is also attached to $\{(x), (\frac{1}{x}), (x-1)\}$ or $\{(x), (\frac{1}{x}), (x+1)\}$.

Proposition 3.5 ([5]). *Let (S,T) be a* $\mathrm{ht}(1,2)$*-pair and let C be a coefficient subset of* $\mathrm{Proj}(\mathbb{Z}[h,k])$. *Suppose that there exist distinct elements P_0 and P_1 of C such that $P_0 \in S$ and $T \cap P_0^\uparrow = \emptyset$, but $T \cap P_1^\uparrow \neq \emptyset$. Then*

(i) *(S,T) has no radical element except possibly P_1,*

(ii) *If $T \nsubseteq P_1^\uparrow$, then P_1 is not a radical element by Definition 2.2 (i),*

(iii) *There exists $Q \in H_1(\mathrm{Proj}(\mathbb{Z}[h,k])) \setminus C$ and $t \in P_1^\uparrow \cap Q^\uparrow \cap T$; thus P_1 is not a radical element for $(S \cup \{Q\}, T)$.*

Proof. For (i), let $t \in T \cap P_1^\uparrow$. Suppose Q were a radical element for (S,T) and $Q \neq P_1$. If $Q \in C$, then $(Q, P_1)^\uparrow = \emptyset$ by (ii) of Definition 3.2, and so $t \notin Q^\uparrow$, a contradiction to Definition 2.2 for Q a radical element. Thus $Q \notin C$, and so there exists $t' \in (P_0, Q)^\uparrow$ by (4) of Definition 3.2. By hypothesis $t' \in P_0^\uparrow \implies t' \notin T$, again contradicting that Q is a radical element. Thus (S,T) has no radical element except possibly P_1.

(ii) follows directly from Definition 2.2.

For (iv), since $P_1^\uparrow$ is infinite, there exists $t \in P_1^\uparrow \setminus T$. Now by (4) of Definition 3.2, there exists $Q \notin C$ with $t \in P_1^\uparrow \cap Q^\uparrow$. Thus P_1 is not a radical element for the pair $(S \cup \{Q\}, T)$. $\square$

Corollary 3.6 ([5]). *Let (S,T) be a* $\mathrm{ht}(1,2)$*-pair in* $\mathrm{Proj}(\mathbb{Z}[h,k])$. *If $T \neq \emptyset$, then there exists a finite subset S' of $H_1(\mathrm{Proj}(\mathbb{Z}[h,k]))$ such that $S \subseteq S'$ and (S',T) has no radical element in* $\mathrm{Proj}(\mathbb{Z}[h,k])$.

The following results, Proposition 3.7 and Theorem 3.8, are used later to construct radical elements in various cases.

Proposition 3.7 ([2, page 102, Exercise 3]). *Let R be a domain and let y be an indeterminate over R. Suppose* (i) *$\{a, b\}$ is an R-sequence or* (ii) *$(a, b) = R$, where $b \neq 0$. Then $(a + by)$ is a prime ideal of $R[y]$.*

Theorem 3.8 (Hilbert's Irreducibility Theorem, [3, page 141]). *If $f \in \mathbb{Q}[x_1, \ldots, x_r, x]$ is an irreducible polynomial, then there exist $a_1, \ldots, a_r \in \mathbb{Q}$ such that $f(a_1, \ldots, a_r, x)$ remains irreducible in $\mathbb{Q}[x]$.*

Meral Arnavut shows that the coefficient subset of $\operatorname{Proj}(\mathbb{Z}[h, k])$ is unique. She also gives partial results concerning the existence of radical elements in $\operatorname{Proj}(\mathbb{Z}[h, k])$.

Proposition 3.9 ([1]). *$C_0 := \{p\mathbb{Z}[x] \mid p \text{ is a prime integer}\}$ is the only coefficient subset of $\operatorname{Proj}(\mathbb{Z}[h, k])$.*

Proof. We sketch the proof from [1] briefly. If Γ is a coefficient subset of $\operatorname{Proj}(\mathbb{Z}[h, k])$ such that $\Gamma \neq C_0$, then $\Gamma \cap C_0 = \emptyset$. Let p be a prime integer. Then $(p)^{\uparrow}$ is infinite and $\bigcup_{\gamma \in \Gamma}(\gamma, p)^{\uparrow} = (p)^{\uparrow}$. Hence Γ is infinite. Therefore there exist distinct elements α and β in $\Gamma \setminus C_0 \setminus \{(x), (\frac{1}{x})\}$; say $\alpha = (f(x))$, $\beta = (g(x))$, for two relatively prime irreducible polynomials $f(x)$ and $g(x)$ of $\mathbb{Z}[x]$ of positive degree. By Proposition 3.7, $(f + yg)$ is a prime ideal in $\mathbb{Z}[x, y]$, where y is an indeterminate over $\mathbb{Z}[x]$. By Hilbert's Irreducibility Theorem 3.8, there exists a prime integer p so that $f + pg$ is irreducible in $\mathbb{Z}[x]$. By Definition 3.2 (ii), no height-two prime ideals contain both f and g. If $(f + pg) \notin \Gamma$, we contradict $(f, g)^{\uparrow} = \emptyset$. Hence $(f + pg) \in \Gamma$. But $(f, p)^{\uparrow} \subseteq (f)^{\uparrow} \cap (f + pg)^{\uparrow} = (f, f + pg)^{\uparrow}$. This contradicts Definition 3.2 (ii). ☐

Remark 3.10 ([1]). Let (S, T) be a $\operatorname{ht}(1, 2)$-pair in $\operatorname{Proj}(\mathbb{Z}[h, k])$. If $T \neq \emptyset$, then (S, T) has at most one radical element in C_0.

Proposition 3.11 ([1]). *Let (S, T) be a $\operatorname{ht}(1, 2)$-pair in $\operatorname{Proj}(\mathbb{Z}[h, k])$. If (S, T) has a radical element Q in $\operatorname{Proj}(\mathbb{Z}[h, k])$ then either*

(i) *$S \cap C_0 \subseteq \bigcup_{M \in T}(M^{\downarrow} \cap C_0)$ or*

(ii) *$Q \in C_0$.*

In case (ii), *if $T = \emptyset$, then $S \subseteq C_0$; if $T \neq \emptyset$, then Q is the only radical element.*

Sketch of the proof from [1]. If (i) fails, there exists $P \in S \cap C_0$ with $T \cap P^{\uparrow} = \emptyset$. Then $Q^{\uparrow} \cap P^{\uparrow} = \emptyset$. Thus, by Definition 3.2 (iv), $Q \in C_0$. Also $\bigcup_{s \in S}(s, Q)^{\uparrow} \subseteq T \subseteq Q^{\uparrow}$. Thus if $T = \emptyset$, then $s \in C_0$, for all $s \in S$. If $T \neq \emptyset$, then T contains an element of form $(f(x), p)$, where p is a prime integer and either $f(x) \in \mathbb{Z}[x]$ has positive degree or $f(x) = \frac{1}{x}$. In either case $(f(x), p) \in Q^{\uparrow}$ implies $(p) = Q$, and so Q is unique. ☐

Meral Arnavut notes that, if Condition 1 of Proposition 3.11 (i) is not satisfied, then it is difficult to find radical elements; cf. [1], and Proposition 3.5 and Proposition 3.11 of this paper.

Proposition 3.12 ([1]). *Let* (S, T) *be a* $\mathrm{ht}(1, 2)$*-pair in* $\mathrm{Proj}(\mathbb{Z}[h, k])$ *such that*

(i) $S \cap C_0 \subseteq \bigcup_{M \in T} (M^{\downarrow} \cap C_0)$, *and*

(ii) $\bigcup_{s \in S} (s, \frac{1}{x})^{\uparrow} \subseteq T$, *or* (ii') $\bigcup_{s \in S} (s, x)^{\uparrow} \subseteq T$.

Then (S, T) *has infinitely many radical elements in* $\mathrm{Proj}(\mathbb{Z}[h, k])$.

Proof. We give the proof with hypothesis (ii); the proof for (ii') is similar (replace $\frac{1}{x}$ by x). Since $(s, \frac{1}{x})^{\uparrow} \subseteq T$, for every $s \in S$, and T is finite, $(\frac{1}{x}) \notin S$. Therefore $S \subseteq \mathrm{Spec}(\mathbb{Z}[x])$. If $T = \emptyset$, then, for every $s \in S$, $s^{\uparrow} \subseteq \mathrm{Spec}(\mathbb{Z}[x])$. Thus, by Proposition 3.1, (S, T) has infinitely many radical elements in $\mathrm{Proj}(\mathbb{Z}[h, k])$ as desired. If $T \neq \emptyset$, let $p_1, \ldots, p_r$ denote the distinct positive prime integers such that

$$\{(p_1), \ldots, (p_r)\} = \bigcup_{M \in T} (M^{\downarrow} \cap C_0).$$

Then, for each $t \in T$, some $p_i \in t$. Let $f_1, \ldots, f_n$ be irreducible polynomials of $\mathbb{Z}[x]$ of positive degree so that $S - C_0 = \{(f_1), \ldots, (f_n)\}$. Let $T' = T - (\frac{1}{x})^{\uparrow}$. Therefore $T' \subseteq \mathrm{Spec}(\mathbb{Z}[x])$ and $S \subseteq \mathrm{Spec}(\mathbb{Z}[x])$. Since $\mathrm{Spec}(\mathbb{Z}[x])$ is CZP, there are infinitely many radical elements for (S, T') in $\mathrm{Spec}(\mathbb{Z}[x])$. By Proposition 3.10, (S, T') has at most one radical element in C_0. Thus (S, T') has infinitely many radical elements in $\mathrm{Spec}(\mathbb{Z}[x]) - C_0$. Let P_0 be such a radical element; say $P_0 = (f(x))$, where $f(x)$ is an irreducible polynomial of $\mathbb{Z}[x]$ of positive degree so that $f(x) \notin x\mathbb{Z}[x] \cup f_1\mathbb{Z}[x] \cup \cdots \cup f_n\mathbb{Z}[x] \cup \mathbb{Z}$. Let λ be a positive integer greater than the degree of $f(x)$. Then $f(x)$ and the product $p_1 \cdots p_r f_1 \cdots f_n x^{\lambda}$ are relatively prime in $\mathbb{Z}[x]$. By Proposition 3.7, $(y p_1 \cdots p_r f_1 \cdots f_n x^{\lambda} + f(x))$ is a prime ideal of $\mathbb{Z}[x, y]$, where y is an indeterminate over $\mathbb{Z}[x]$. By Hilbert's Irreducibility Theorem 3.8, for each λ, there exists a prime integer p_{λ} such that $g_{\lambda}(x) = p_{\lambda} p_1 \cdots p_r f_1 \cdots f_n x^{\lambda} + f(x)$ is an irreducible polynomial of $\mathbb{Z}[x]$; thus $w_{\lambda} := (g_{\lambda}(x))$ is a prime ideal of $\mathbb{Z}[x]$. For each $\lambda > \deg(f)$, w_{λ} is a radical element for (S, T) in $\mathrm{Proj}(\mathbb{Z}[h, k])$. Thus (S, T) has infinitely many radical elements. $\square$

4 The Conjecture for $\mathrm{Proj}(\mathbb{Z}[h, k])$ and Previous Partial Results

In Proposition 3.12 some conditions are given for a $\mathrm{ht}(1, 2)$-pair (S, T) so that there are infinitely many radical elements. Item (ii) of Proposition 3.12 implies $(\frac{1}{x}) \notin S$ and item (ii)' implies that $(x) \notin S$. In either case, we get infinitely many radical elements in $\mathrm{Proj}(\mathbb{Z}[h, k])$. If both (x) and $(\frac{1}{x})$ belong to S, it is more difficult to find a radical

element. The following conjecture first given by Aihua Li and Sylvia Wiegand, then adjusted by Meral Arnavut, addresses this case; cf. [1, 5].

Proj($\mathbb{Z}[h, k]$) Conjecture 4.1 ([1]). Let (S, T) be a ht$(1, 2)$-pair in Proj($\mathbb{Z}[h, k]$). Assume

(i) $S \cap C_0 \subseteq \bigcup_{m \in T} (m^{\downarrow} \cap C_0)$, and

(ii) $(x) \in S, (\frac{1}{x}) \in S$.

Then there exist infinitely many radical elements for (S, T) in Proj($\mathbb{Z}[h, k]$).

It appears that some axiom regarding the existence of radical elements analogous to Axiom RW is necessary for Proj($\mathbb{Z}[h, k]$). The following axiom was proposed by Li and Wiegand and modified by Arnavut, cf. [1, 5].

Axiom 4.2 (Axiom P5, [1]). Let U be a poset of dimension two.

(P5a) There exist a unique coefficient subset Γ of U and special elements $u_1, u_2 \in U$ such that $(u_1, u_2)^{\uparrow} = \emptyset$ and Γ is attached to u_1 and u_2. (Thus, for every $\gamma \in \Gamma$, $|(\gamma, u_1)^{\uparrow}| = 1 = |(\gamma, u_2)^{\uparrow}|$.)

(P5b) Let S be a nonempty finite subset of $H_1(U)$ and let T be a nonempty finite subset of $H_2(U)$.

    (P5b.1) If $\gamma^{\uparrow} \cap T \neq \emptyset$, for every $\gamma \in S \cap \Gamma$, then there exist infinitely many radical elements for (S, T).

    (P5b.2) If there exists an element $\gamma \in S \cap \Gamma$ such that $\gamma^{\uparrow} \cap T = \emptyset$, then there is at most one possible radical element γ_0 for (S, T), and $\gamma_0 \in \Gamma \setminus S$.

Arnavut shows that Conjecture 4.1 implies Axiom P5 above for Proj($\mathbb{Z}[h, k]$) and that $U := \text{Proj}(\mathbb{Z}[h, k]) \setminus C_0$ is CZP; cf. [1]. We believe that this will lead to a complete characterization of Proj($\mathbb{Z}[h, k]$).

We give a special case of the Conjecture 4.1 when $T = \emptyset$.

Proposition 4.3 ([1]). *Suppose S is a finite subset of $H_1(\text{Proj}(\mathbb{Z}[h, k]))$ of the form*

$$S = \left\{ (x), \left(\frac{1}{x} \right), (f_1), \dots, (f_n) \right\},$$

where $f_1, \dots, f_n$ are monic irreducible polynomials of $\mathbb{Z}[x]$ of positive degree. Then $(S, \emptyset)$ has infinitely many radical elements in Proj($\mathbb{Z}[h, k]$).

Remark 4.4. Similarly one can find infinitely many radical elements if $T = \emptyset$ and S is a finite subset of $H_1(\text{Proj}(\mathbb{Z}[h, k]))$ such that $S = \{(x), (\frac{1}{x}), (f_1), \dots, (f_n)\}$, where $f_1, \dots, f_n$ are irreducible polynomials in $\mathbb{Z}[x]$ of positive degree with $c(f_i) = \pm 1$. However we do not know what happens when $T = \emptyset$, $c(f_i) \neq \pm 1$ and $\ell(f_i) \neq \pm 1$. In this case if there is a radical element $(g(x))$ where $g(x)$ is an irreducible polynomial,

then $c(g) = \pm 1$, $\ell(g) = \pm 1$ and $(g(x), f_i(x)) = 1$. If we could find such radical elements, the conjecture would hold for $T = \emptyset$. This might help prove the conjecture for the $T \neq \emptyset$ case as well.

Meral Arnavut introduces the following notation and gives some partial results related to the conjecture, recorded here as Theorem 4.6, cf. [1].

Notation 4.5. Let T be a nonempty finite subset of $H_2(\mathrm{Proj}(\mathbb{Z}[h, k]))$.

Let $F := \{p \in \mathbb{Z}, p \text{ prime} \mid (x, p) \in T\}$ and let $G := \{p \in \mathbb{Z}, p \text{ prime} \mid (\frac{1}{x}, p) \in T\}$. Then $A_1 := F \setminus G$, $A_2 := F \cap G$, and $A_3 := G \setminus F$ are disjoint sets.

Define $a_i := \prod_{p \in A_i} p$, for $i = 1, 2, 3$. Thus a_1, a_2 and a_3 are pairwise relatively prime integers. For each i, if $A_i = \emptyset$, we set $a_i = 1$. Now let $n \in \mathbb{N}$, and define $f_n(x) \in \mathbb{Z}[x]$ by

$$f_n(x) := \begin{cases} a_3 x^n + a_1, & \text{if } F \cap G = \emptyset \text{ (i.e., } a_2 = 1), \\ a_2^n a_3 x^2 + a_1 a_3 x + a_2^n a_1, & \text{if } F \cap G \neq \emptyset. \end{cases}$$

Theorem 4.6 ([1]). *Let (S, T) be an ht$(1, 2)$-pair in $\mathrm{Proj}(\mathbb{Z}[h, k])$ and let F, G, A_1, A_2, A_3, a_1, a_2, a_3 and f_n be as in as in Notation 4.5. Suppose*

- $T \subseteq (x)^\uparrow \cup (\frac{1}{x})^\uparrow$,
- $S \cap C_0 \subseteq \{(p) \mid p \in F \cup G\}$,
- $(x) \in S$, $(\frac{1}{x}) \in S$.

Then:

(i) *If $(s, f_n)^\uparrow \subseteq T$, for every $s \in S \setminus (C_0 \cup \{(x), (\frac{1}{x})\})$, then (f_n) is a radical element for (S, T) in $\mathrm{Proj}(\mathbb{Z}[h, k])$.*

(ii) *If $S \setminus C_0 = \{(x), (\frac{1}{x})\}$, then (S, T) has infinitely many radical elements in $\mathrm{Proj}(\mathbb{Z}[h, k])$.*

(iii) *If $F \cap G = \emptyset$ and, for every irreducible polynomial $f(x)$ of $\mathbb{Z}[x]$ such that $(f) \in S \setminus (C_0 \cup \{(x), (\frac{1}{x})\})$, (a) or (b) holds, that is,*

    (a) *$\ell(f)$ is a unit, and a_1 divides every coefficient of $f(x)$ except $\ell(f)$,*

    (b) *$c(f)$ is a unit, and a_3 divides every coefficient of $f(x)$ except $c(f)$,*

    then (S, T) has infinitely many radical elements in $\mathrm{Proj}(\mathbb{Z}[h, k])$.

(iv) *If $F \cap G = \emptyset$ and $S \setminus C_0 = \{(x), (\frac{1}{x})\} \cup \{(x + \alpha)\}$, for some $\alpha \in \mathbb{Z}$ such that a_1 and α are relatively prime, then (S, T) has a radical element in $\mathrm{Proj}(\mathbb{Z}[h, k])$.*

Corollary 4.7 ([1]). *Let*

$$S = \left\{ (p_1), \ldots, (p_n), (x), \left(\frac{1}{x}\right), (f_1), \ldots, (f_m) \right\},$$

$$T = \left\{ (x, p_1), \ldots, (x, p_l), \left(\frac{1}{x}, p_{l+1}\right), \ldots, \left(\frac{1}{x}, p_n\right) \right\},$$

where $0 \leq l \leq n$, $p_1, \ldots, p_n$ are distinct prime integers.

(i) If $f_i(x) \in \mathbb{Z}[x]$ has the form $x^{d_i} + p_1 \cdots p_l b_i$, for some $d_i \in \mathbb{N}$ and $b_i \in \mathbb{Z}$ with $1 \leq i \leq m$, then (S, T) has infinitely many radical elements.

(ii) If $f_i(x) \in \mathbb{Z}[x]$ has the form $b_i\, p_{l+1} \cdots p_n x^{d_i} + 1$, for some $d_i \in \mathbb{N}$ and $b_i \in \mathbb{Z}$ with $1 \leq i \leq m$, then (S, T) has infinitely many radical elements.

5 New Results Supporting the Conjecture

In this section we give some new results that further support Conjecture 4.1. We consider various different types of $\mathrm{ht}(1, 2)$-pairs in $\mathrm{Proj}(\mathbb{Z}[h, k])$.

Theorem 5.1. *Let (S, T) be an $\mathrm{ht}(1, 2)$-pair in $\mathrm{Proj}(\mathbb{Z}[h, k])$. Suppose*

(i) $T \subseteq (x)^{\uparrow}$,

(ii) $S \cap C_0 \subseteq \{(p) \mid (x, p) \in T, p \in \mathrm{Spec}(\mathbb{Z})\}$,

(iii) $S \setminus C_0 = \{(x), (\frac{1}{x})\} \cup \{(a_1 x + 1), \ldots, (a_m x + 1)\}$ for some $a_i \in \mathbb{Z}, i = 1, \ldots, m$.

Then (S, T) has infinitely many radical elements in $\mathrm{Proj}(\mathbb{Z}[h, k])$.

Proof. Assume that $T \neq \emptyset$. Since $T \subseteq (x)^{\uparrow}$ by (i), we have $F \neq \emptyset$ where $F := \{p \in \mathbb{Z}, p\text{ prime} \mid (x, p) \in T\}$. Let $\lambda \in \mathbb{N}$ be such that $\lambda \geq 2$. Define

$$g_\lambda(x) := x^{m+\lambda} + b(a_1 x + 1) \cdots (a_m x + 1) \in \mathbb{Z}[x]$$

where the a_i are as in (iii) and $b = \prod_{p \in F} p$. We show $w_\lambda = (g_\lambda(x))$ is a radical element for (S, T) in $\mathrm{Proj}(\mathbb{Z}[h, k])$. By Eisenstein's Criteria, $g_\lambda(x)$ is irreducible in $\mathbb{Z}[x]$. To see that w_λ satisfies Definition 2.2, let $t \in T$. Then $t = (x, p)$, for some $p \in F$. But $p \mid c(g_\lambda)$, and so $w_\lambda \subset t$, for every $t \in T$. Let $s \in S$ and let $M \in H_2(\mathrm{Proj}(\mathbb{Z}[h, k]))$ be such that $g_\lambda(x) \in M$ and $s \subset M$. We consider $(w_\lambda, s)^{\uparrow}$ for all possible types of $s \in S$:

(i) Since $(g_\lambda(x), a_i x + 1) = (1)$, $(g_\lambda(x), a_i x + 1)^{\uparrow} = \emptyset$, for all $i = 1, \ldots, m$.

(ii) Since $(g_\lambda(x), \frac{1}{x}) = (1)$, $(\frac{1}{x}, g_\lambda(x))^{\uparrow} = \emptyset$.

(iii) Since $(g_\lambda(x), x) = (x, b)$, $M = (x, p)$, for some $p \in F$, and hence $M \in T$.

(iv) Since $(g_\lambda(x), p) = (x^{m+\lambda}, p)$, for $p \in F$ such that $p \mid b$, $M = (x, p)$. Thus $M \in T$, and so $(p, g_\lambda(x))^{\uparrow} \in T$.

Thus $w_\lambda = (g_\lambda(x))$ is a radical element for (S, T) in $\mathrm{Proj}(\mathbb{Z}[h, k])$ for each $\lambda \in \mathbb{N}$, and so there are infinitely many radical elements w_λ for (S, T).

If $T = \emptyset$, then take $b = 1$ and define

$$g_\lambda(x) := x^{m+\lambda} + (a_1 x + 1) \cdots (a_m x + 1) \in \mathbb{Z}[x].$$

Similarly $w_\lambda = (g_\lambda(x))$ is a radical element for (S, T) in $\mathrm{Proj}(\mathbb{Z}[h, k])$, for $\lambda \in \mathbb{N}$. $\qquad \square$

Remark 5.2. Similarly there exist infinitely many radical elements for a ht$(1, 2)$-pair (S, T) in Proj$(\mathbb{Z}[h, k])$ satisfying the following:

 (i) $T \subseteq (\frac{1}{x})^{\uparrow}$,

 (ii) $S \cap C_0 \subseteq \{(p) \mid (\frac{1}{x}, p) \in T, p \in \text{Spec}(\mathbb{Z})\}$,

 (iii) $S \setminus C_0 = \{(x), (\frac{1}{x})\} \cup \{(x + a_1), \ldots, (x + a_m)\}$ for some $a_i \in \mathbb{Z}, i = 1, \ldots, m$.

Proposition 5.3. *Consider*

$$S = \{(p_1), \ldots, (p_n), (x), (\frac{1}{x}), (x + a_1), \ldots, (x + a_m)\},$$

$$T = \{(x, p_1), (\frac{1}{x}, p_2), \ldots, (\frac{1}{x}, p_n), (x + a_1, p_1), \ldots, (x + a_m, p_1)\}$$

where $p_1, \ldots, p_n$ are distinct prime integers, $n > 1$, $a_1, \ldots, a_m \in \mathbb{Z}$ and $(a_k, p_1) = 1$ for each $k = 1, \ldots, m$. Then (S, T) has infinitely many radical elements in Proj$(\mathbb{Z}[h, k])$.

Proof. Let $\lambda \in \mathbb{N}$. Define $h_\lambda(x) = b^\lambda x^\lambda (x + a_1) \ldots (x + a_m) + p_1^\lambda$ where $b = \prod_{i=2}^{n} p_i$. We show that $w_\lambda = (h_\lambda(x))$ is a radical element for (S, T) in Proj$(\mathbb{Z}[h, k])$. First, by Eisenstein's Criteria for $\mathbb{Z}[\frac{1}{x}]$, $h_\lambda(x)$ is irreducible in $\mathbb{Z}[\frac{1}{x}]$. Also $w_\lambda \subset t$ for all $t \in T$. Let $s \in S$ and $M \in H_2(\text{Proj}(\mathbb{Z}[h, k]))$ be such that $h_\lambda(x) \in M$ and $s \subset M$. We consider $(w_\lambda, s)^{\uparrow}$ for all possible types of $s \in S$:

Since $(h_\lambda(x), x + a_k) = (x + a_k, p_1^\lambda)$, $M = (x + a_k, p_1)$ is the only maximal ideal that contains $(h_\lambda(x), x + \alpha_k)$, for $k = 1, \ldots, m$, that is, $(h_\lambda(x), x + a_k)^{\uparrow} \in T$.

Since $(h_\lambda(x), x) \subseteq (x, p_1^\lambda)$, $M = (x, p_1)$ is the only maximal ideal that contains $(h_\lambda(x), x)$, that is, $(h_\lambda(x), x)^{\uparrow} \in T$.

Since $(h_\lambda(x), \frac{1}{x}) = (b^\lambda, \frac{1}{x})$, for $i = 2, \ldots, n$, M has form $(\frac{1}{x}, p_i)$ for some i, and the $(\frac{1}{x}, p_i)$ are the only maximal ideals that contain $(h_\lambda(x), \frac{1}{x})$, for $i = 2, \ldots, n$.

Since $(h_\lambda(x), p_1) = (b^\lambda x^\lambda (x + a_1) \ldots (x + a_m))$, $M = (x, p_1)$ or $M = (x + a_k, p_1) \in T$, for some $k = 1, \ldots, m$, and these are the only maximal ideals that contain $(h_{\lambda(x)}, p_1)$.

If $s = (p_i)$, for $i = 2, \ldots, n$, then we get $(h_\lambda(x), p_i) = (p_1^\lambda, p_i) = (1)$ since $p_i \mid b$. Therefore, for each $\lambda \in \mathbb{N}$, w_λ is a radical element for (S, T). $\square$

Proposition 5.4. *Let $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$ be such that $\gcd(\alpha_1, \ldots, \alpha_m) \neq 1$. Suppose that $p_1, \ldots, p_k$ are all the prime integers that are factors of any of the α_i and that p_1 divides each of the α_i. Say each $\alpha_i = p_1^{e_{i1}} \cdots p_k^{e_{ik}}$, for some $e_{i\ell} \geq 0$. Then let $n \geq 1$ and choose prime integers $q_1, \ldots, q_n$ distinct from $p_1, \ldots, p_k$. Let*

$$B_1 := \{(x, q_j), (x + \alpha_i, q_j)\}_{1 \leq j \leq n}^{1 \leq i \leq m},$$

$$B_2 := \{(x + \alpha_i, p_\ell) \mid p_\ell \nmid \alpha_i\}_{1 \leq i \leq m}^{1 \leq \ell \leq k},$$

$$B_3 := \{(x, p_1) \ldots (x, p_k)\},$$

and set

$$S = \left\{(x), \left(\frac{1}{x}\right), (x + \alpha_1) \dots, (x + \alpha_m)\right\} \cup \{(q_j)\}_{1 \le j \le n} \cup \{(p_\ell)\}_{1 \le \ell \le k},$$

$$T = B_1 \cup B_2 \cup B_3.$$

Then (S, T) has infinitely many radical elements in $\mathrm{Proj}(\mathbb{Z}[h, k])$.

Proof. Let $\lambda \in \mathbb{N}$. Define $a_0 := \prod_{\substack{1 \le \ell \le k \\ 1 \le j \le n}} p_\ell \cdot q_j$ and $h_\lambda(x) = x^\lambda (x + \alpha_1) \cdots (x + \alpha_m) + a_0$.

We show that $w_\lambda = (h_\lambda(x))$ is a radical element for (S, T) in $\mathrm{Proj}(\mathbb{Z}[h, k])$.

Note that $h_\lambda(x)$ is irreducible by Eisenstein in $\mathbb{Z}[x]$, since $\gcd(\alpha_1, \dots, \alpha_m) \ne 1$ and $p_1 \mid \gcd(\alpha_1, \dots, \alpha_m)$. Also $w_\lambda \subset t$ for all $t \in T$.

Let $s \in S$ and $t \in H_2(\mathrm{Proj}(\mathbb{Z}[h, k]))$ be such that $h_\lambda(x) \in t$ and $s \subseteq t$.

If $s = (q_j)$, $(h_\lambda, q_j) = (x^\lambda (x + \alpha_1) \cdots (x + \alpha_m), q_j)$, for $j = 1, \dots, n$, and so $(h_\lambda, q_j)^\uparrow = \{(x, q_j), (x + \alpha_1, q_j), \dots, (x + \alpha_m, q_j)\} \subset B_1$. Similarly, if $s = (p_\ell)$, then $(h_\lambda, p_\ell)^\uparrow \subset B_2 \cup B_3$, for $\ell = 1, \dots, k$. If $s = (x)$, then $(h_\lambda, x) \subset (x, q_j)$, for all $j, 1 \le j \le n$ and also $(h_\lambda, x) \subset (x, p_\ell)$, $1 \le \ell \le k$. If $s = (\frac{1}{x})$, then $(h_\lambda, \frac{1}{x}) = (1)$ because h_λ is a monic polynomial of $\mathbb{Z}[x]$. If $s = (x + \alpha_i)$ for some i, $1 \le i \le m$, then $(h_\lambda, x + \alpha_i) \subset (x + \alpha_i, q_j) \in B_1$ for some $j, 1 \le j \le \ell$. If $p_\ell \nmid \alpha_i$, then $(h_\lambda, x + \alpha_i) \subset (x + \alpha_i, p_\ell) \in B_2$ and if $p_\ell \mid \alpha_i$, $(h_\lambda, x + \alpha_i) \subset (x + \alpha_i, p_\ell) \in B_3$, for each $i, 1 \le i \le m$ and $1 \le \ell \le k$.

Therefore, in any of the latter cases, $(h_\lambda, x + \alpha_i)^\uparrow \subset T$, for $i, 1 \le i \le m$. Thus w_λ is a radical element for (S, T) in $\mathrm{Proj}(\mathbb{Z}[h, k])$. Now, since $\lambda \in \mathbb{N}$, there are infinitely many w_λ in $\mathrm{Proj}(\mathbb{Z}[h, k])$ and so (S, T) has infinitely many radical elements. $\square$

Theorem 5.5. *There exist infinitely many radical elements for every* $\mathrm{ht}(1, 2)$*-pair in* $\mathrm{Proj}(\mathbb{Z}[h, k])$ *of the form* $S = \{(x), (\frac{1}{x}), (p_1), \dots, (p_n)\}$ *and* $T = \{(x, p_1), \dots, (x, p_n), (\frac{1}{x}, p_1), \dots, (\frac{1}{x}, p_n)\}$*, where* $p_1, \dots, p_n$ *are distinct prime integers.*

Proof. First consider the subsets

$$S_x := \{(x), (p_1), \dots, (p_n)\}, \qquad T_x := \{(x, p_1), \dots, (x, p_n)\},$$

$$S_{\frac{1}{x}} := \left\{\left(\frac{1}{x}\right), (p_1), \dots, (p_n)\right\}, \quad T_{\frac{1}{x}} := \left\{\left(\frac{1}{x}, p_1\right), \dots, \left(\frac{1}{x}, p_n\right)\right\}.$$

Then $S_x \cup T_x \subseteq \mathrm{Spec}(\mathbb{Z}[x])$. Thus we see that for every $\lambda \in \mathbb{N}$,

$$f_\lambda(x) := x^\lambda + p_1 \cdots p_n \in \mathbb{Z}[x]$$

(f_λ) is a radical element for (S_x, T_x) in $\mathrm{Spec}(\mathbb{Z}[x])$ since $f(x)$ is irreducible by Eisenstein. Similarly for

$$h_\lambda\left(\frac{1}{x}\right) := p_1 \cdots p_n + \frac{1}{x^\lambda} \in \mathbb{Z}\left[\frac{1}{x}\right]$$

$(h(\frac{1}{x}))$ is a radical element for $\{S_{\frac{1}{x}}, T_{\frac{1}{x}}\}$. We identify $h(\frac{1}{x})$ with

$$g_\lambda(x) := x^\lambda h_\lambda\left(\frac{1}{x}\right) = x^\lambda p_1 \cdots p_n + 1 \in \mathbb{Z}[x].$$

Let y be another indeterminate over $\mathbb{Z}[x]$ and let $k(x) = p_1 \cdots p_n x^\lambda$. Then

$$f_\lambda(x)g_\lambda(x) = x^{2\lambda} p_1 \cdots p_n + ((p_1 \cdots p_n)^2 + 1)x^\lambda + p_1 \cdots p_n.$$

Since $f_\lambda(x)g_\lambda(x)$ and $k(x)$ are relatively prime elements of $\mathbb{Z}[x]$, $f_\lambda(x)g_\lambda(x) + yk(x)$ is a prime ideal in $\mathbb{Z}[x, y]$ by Proposition 3.7. Thus there exists a prime integer q so that $f_\lambda(x)g_\lambda(x)+q(p_1 \cdots p_n x^\lambda)$ is irreducible in $\mathbb{Z}[x]$ by Hilbert's Irreducibility Theorem 3.8.

We show that $w_\lambda := (r_\lambda(x)) = (f_\lambda(x)g_\lambda(x) + qk(x))$ is a radical element for (S, T) for all $\lambda \in \mathbb{N}$. First observe

$$r_\lambda(x) = p_1 \cdots p_n x^{2\lambda} + ((p_1 \cdots p_n)^2 + 1 + qp_1 \cdots p_n)x^\lambda + p_1 \cdots p_n.$$

It is easy to see that $w_\lambda \subset t$ for every $t \in T$, since $p_i \mid \ell(r)$ and $p_i \mid c(r)$, for $i = 1, \ldots, n$. Also $(r_\lambda, x) \subseteq (p_i, x)$ for all $i = 1, \ldots, n$. Similarly $(r_\lambda, \frac{1}{x}) \subseteq (\frac{1}{x}, p_i)$, for all $i = 1, \ldots, n$. Moreover $(r_\lambda, p_i) = (x^\lambda, p_i)$ and so (x, p_i) is the only maximal element that contains $(r_\lambda, p_i)^\uparrow$, for $i = 1, \ldots, n$. Thus $(r_\lambda, p_i)^\uparrow \in T$, for $i = 1, \ldots, n$. Therefore w_λ is a radical element for each $\lambda \in \mathbb{N}$. $\square$

Example 5.6. There are infinitely many radical elements for every ht$(1, 2)$-pair in Proj$(\mathbb{Z}[h, k])$ of the form

$$S = \left\{(x), \left(\frac{1}{x}\right), (2), (3), (5)\right\},$$

$$T = \left\{(x, 2), (x, 3), (x, 5), \left(\frac{1}{x}, 2\right), \left(\frac{1}{x}, 3\right), \left(\frac{1}{x}, 5\right)\right\}.$$

First consider the following subsets as in the previous proof of Theorem 5.5:

$$S_x = \{(x), (2), (3), (5)\}, \qquad T_x = \{(x, 2), (x, 3), (x, 5)\},$$

$$S_{\frac{1}{x}} = \left\{\left(\frac{1}{x}\right), (2), (3), (5)\right\}, \quad T_{\frac{1}{x}} = \left\{\left(\frac{1}{x}, 2\right), \left(\frac{1}{x}, 3\right), \left(\frac{1}{x}, 5\right)\right\}.$$

Then $S_x \cup T_x \subseteq \mathrm{Spec}\mathbb{Z}[x]$ and for every $\lambda \in \mathbb{N}$, $f_\lambda(x) := x^\lambda + 30$ in $\mathbb{Z}[x]$ generates a radical element for (S_x, T_x) in $\mathrm{Spec}(\mathbb{Z}[\frac{1}{x}])$. Similarly $h_\lambda(\frac{1}{x}) := 30 + \frac{1}{x^\lambda} \in \mathbb{Z}[\frac{1}{x}]$ is a radical element for $(S_{\frac{1}{x}}, T_{\frac{1}{x}})$. We identify $h_\lambda(\frac{1}{x})$ with $g_\lambda(x) := 30x^\lambda + 1 \in \mathbb{Z}[x]$. Let y be another indeterminate over $\mathbb{Z}[x]$. Since $f_\lambda(x)g_\lambda(x)$ and $30x^\lambda$ are relatively prime elements of $\mathbb{Z}[x]$, $(f_\lambda(x)g_\lambda(x) + y(30x^\lambda))$ is a prime ideal of $\mathbb{Z}[x, y]$ by Proposition 3.7. There exists a prime integer q so that $f_\lambda(x)g_\lambda(x) + q(30x^\lambda)$ is irreducible in $\mathbb{Z}[x]$ by Hilbert's Irreducibility Theorem 3.8. Therefore $w = (f_\lambda(x)g_\lambda(x) + 30qx^\lambda)$ is a radical element for each $\lambda \in \mathbb{N}$.

In [1], Arnavut raises some questions about particular $\mathrm{ht}(1, 2)$-pairs in $\mathrm{Proj}(\mathbb{Z}[h, k])$. We consider one such unanswered question below.

Question 5.7. Does (S, T) have a radical element if

$$S = \left\{(p_1), \ldots, (p_n), (x), \left(\frac{1}{x}\right), (x - a), (x - b)\right\},$$

$$T = \left\{(x, p_1), \ldots, (x, p_\ell), \left(\frac{1}{x}, p_{\ell+1}\right), \ldots, \left(\frac{1}{x}, p_n\right)\right\},$$

where $0 \leq \ell \leq n$, $\gcd(ab, p_1 \cdots p_\ell) = 1$, and the p_i are distinct prime integers for $i = 1, \ldots, n$?

Theorem 5.8 answers Question 5.7 in a special case.

Theorem 5.8. *Assume a and b are relatively prime integers and let S and T be the following subsets of* $\mathrm{Proj}(\mathbb{Z}[h, k])$:

$$S := \left\{(p_1), \ldots, (p_n), (x), \left(\frac{1}{x}\right), (x - a), (x - b)\right\},$$

$$T := \left\{(x, p_1), \ldots, (x, p_\ell), \left(\frac{1}{x}, p_{\ell+1}\right), \ldots, (\frac{1}{x}, p_n)\right\},$$

where $0 \leq \ell \leq n$, $\gcd(ab, p_1 \ldots p_\ell) = 1$, *and the* p_i *are distinct prime integers for* $i = 1, \ldots, n$. *Suppose also that* $\mathbf{pq}$ *divides* $(1 - \mathbf{p}^t)(b^2 + ab + a^2) + \mathbf{q}a^3 b^3$ *and* $(1 - \mathbf{p}^t + \mathbf{q}b^2 a^2)(b + a)$ *where* $\mathbf{p} = p_1 \ldots p_\ell$, $\mathbf{q} = p_{\ell+1} \ldots p_n$, $t = lcm(\phi(a^2), \phi(b^2))$, *and* ϕ *is the Euler phi function. Then* (S, T) *has infinitely many radical elements in* $\mathrm{Proj}(\mathbb{Z}[h, k])$.

Proof. Consider the polynomial $g(x; u, v, w)$ of the form

$$g(x; u, v, w) = \mathbf{q}x^4 + (\mathbf{pq}u)x^3 + (\mathbf{pq}v)x^2 + (\mathbf{pq}w)x + (\mathbf{p})^t$$

where $t = lcm(\phi(a^2), \phi(b^2))$.

We show there exist infinitely many triples u, v, and $w \in \mathbb{Z}$ such that $(g(x; u, v, w))$ is a radical element for (S, T) in $\mathrm{Proj}(\mathbb{Z}[h, k])$.

First, by Euler's theorem, $(\mathbf{p})^{\phi(a^2)} \equiv 1 \pmod{a^2}$ and $(\mathbf{p})^{\phi(b^2)} \equiv 1 \pmod{b^2}$, since $\gcd(a, \mathbf{p}) = 1$ and $\gcd(b, \mathbf{p}) = 1$. Thus $\mathbf{p}^t - 1 \equiv 0 \pmod{a^2 b^2}$, that is, $a^2 b^2$ divides $\mathbf{p}^t - 1$.

To find u, v, and $w \in \mathbb{Z}$, we solve the system of linear equations $g(a; u, v, w) = 1$ and $g(b; u, v, w) = 1$; that is,

$$\mathbf{q}a^4 + \mathbf{pq}a^3 u + \mathbf{pq}a^2 v + \mathbf{pq}aw + \mathbf{p}^t = 1, \quad \text{and}$$

$$\mathbf{q}b^4 + \mathbf{pq}b^3 u + \mathbf{pq}b^2 v + \mathbf{pq}bw + \mathbf{p}^t = 1.$$

This becomes:

$$u + \frac{v}{a} + \frac{w}{a^2} = \frac{1 - \mathbf{p}^t - \mathbf{q}a^4}{\mathbf{p}\mathbf{q}a^3} \tag{5.1}$$

$$u + \frac{v}{b} + \frac{w}{b^2} = \frac{1 - \mathbf{p}^t - \mathbf{q}b^4}{\mathbf{p}\mathbf{q}b^3} \tag{5.2}$$

By subtracting (5.2) from (5.1), we get

$$v\left(\frac{b-a}{ab}\right) + w\left(\frac{b^2 - a^2}{a^2 b^2}\right) = \frac{(1 - \mathbf{p}^t)(b^3 - a^3) + q(b-a)a^3 b^3}{pqa^3 b^3}. \tag{5.3}$$

After simplifying (5.3), we deduce

$$v + w\left(\frac{a+b}{ab}\right) = \frac{(1 - \mathbf{p}^t)(b^2 + ab + a^2) + qa^3 b^3}{pqa^2 b^2}. \tag{5.4}$$

Therefore, for every $w = abk$ where $k \in \mathbb{Z}$, we get

$$v = \frac{(1 - \mathbf{p}^t)(b^2 + ab + a^2) + qa^3 b^3}{pqa^2 b^2} - (a+b)k. \tag{5.5}$$

Similarly, by eliminating v, and letting $w = abk$ for $k \in \mathbb{Z}$, we get

$$u = -\frac{(1 - \mathbf{p}^t + \mathbf{q}b^2 a^2)(b+a)}{\mathbf{p}\mathbf{q}a^2 b^2} - k. \tag{5.6}$$

Note that $\mathbf{p}\mathbf{q}$ divides $(1 - \mathbf{p}^t)(b^2 + ab + a^2) + \mathbf{q}a^3 b^3$ and $(1 - \mathbf{p}^t + \mathbf{q}b^2 a^2)(b+a)$. Moreover $a^2 b^2$ divides $1 - p^t$. Hence u and v are integers in (5.5) and (5.6).

Now we claim that for every triple of integers u, v and w that we have found above, the polynomial $g(x; u, v, w) := \mathbf{q}x^4 + (\mathbf{p}\mathbf{q}u)x^3 + (\mathbf{p}\mathbf{q}v)x^2 + (\mathbf{p}\mathbf{q}w)x + (\mathbf{p})^t \in \mathbb{Z}[x]$ generates a radical element for (S, T). First $g(x; u, v, w)$ is irreducible by Eisenstein's Criteria in $\mathbb{Z}[\frac{1}{x}]$. Since $c(g) = \mathbf{p}^t$ and $\ell(g) = \mathbf{q}$, we have $(g(x; u, v, w)) \subseteq z$, $\forall$ $z \in T$. Consider $(g(x; u, v, w), s)^{\uparrow}$ for each $s \in S$:

For $s = (x)$, $(g(x; u, v, w), x) = (\mathbf{p}^t, x) \subseteq (p_i, x) \in T$, where $i = 1, \ldots, \ell$.

For $s = (\frac{1}{x})$, we have $(g(x; u, v, w), \frac{1}{x}) = (\mathbf{q}, \frac{1}{x})$. The only maximal ideals containing $(\mathbf{q}, \frac{1}{x})$ are $(p_j, \frac{1}{x}) \in T$, for $j = \ell + 1, \ldots, n$.

For $s = (p_i)$, where $i = 1, \ldots, \ell$, we get $(g(x; u, v, w), p_i) = (\mathbf{q}x^4, p_i)$. The only maximal ideals containing $(\mathbf{q}x^4, p_i)$ are (x, p_i), since $(\mathbf{q}, p_i) = (1)$.

For $s = (p_j)$, where $j = \ell + 1, \ldots, n$, we have $(g(x; u, v, w), p_j) = (\mathbf{p}^t, p_j) = (1)$.

For $s = (x - a)$, we have $(g(x; u, v, w), x - a) = 1$ since $g(a; u, v, w) = (1)$.

Similarly, for $s = (x-b)$, we get $(g(x; u, v, w), x-b) = (1)$ since $g(b; u, v, w) = 1$.

Therefore we conclude that $(g(x; u, v, w))$ is a radical element for (S, T), for all u, v and $w \in \mathbb{Z}$ as chosen in the proof. Thus there are infinitely many radical elements for this (S, T)-pair in $\mathrm{Proj}(\mathbb{Z}[h, k])$. $\qquad\square$

Example 5.9. For $S = \{(2), (3), (x), (\frac{1}{x}), (x - 5), (x - 7)\}$ and $T = \{(x, 2), (\frac{1}{x}, 3)\}$, the polynomial $g(x; u, v, w) := 3x^4 + 6ux^3 + 6vx^2 + 6wx + 2^{420} \in \mathbb{Z}[x]$ generates a radical element for (S, T) for $w = 0$,

$$u = \frac{(1 - 2^{420} + 3 \cdot 5^2 \cdot 7^2)(5 + 7)}{2 \cdot 3 \cdot 5^2 \cdot 7^2} \in \mathbb{Z}, \quad \text{and}$$

$$v = \frac{(1 - 2^{420})(5^2 + 35 + 7^2) + 3 \cdot 5^3 \cdot 7^3}{2 \cdot 3 \cdot 5^2 \cdot 7^2} \in \mathbb{Z}.$$

Note that u and v are integers since $5^2 \cdot 7^2$ divides $1 - 2^{420}$, and also $2 \cdot 3 = 6$ divides the numerators $(1 - 2^{420} + 3 \cdot 5^2 \cdot 7^2)(5 + 7)$ and $(1 - 2^{420})(5^2 + 35 + 7^2) + 3 \cdot 5^3 \cdot 7^3$.

Also, if $w = 5 \cdot 7 \cdot k = 35k$, for $k \in \mathbb{Z}$, then we get different integers u and v, that is, $g(x; u, v, w)$ generates a different radical element for every $k \in \mathbb{Z}$. Therefore (S, T) has infinitely many radical elements in $\text{Proj}(\mathbb{Z}[h, k])$.

6 Summary and Questions

As the reader can see, there is still much to be done for the characterization of $\text{Proj}(\mathbb{Z}[h, k])$. In particular, the determination of which (S, T)-pairs have radical elements appears to be very challenging. In the future we hope to address some of the following questions:

Questions 6.1.   (i) In the setting of Theorem 4.7 with

$$S = \left\{ (p_1), \ldots, (p_n), (x), \left(\frac{1}{x} \right), (f_1), \ldots, (f_m) \right\},$$

$$T = \left\{ (x, p_1), \ldots, (x, p_l), \left(\frac{1}{x}, p_{l+1} \right), \ldots, \left(\frac{1}{x}, p_n \right) \right\},$$

where $0 \leq l \leq n$, $p_1, \ldots, p_n$ are distinct prime integers, is there a radical element for (S, T) if

   (a) The leading coefficient of $f_1 \cdots f_m$ is not a unit and $p_{l+1} \cdots p_n$ does not divide the leading coefficient of f_i, for some i?

   (b) The constant coefficient of $f_1 \cdots f_m$ is not a unit and $p_1 \cdots p_l$ does not divide the constant coefficient of f_i, for some i?

   (c) $\gcd(p_1 \cdots p_n, \ell(f_1 \cdots f_m)) = 1$ and $\gcd(p_1 \cdots p_n, c(f_1 \cdots f_m)) = 1$?

 (ii) Does the (S, T)-pair in Theorem 5.8 have a radical element if we remove some assumptions?

(iii) Let $u_1, \ldots, u_n, v_1, \ldots, v_m \in H_1(\text{Proj}(\mathbb{Z}[h, k])) - C_0$, and let $P \in C_0$. Does there exist a $Q \in C_0$ such that $|\bigcup_{i=1}^n (u_i, P)^{\uparrow}| = |\bigcup_{j=1}^m (v_j, P)^{\uparrow}|$?

(iv) What happens if we change T?

Bibliography

[1] Arnavut, M., The projective line over the integers. Arab J Sci Eng Sect C Theme Issues. 2001;26:1,31–44,1319–8025.

[2] Kaplansky, I., Commutative rings, Boston: Allyn and Bacon; 1970.

[3] Lang, S., Diophantine geometry. New York: Interscience; 1959.

[4] Li, A., Wiegand. S., Polynomial behavior of prime ideals in polynomial rings and the projective line over $\mathbb{Z}$. Proceedings, Factorization in Integral Domains; 1996, Iowa City, IA. Lecture notes in Pure and applied mathematics. New York: Marcel Dekker; 1997. p. 383–399.

[5] Li, A., Wiegand, S., Prime ideals in birational extensions of polynomials over the integers. J Pure Appl Algebra 1998;130:313–324.

[6] Wiegand, R., Homomorphisms of affine surfaces over a finite field. J Lond Math Soc (2). 1978;18:28–32.

[7] Wiegand, R., The prime spectrum of a two-dimensional affine domain. J. Pure Appl Algebra. 1986;40:209–214.

Author Information

Ela Celikbas, Department of Mathematics, University of Nebraska-Lincoln, Lincoln, NE, USA.
E-mail: s-ecelikb1@math.unl.edu

Christina Eubanks-Turner, Department of Mathematics, University of Louisiana at Lafayette, Lafayette, LA, USA.
E-mail: ceturner@louisiana.edu

On Zero Divisor Graphs

Jim Coykendall, Sean Sather-Wagstaff, Laura Sheppardson, and
Sandra Spiroff

Abstract. We survey the research conducted on zero divisor graphs, with a focus on zero
divisor graphs determined by equivalence classes of zero divisors of a commutative ring R.
In particular, we consider the problem of classifying star graphs with any finite number of
vertices. We study the pathology of a zero divisor graph in terms of cliques, we investigate
when the clique and chromatic numbers are equal, and we show that the girth of a Noetherian
ring, if finite, is 3. We also introduce a graph for modules that is useful for studying zero
divisor graphs of trivial extensions.

Keywords. Zero Divisor Graphs, Star Graphs, Commutative Rings.

2010 Mathematics Subject Classification. 13E15, 05C99.

1 Introduction

In this paper, the term "ring" (unless explicitly stated otherwise) means "commutative
ring with identity," and ring homomorphisms are assumed to respect identities.

This paper continues with the overarching goal of research in the area of zero divisor
graphs, namely the investigation of the interplay between the ring-theoretic properties
of a ring R and the graph theoretic properties of certain graphs obtained from R.
Our particular focus is on $\Gamma_E(R)$, the zero divisor graph determined by equivalence
classes, introduced in [29], and further studied in [8, 35] (see Definition 2.13). We
sometimes discuss $G(R)$, the graph defined by I. Beck, and $\Gamma(R)$, the graph defined
by D. F. Anderson and P. S. Livingston; see Definitions 2.1 and 2.4. A survey of the
research concerning these graphs is given in Section 2.

The graph $\Gamma_E(R)$ is a condensed version of $G(R)$ and $\Gamma(R)$, constructed in such a
way as to reduce the "noise" produced by individual zero divisors. (In [8], this is called
the "compressed" zero divisor graph.) Accordingly, $\Gamma_E(R)$ is smaller and simpler than
$G(R)$ and $\Gamma(R)$. One might expect that these graphs are finite or at least have a finite
clique number[1] if some finiteness condition is imposed on the ring, for example, if the
ring is Noetherian or Artinian. However, in [35], S. Spiroff and C. Wickham show
that the Noetherian condition is not enough to ensure a finite graph by exhibiting a

---

[1] See Appendix B for a brief dictionary of terms from graph theory.

Noetherian ring R such that $\Gamma_E(R)$ is an infinite star. Moreover, in the current paper, we show how to construct an Artinian ring R such that $\Gamma_E(R)$ is an infinite star; see Examples 3.28–3.30. Proposition 5.3 shows that these examples are minimal with respect to length.

Recall that Anderson and Livingston [10] completely characterized the star graphs of the form $\Gamma(R)$ where R is finite, proving that the star graphs G that occur as $\Gamma(R)$ are precisely those such that $|G|$ is a prime power. This leads to the question of whether or not a star graph of any size could be realized as $\Gamma_E(R)$. In Section 3, we investigate this question. In particular, Example 3.25 shows how to find rings R such that $\Gamma_E(R)$ is a star with c vertices where c is any positive number of the following form

$2^n - 4,$	$2^n - 3,$	$2^n - 2,$	$2^n - 1,$
$2^n,$	$2^n + 1,$	$2^n + 2,$	$2^n + 3,$
$2^n \cdot 3 - 2,$	$2^n \cdot 3 - 1,$	$2^n \cdot 3,$	$2^n \cdot 3 + 1,$
$2^n \cdot 3 + 2,$	$2^n \cdot 3 + 3,$	$2^n \cdot 7 - 4,$	$2^n \cdot 7 - 3,$
$2^n \cdot 7 - 2,$	$2^n \cdot 7 - 1,$	$2^n \cdot 7,$	$2^n \cdot 7 + 1,$
$2^n \cdot 7 + 2,$	$2^n \cdot 7 + 3,$	$2^n \cdot 15 - 12,$	$2^n \cdot 15 - 11,$
$2^n \cdot 15 - 6,$	$2^n \cdot 15 - 5,$	$2^n \cdot 15 - 4,$	$2^n \cdot 15 - 3$
$2^n \cdot 15,$	$2^n \cdot 15 + 1,$	$2^n \cdot 15 + 2,$	$2^n \cdot 15 + 3$

with n a non-negative integer. At this time, the smallest star graph we do not know how to obtain is the star with 36 vertices; see Examples 3.14, 3.15, and 3.24.

In addition, we show that the Artinian condition not is enough to guarantee finite clique number. In particular, in Section 5, we construct an Artinian local ring with length 6 whose graph contains an infinite clique; see Example 5.2. Our method uses the trivial extension of the ring by its dualizing module. This is facilitated by our use of a graph associated to an R-module M, called the torsion graph of M. In an effort to show that our example with infinite clique number is minimal, we show that for rings R of length at most 4, the graph $\Gamma_E(R)$ has a finite clique number; see Propositions 5.3 and 5.8. The case where R is local of length 5 is still open.

In terms of the classification of these zero divisor graphs, we investigate cut vertices, girth, and edge domination in Section 6 when R is Noetherian. In particular, we show that a cut vertex of $\Gamma_E(R)$ corresponds to an associated prime, and the girth of the graph, if finite, is 3; see Proposition 6.9 and Theorem 6.6. (If R is non-Noetherian and girth($\Gamma_E(R)$) $< \infty$, then girth($\Gamma_E(R)$) ≤ 4; see Proposition 6.1 (iii).)

In keeping with the previous research on zero divisor graphs, we also consider graph homomorphisms and colorings in Sections 4 and 7, respectively. For colorings, we are able to address a version of Beck's conjecture regarding chromatic numbers for the graph $\Gamma_E(R)$ by constructing a ring R such that $\omega(\Gamma_E(R)) = 3$, but $\chi(\Gamma_E(R)) = 4$; see Example 7.7.

2 Survey of Past Research on Zero Divisor Graphs

Because so much literature has been written on the topic of various zero divisor graphs, often from very different points of view, we collect here an overview of the material. The terms in **bold** are defined within the text, while the *italicized* terms appear in Appendix B. Throughout, and unless otherwise stated, R will be a commutative ring with unity.

2.1 Beck's Zero Divisor Graph

The idea of a zero divisor *graph* originated with I. Beck [12].

Definition 2.1 ([12]). Given a ring R, let $G(R)$ denote the graph whose vertex set is R, such that distinct vertices r and s are *adjacent* provided that $rs = 0$.

   By definition, $G(R)$ is a *simple graph*, so there are no loops; thus the existence of self-annihilating elements of R is not encoded in the graph. Moreover, because the zero vertex is adjacent to every ring element, the graph $G(R)$ is *connected* with *diameter* at most 2.

   Beck's main interest was the *chromatic number* $\chi(G(R))$ of the graph $G(R)$. He conjectured that $\chi(G(R))$ equals $\omega(G(R))$, the *clique number* of $G(R)$. The clique number is a lower bound for the chromatic number since all the vertices in a *clique* are adjacent to one another and require distinct colors. Moreover, we have the following:

Theorem 2.2 ([12, Theorems 3.9, 6.13, 7.3, Propositions 7.1, 7.2]). *Let R be a ring.*

  (i) *The following conditions are equivalent:*

    (a) $\chi(G(R))$ *is finite;*

    (b) $\omega(G(R))$ *is finite;*

    (c) *the nilradical of R is finite and is a finite intersection of prime ideals; and*

    (d) $G(R)$ *does not contain an infinite clique.*

 (ii) *Let R be such that $\chi(G(R))$ is finite. If R is a finite product of reduced rings and principal ideal rings, then $\omega(G(R)) = \chi(G(R))$.*

(iii) *If $\chi(G(R)) < \infty$, then $\chi(G(R)) = n$ if and only if $\omega(G(R)) = n$, for $n \leq 4$.*

(iv) *If $\chi(G(R)) = 5$, then $\omega(G(R)) = 5$.*

   In addition, Beck lists all the finite rings R with $\chi(G(R)) \leq 3$.

   Although this result provides evidence for Beck's conjecture, D. D. Anderson and M. Naseer [4] provided a example where the chromatic number is strictly greater than the clique number.

Example 2.3 ([4, Theorem 2.1]). If R is the factor ring of $\mathbb{Z}_4[X, Y, Z]$ determined by the ideal $(X^2 - 2, Y^2, Z^2, 2X, 2Y, 2Z, YX, XZ, YZ - 2)$, then $\chi(G(R)) = 6$ and $\omega(G(R)) = 5$.

Moreover, they extended Beck's classification of finite rings with small chromatic number to $\chi(G(R)) = 4$.

2.2 Anderson and Livingston's Zero Divisor Graph

The first simplification of Beck's zero divisor graph was introduced by D. F. Anderson and P. S. Livingston [10]. Their motivation was to give a better illustration of the zero divisor structure of the ring. In this new zero divisor graph, which is still a simple graph with edges defined the same way as above, only the **zero divisors** of the ring are included; i.e., non-zero elements r of R such that $\mathrm{Ann}_R(r) \neq (0)$.

Definition 2.4 ([10]). Given a ring R, let $Z^*(R)$ denote the set of zero divisors of R. Let $\Gamma(R)$ denote the graph whose vertex set is $Z^*(R)$, such that distinct vertices r and s are adjacent provided that $rs = 0$.

In general, we have the following, despite the absence of the zero vertex:

Theorem 2.5 ([10, Theorem 2.3]). *Given a ring R, the graph $\Gamma(R)$ is connected with diameter at most* 3.

Anderson and Livingston often focus on the case when R is finite, as these rings yield finite graphs. They determine for which rings the graph is *complete* or a *star*. For the stars, we have the following:

Theorem 2.6 ([10, Theorem 2.13]). *Given a finite ring R, if the graph $\Gamma(R)$ is a star with at least four vertices, then $|\Gamma(R)| = p^n$, for some prime p and integer $n \geq 0$. Moreover, each star graph of order p^n can be realized as $\Gamma(R)$ for some R.*

Anderson and Livingston, and others, e.g., [1, 2, 7, 29], investigate the interplay between the graph theoretic properties of $\Gamma(R)$ and the ring theoretic properties of R. For example, D. F. Anderson, A. Frazier, A. Lauve, and P. S. Livingston [7] study the clique number of $\Gamma(R)$ and the relationship between graph isomorphisms and ring isomorphisms. A particularly important and surprising result is the following:

Theorem 2.7 ([7, Theorem 4.1]). *Given finite reduced rings R and S that are not fields, the graphs $\Gamma(R)$ and $\Gamma(S)$ are graph isomorphic if and only if R and S are ring isomorphic.*

The authors [7] also determine all n for which $\Gamma(\mathbb{Z}_n)$ is *planar*, and pose the question of which finite rings in general determine a planar zero divisor graph. This was

partially answered by S. Akbari, H. R. Maimani, and S. Yassemi [1], who were able to refine the question to local rings of cardinality at most thirty-two:

Theorem 2.8 ([1, Theorems 1.2 and 1.4]). *If R is a finite local ring that is not a field and contains at least thirty-three elements, then $\Gamma(R)$ is not planar.*

However, at the same time, N. O. Smith [33], independently provided a complete answer, as well as a classification of which rings are planar, listing forty-four isomorphism classes in all.

Theorem 2.9 ([33, Theorems 3.7 and Corollary 3.8]). *If R is a finite local ring that is not a field and contains at least twenty-eight elements or ten zero divisors, then $\Gamma(R)$ is not planar.*

Some of these results were recovered by R. Belshoff and J. Chapman [13], who have also worked on questions concerning planarity, also known as genus zero. Additionally, Smith [34] studied planarity of infinite rings, as well as zero divisor graphs with genus one, also known as toroidal zero divisor graphs. In particular, H.-J. Chiang-Hsieh, N. O. Smith, and H.-J. Wang [16] consider rings with toroidal zero divisor graphs. C. Wickham [36] is another researcher who has studied zero divisor graphs of genus one. Moreover, along with N. Bloomfield, C. Wickham [14] considers graphs of genus two.

A key component to proofs concerning planarity is Kuratowski's Theorem, which says that a graph is planar if and only if it contains no subgraph homeomorphic to the complete graph K_5 or the *complete bipartite* graph $K_{3,3}$. Akbari, Maimani, and Yassemi [1] list the rings that determine a *complete r-partite* graph. In particular, they show the following:

Theorem 2.10 ([1, Theorems 2.4 and 3.2]). *Let R be a finite ring such that $\Gamma(R)$ is r-partite.*

(i) *Then r is a prime power.*

(ii) *If $r \geq 3$, then at most one partitioning subset of $\Gamma(R)$ can have more than one vertex.*

(iii) *If R is reduced, then $\Gamma(R)$ is bipartite (i.e., $r = 2$) if and only if there exist two distinct primes in R with trivial intersection.*

(iv) *If R is reduced and $\Gamma(R)$ is bipartite, then $\Gamma(R)$ is complete bipartite.*

These results are similar to those of Theorem 2.6 which describe the rings R such that $\Gamma(R)$ is a star, i.e., a complete bipartite graph of the form $K_{1,n}$.

Another graph invariant that is studied for zero divisor graphs is the *girth*. Anderson and Livingston showed that if R is Artinian and $\Gamma(R)$ contains a cycle, then the girth is no more than four, and they conjectured that this upper bound would hold in general. This conjecture was subsequently, and independently, established as fact by F. DeMeyer and K. Schneider [19] and S. B. Mulay [29].

Theorem 2.11 ([19, Theorem 1.6], [29, (1.4)]). *Given a ring R, if $\Gamma(R)$ is not acyclic, then the girth of $\Gamma(R)$ is at most* 4.

This bound on the girth is sharp, given the following:

Example 2.12 ([10, Example 2.1 (b)]). The graph $\Gamma(\mathbb{Z}_3 \times \mathbb{Z}_3)$ is a 4-cycle.

Moreover, this example shows that zero divisor graphs are not *chordal*. This jibes with the fact chordal graphs are *perfect*. Additional results concerning the girth of $\Gamma(R)$ can also be found in [1, 7].

2.3 Mulay's Zero Divisor Graph

S. B. Mulay [29] introduces the next zero divisor graph associated to a ring.

Definition 2.13 ([29]). Given a ring R, two zero divisors $r, s \in Z^*(R)$ are **equivalent** if $\text{Ann}_R(r) = \text{Ann}_R(s)$. The equivalence class of r is denoted $[r]$. The graph $\Gamma_E(R)$ has vertex set equal to the set of equivalence classes $\{[r] \mid r \in Z^*(R)\}$, and distinct classes $[r]$ and $[s]$ are adjacent in $\Gamma_E(R)$ provided that $rs = 0$ in R.

It is shown in [29] that this is well-defined, that is, that adjacency in $\Gamma_E(R)$ is independent of representatives of $[r]$ and $[s]$. By definition, the graph $\Gamma_E(R)$ is simple. Furthermore, we have the following:

Theorem 2.14 ([29]; see also [18, Theorem 1.2] and [35, Proposition 1.4]). *Given a ring R, the graph $\Gamma_E(R)$ is connected with diameter at most* 3.

In [35], S. Spiroff and C. Wickham compare and contrast $\Gamma_E(R)$ with $\Gamma(R)$. One important difference between this new graph and its two predecessors is that $\Gamma_E(R)$ can be finite even when R is infinite, thus giving a more succinct visual description of the zero divisor structure of the ring. Another difference is found in the set of graphs that can be realized as $\Gamma_E(R)$. For instance, we have the following, in contrast with the results of [1, 10]:

Theorem 2.15 ([35]). *Let R be a Noetherian ring.*

  (i) *If $\Gamma_E(R)$ is complete K_n, then $n = 2$.*

 (ii) *If $\Gamma_E(R)$ is complete bipartite $K_{n,m}$, then $n = 1$, i.e., $\Gamma_E(R)$ is a star.*

(iii) *If $\Gamma_E(R)$ has at least three vertices, then it is not a cycle, more generally, it is not regular.*

One important aspect of this graph is that, since the vertices in the graph correspond to annihilator ideals in the ring, the associated primes of R are represented in $\Gamma_E(R)$.

In order to illustrate the difference between the three zero divisor graphs discussed so far, we provide an example of each for the same ring.

Example 2.16. Let $R = \mathbb{Z}/12\mathbb{Z}$.

$G(\mathbb{Z}/12\mathbb{Z})$
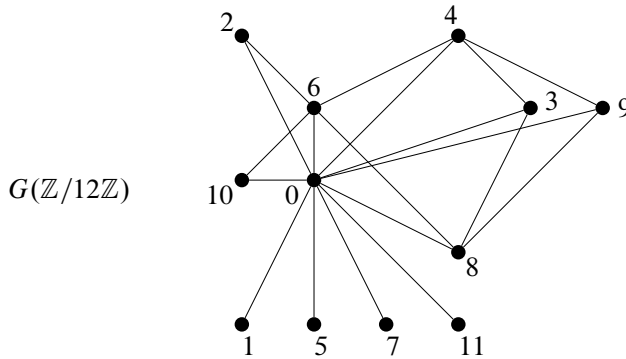
In Beck's graph above, every element of $\mathbb{Z}/12\mathbb{Z}$ is represented by a distinct vertex.

$\Gamma(\mathbb{Z}/12\mathbb{Z})$
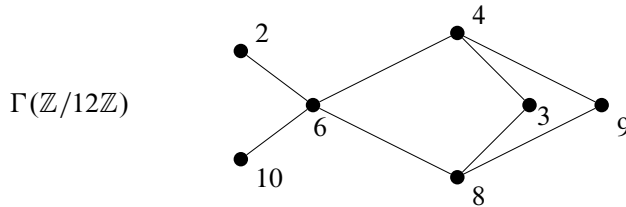
Anderson and Livingston's graph includes only the zero divisors, but each such element determines a distinct vertex.

$\Gamma_E(\mathbb{Z}/12\mathbb{Z})$

[2]   [6]   [4]   [3]
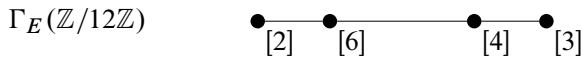
In Mulay's graph, the four distinct classes are determined by $\mathrm{Ann}_R(2) = (6)$, $\mathrm{Ann}_R(3) = (4)$, $\mathrm{Ann}_R(4) = (3)$, and $\mathrm{Ann}_R(6) = (2)$.

2.4 Other Zero Divisor Graphs

S. P. Redmond [31] introduces a zero divisor graph with respect to an ideal.

Definition 2.17 ([31]). Given a ring R and an ideal I, the graph $\Gamma_I(R)$ has vertices x from $R \backslash I$ such that $(I :_R x) \neq I$. Distinct vertices x and y are adjacent if $xy \in I$.

Of course, if $I = (0)$, then $\Gamma_I(R)$ is just $\Gamma(R)$. If I is prime, then $\Gamma_I(R) = \emptyset$. Redmond discusses the relationship between $\Gamma_I(R)$ and $\Gamma(R/I)$.

Theorem 2.18 ([31, Corollary 2.7 and Remark 2.8]). *Given a ring R and an ideal I, the graph $\Gamma_I(R)$ contains $|I|$ disjoint subgraphs isomorphic to $\Gamma(R/I)$. Moreover, if $\Gamma(R/I)$ is a graph on n vertices, then $\Gamma_I(R)$ has $n \cdot |I|$ vertices.*

In contrast with Theorem 2.7, we have the following:

Example 2.19 ([31, Remark 2.3]). Set $R = \mathbb{Z}_6 \times \mathbb{Z}_3$ and $S = \mathbb{Z}_{24}$, with ideals $I = (0) \times \mathbb{Z}_3$ and $J = (8)$, respectively. Then the graphs $\Gamma(R/I)$ and $\Gamma(S/J)$ are isomorphic, but $\Gamma_I(R)$ and $\Gamma_J(S)$ are not.

H. R. Maimani, M R. Pournaki, and S. Yassemi [27] continue the study of this new graph and take up the question of when $\Gamma_I(R) \cong \Gamma_J(S)$ might imply $\Gamma(R/I) \cong \Gamma(S/J)$. They show the following:

Theorem 2.20 ([27, Theorem 2.2]). *If I and J are finite radical ideals of the rings R and S, respectively, then $\Gamma(R/I) \cong \Gamma(S/J)$ and $|I| = |J|$ iff $\Gamma_I(R) \cong \Gamma_J(S)$.*

Further incarnations of zero divisor graphs involve objects other than commutative rings. For example, given a commutative semigroup S, expressed multiplicatively, which contains 0, F. DeMeyer, T. McKenzie, and K. Schneider [18] defined a graph in the spirit of Anderson and Livingston.

Definition 2.21 ([18]). Let S be a commutative multiplicative semigroup with 0. Denote by $\Gamma(S)$ the graph whose vertex set is the (non-zero) zero divisors of S, with an edge drawn between distinct zero divisors x and y if and only if $xy = 0$.

F. DeMeyer and L. DeMeyer [17] further this construction and give some necessary conditions for a graph G to be of the form $\Gamma(S)$. For example:

Theorem 2.22 ([17, Theorem 1]). *If G is the graph of a semigroup, then for each pair x, y of non-adjacent vertices of G, there is a vertex z with $\mathcal{N}(x) \cup \mathcal{N}(y) \subseteq \overline{\mathcal{N}(z)}$, where $\overline{\mathcal{N}(z)} = \mathcal{N}(z) \cup \{z\}$ is the* closure *of the* neighborhood $\mathcal{N}(z)$ *of z.*

In addition, they provide some classes of graphs that can be realized from semigroups, e.g., G is complete, complete bipartite, or has at least one *end* and diameter 2. See [17, Theorems 1 and 3]. They also consider a zero divisor graph more in line with Beck's original one by including 0 in the vertex set. Denote this graph by $G(S)$. In [30], S. K. Nimbhokar, M. P. Wasadikar, and L. DeMeyer study these graphs under the additional assumption that every element of S is idempotent, in which case S is called a meet-semilattice, and show that a version of Beck's conjecture regarding the chromatic number holds in this setting:

Theorem 2.23 ([30, Theorem 2 and Corollary 1]). *Let S be a commutative multiplicative semigroup with 0 such that every element of S is idempotent. If $\omega(G(S)) < \infty$, then $\chi(G(S)) = \omega(G(S))$ and $\chi(\Gamma(S)) = \omega(\Gamma(S))$.*

Zero divisor graphs associated to semigroups are also studied by L. DeMeyer, L. Greve, A. Sabbaghi, and J. Wang [21] and L. DeMeyer, M. D'Sa, I. Epstein, A. Geiser, and K. Smith [20], among others.

Remark 2.24. It is important to note that when R is a commutative ring, $\Gamma_E(R)$ is the zero divisor graph of a semigroup, namely the semigroup determined by the equivalence classes of zero divisors. Therefore, some of the results on semigroups may be applied to $\Gamma_E(R)$; e.g., connected and diameter less than or equal to three [18, Theorem 1.2]. However, not every semigroup graph can be obtained as $\Gamma_E(R)$ for some commutative ring R; e.g., if G is complete or complete bipartite but not a star graph, then it can be realized as $\Gamma(S)$ [17, Theorems 3], but not as $\Gamma_E(R)$ [35, Propositions 1.5 and 1.7].

Yet another interpretation of a zero divisor graph focuses on posets P containing 0, a concept which was introduced by R. Halaš and M. Jukl [24]. Their graph is in the spirit of Beck's original definition.

Definition 2.25 ([24]). Given a poset P containing 0, let $G(P)$ be the graph whose vertex set is P, such that distinct vertices x and y are adjacent provided that 0 is the only element lying below x and y.

Theorem 2.26 ([24, Theorem 2.9]). *Given a poset P containing 0, if $\omega(G(P))$ is finite, then $\chi(G(P)) = \omega(G(P))$.*

Subsequently, D. Lu and T. Wu [26] define a zero divisor graph for posets à la Anderson and Livingston:

Definition 2.27 ([26]). Let P be a poset containing 0. A non-zero element $x \in P$ is a **zero divisor** if there is a non-zero element $y \in P$ such that 0 is the only element lying below x and y. Let $\Gamma(P)$ be the graph whose vertex set is $Z^*(P)$, such that distinct vertices x and y are adjacent provided that 0 is the only element lying below x and y.

Of particular importance in the work in [26] is the notion of a *compact graph*. For instance, we have the following:

Theorem 2.28 ([26, Theorems 3.1 and 3.2]). *A simple graph G is the zero divisor graph of a poset if and only if G is compact. Moreover, if G is compact with $\omega(G) < \infty$, then $\omega(G) = \chi(G)$.*

In general, zero divisor graphs of rings are not compact because of the possible existence of nilpotent elements in the ring and the absence of loops in the graph. Accordingly, it can be shown that reduced rings yield compact zero divisor graphs (using any of the definitions), and hence satisfy $\omega(G) = \chi(G)$ whenever either is finite, or $\omega(G)$ is infinite. Similarly, we have the following:

Theorem 2.29 ([26, Propositions 2.2 (1) and 4.1]). *Given a commutative reduced multiplicative semigroup S with 0, the graph $\Gamma(S)$ is compact and if $\Gamma(S)$ has finite girth, then it has girth at most 4.*

Lastly, zero divisor graphs have also been defined for non-commutative rings.

Definition 2.30 ([32]). In a non-commutative ring D, a non-zero element x is a **zero divisor** if either $xy = 0$ or $yx = 0$ for some non-zero element y. Let $\Gamma(D)$ be the *directed graph* whose vertices are the zero divisors of D, with an edge $x \rightarrow y$ drawn between distinct vertices provided that $xy = 0$.

From the viewpoint that an undirected edge is a pair of directed edges, this definition reverts to that of $\Gamma(R)$ in the case of a commutative ring R. S. P. Redmond showed that connectivity in the non-commutative case depends upon whether or not the set of left and right zero-divisors coincide. S. Akbari and A. Mohammadian [3] continue the study of this directed graph, giving an example of the smallest zero divisor graph associated to a non-commutative ring, namely $\Gamma(D)$, for $D = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Z}_2 \right\}$, which has the form $E_{11} \leftarrow E_{12} \rightarrow (E_{11} + E_{12})$.

Redmond also defined an undirected graph for a non-commutative ring.

Definition 2.31 ([32]). Given a non-commutative ring D, let $\Gamma'(D)$ be the graph whose vertices are the zero divisors of D, with an edge drawn between distinct vertices x and y provided that $xy = 0$ or $yx = 0$.

For this graph, the properties of connectivity, diameter less than or equal to 3, and girth less than or equal to 4 when finite, all hold, as with earlier zero divisor graphs. Moreover, Akbari and Mohammadian show the following:

Theorem 2.32 ([3, Corollary 10]). *A finite star graph can be realized as $\Gamma'(D)$ if and only if the vertices number p^n or $2p^n - 1$, for some prime p and some integer $n \geq 0$.*

It should be noted that over 100 papers, by many authors, have been written on the topic of zero divisor graphs, and hence we only highlight a handful of results from a few papers. Our aim in the above survey is to give a flavor of the available research on zero divisor graphs, especially as it pertains to the current project, which focuses on $\Gamma_E(R)$, the zero divisor graph determined by equivalence classes. For another survey article on the topic of zero divisor graphs, see D. F. Anderson, M. C. Axtell, and J. A. Stickles [6].

3 Star Graphs

In this section, we describe some rings R such that $\Gamma_E(R)$ is a star. The constructions are not only different, but more complicated than for $\Gamma(R)$, which have a nice characterization, namely having exactly p^n vertices for p a prime and $n \geq 0$. By our methods, stars with $c < 100$ vertices can be constructed as $\Gamma_E(R)$ for the following c values: 1–35, 42–67, 90–99. At the time of this publication, we do not have a complete characterization of which stars are possible.

To motivate our constructions, note that small stars, as well as an infinite star, are constructed in [35]; see also Examples 3.28–3.30. Thus, we may assume that $\Gamma_E(R)$

has at least four vertices. When R is Noetherian, then $\mathrm{Ass}(R) = \{\mathfrak{p}\}$, with $\mathfrak{p}^3 = 0$, and the characteristic of R is either 2, 4, or 8 by [35, Proposition 2.4]. Furthermore, since localization at $\mathfrak{p}$ does not change the graph (see Corollary 4.3), we may take R to be Artinian and local with maximal ideal $\mathfrak{m} = \mathfrak{p}$.

For simplicity, we focus on the case where R is finite of characteristic 2. Also, we take all zero divisors of R to be square-zero, since at most one class of zero divisor can fail to have this property. To aid in computations, we focus on the case where R is a standard graded algebra over $\mathbb{F}_2$ with irrelevant maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^3 = 0$. This implies that the socle of R contains the graded ideal $R_2 = \mathfrak{m}^2$. Thus, the only non-trivial zero divisors are in R_1, that is, they are linear forms in the generators of $\mathfrak{m}$. Furthermore, we have $R \cong \mathbb{F}_2 \oplus R_1 \oplus R_2$.

We begin with a construction $R^\flat$ that yields stars with even numbers of vertices. The distinct annihilator ideals of $R^\flat$ are described in Proposition 3.11. The structure of $\Gamma_E(R^\flat)$ is given in Theorems 3.12 and 3.13, and some specific star graphs are described in Examples 3.14–3.15. In addition, at the end of the section we detail some examples (3.28–3.30) that are relevant to our study in Section 5 of clique numbers of "small" rings.

Construction 3.1. Let R be a $\mathbb{Z}$-graded ring $R = \mathbb{F}_2 \oplus R_1 \oplus R_2$ generated over $\mathbb{F}_2$ by R_1 such that $r^2 = 0$ for all $r \in R_1$. Set $d = \dim_{\mathbb{F}_2}(R_1)$, and choose a basis $X_1, \ldots, X_d$ for R_1 over $\mathbb{F}_2$. Assume that $d \geq 1$, and fix integers e, t such that $e \geq 1$ and $1 \leq t \leq \min(d, e)$. Let $\mathbf{Y} = Y_1, \ldots, Y_e$ be a sequence of indeterminates, and set

$$R' = R[\mathbf{Y}]/(R_2 \, \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) + (\mathbf{Y})^2)$$

$$R^\flat = R[\mathbf{Y}]/(R_2 \, \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) + (\mathbf{Y})^2 + (X_i X_j + X_i Y_j + X_j Y_i \mid 1 \leq i < j \leq t))$$

$$\cong R'/(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \leq i < j \leq t).$$

Remark 3.2. Under the assumptions and notation of Construction 3.1, the ring R is local with maximal ideal $\mathfrak{m} = R_+ = 0 \oplus R_1 \oplus R_2$ because the ideal $\mathfrak{m}$ is maximal and $\mathfrak{m}^3 = 0$. The ring R' is the special case of $R^\flat$ where $t = 1$. The polynomial ring $R[\mathbf{Y}]$ is $\mathbb{Z}^2$-graded where $R[\mathbf{Y}]_{(i,j)}$ consists of all the homogeneous forms in $R[\mathbf{Y}]$ of degree j with coefficients in R_i. For instance, this provides

$$R_i \, \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) = R[\mathbf{Y}]_{(i,1)} \cong \bigoplus_{k=1}^{e} R_i Y_k.$$

The next example shows how to build rings R that satisfy the assumptions of Construction 3.1.

Example 3.3. Fix an integer $d \geq 1$, and let $\mathbf{X} = X_1, \ldots, X_d$ be indeterminates.

(i) First, we consider the ring $R = \mathbb{F}_2[\mathbf{X}]/(\mathbf{X})^2$. Since the ideal $(\mathbf{X})^2$ is homogeneous, the quotient ring R is graded as follows:

$$R = \mathbb{F}_2 \oplus \mathrm{Span}_{\mathbb{F}_2}(\mathbf{X}).$$

It follows that $R_2 = 0$, so $r^2 = 0$ for all $r \in R_+ = 0 \oplus R_1$. We conclude that $\text{Soc}(R) = R_1$, and $\Gamma_E(R)$ is a single vertex $[X_1]$.

(ii) Next, we consider the ring

$$R = \mathbb{F}_2[\mathbf{X}]/((X_1^2, \ldots, X_d^2) + (\mathbf{X})^3).$$

Since the ideal $(X_1^2, \ldots, X_d^2) + (\mathbf{X})^3$ is homogeneous, the quotient ring R is graded as follows:

$$R = \mathbb{F}_2 \oplus \text{Span}_{\mathbb{F}_2}(\mathbf{X}) \oplus \text{Span}_{\mathbb{F}_2}(\{X_i X_j \mid i \neq j\}).$$

Since $X_i^2 = 0$ in R for all i, it follows that $r^2 = 0$ for all $r \in R_+ = 0 \oplus R_1 \oplus R_2$.

If $d = 1$, then R is the same as the ring constructed in part (i), so $\Gamma_E(R)$ is a single vertex $[X_1]$. Assume then that $d \geq 2$. In this event, $\Gamma_E(R)$ is a star with 2^d vertices. Specifically, the zero divisors of R are the non-zero elements of R_+, and for each $l \in R_1$ and $f \in R_2$ with $l, f \neq 0$, one has

$$\text{Ann}_R(f) = R_+ = R_1 \oplus R_2$$

$$\text{Ann}_R(l) = \text{Ann}_R(l + f) = 0 \oplus \text{Span}_{\mathbb{F}_2}(l) \oplus R_2.$$

(Argue as in the proofs of Propositions 3.8 and 3.11.) Thus, $\Gamma_E(R)$ is a star with central vertex $[f]$ and with edges $[f]-[l_1], \ldots, [f]-[l_{2^d-1}]$ where $l_1, \ldots, l_{2^d-1}$ are the distinct non-zero elements of R_1.

Proposition 3.4. *Continue with the assumptions and notation of Construction* 3.1.

(i) *The ring R' is $\mathbb{Z}^2$-graded with*

$$R' = R'_{(0,0)} \oplus [R'_{(1,0)} \oplus R'_{(0,1)}] \oplus [R'_{(2,0)} \oplus R'_{(1,1)}]$$

$$\cong \mathbb{F}_2 \oplus [R_1 \oplus \text{Span}_{\mathbb{F}_2}(\mathbf{Y})] \oplus [R_2 \oplus R_1 \text{Span}_{\mathbb{F}_2}(\mathbf{Y})].$$

(ii) *The ring R' is local with maximal ideal*

$$\mathfrak{m}' = R'_+ = 0 \oplus [R'_{(1,0)} \oplus R'_{(0,1)}] \oplus [R'_{(2,0)} \oplus R'_{(1,1)}].$$

(iii) *For each non-unit $f \in R'$, we have $f^2 = 0$.*

Proof. (i) Following Remark 3.2, we have $R_2 \text{Span}_{\mathbb{F}_2}(\mathbf{Y}) = R[\mathbf{Y}]_{(2,1)}$, and the ideal $(\mathbf{Y})^2$ is generated by $R[\mathbf{Y}]_{(0,2)}$. It follows that the ideal $I = (R_2 \text{Span}_{\mathbb{F}_2}(\mathbf{Y}) + (\mathbf{Y})^2) \subseteq R[\mathbf{Y}]$ is $\mathbb{Z}^2$-graded, generated by $R[\mathbf{Y}]_{(2,1)} + R[\mathbf{Y}]_{(0,2)}$. In other words, I is the direct sum of $R[\mathbf{Y}]_{(i,j)}$ taken over the set of all ordered pairs (i, j) such that either $(j \geq 2)$ or $(i \geq 2$ and $j \geq 1)$. Since $R_i = 0$ for all $i \geq 3$, the only bi-graded pieces of $R[\mathbf{Y}]$ that survive in the quotient R' are the following

$$R'_{(0,0)} = R[\mathbf{Y}]_{(0,0)} = \mathbb{F}_2, \quad R'_{(0,1)} = R[\mathbf{Y}]_{(0,1)} = \text{Span}_{\mathbb{F}_2}(\mathbf{Y}),$$

$$R'_{(1,0)} = R[\mathbf{Y}]_{(1,0)} = R_1, \quad R'_{(1,1)} = R[\mathbf{Y}]_{(1,1)} = R_1 \text{Span}_{\mathbb{F}_2}(\mathbf{Y}),$$

$$R'_{(2,0)} = R[\mathbf{Y}]_{(2,0)} = R_2.$$

(ii) Since $R'_{(1,0)} = R_1$ and $R'_{(0,1)} = \text{Span}_{\mathbb{F}_2}(\mathbf{Y})$ consist of square-zero elements, the ideal $\mathfrak{m}$ they generate is nilpotent. Since $\mathfrak{m}$ is maximal, it is therefore the unique maximal ideal.

(iii) Every non-unit $f \in R'$ is of the form $f_1 + \sum_j g_j Y_j$ where f_1 is a non-unit of R and $g_j \in R$. Since we are working over $\mathbb{F}_2$, the assumption $f_1^2 = 0$ implies that $f^2 = f_1^2 + \sum_j g_j^2 Y_j^2 = 0 + \sum_j g_j^2 0 = 0.$ □

We will often make use of the $\mathbb{Z}^2$-graded structure of R' from Proposition 3.4 (i). Sometimes, though, we only need to know that R' is $\mathbb{Z}$-graded, where we use the standard induced $\mathbb{Z}$-grading:

$$R'_i = \bigoplus_{p+q=i} R_{(p,q)},$$
$$R'_0 \cong \mathbb{F}_2 \oplus 0 \oplus 0,$$
$$R'_1 \cong 0 \oplus [R_1 \oplus \text{Span}_{\mathbb{F}_2}(\mathbf{Y})] \oplus 0,$$
$$R'_2 \cong 0 \oplus 0 \oplus [R_2 \oplus R_1 \text{Span}_{\mathbb{F}_2}(\mathbf{Y})],$$
$$R'_i = 0 \quad \text{for all } i \geq 3.$$

Proposition 3.5. *Continue with the assumptions and notation of Construction* 3.1.

(i) *The ring $R^\flat$ is $\mathbb{Z}$-graded with*

$$R^\flat = R_0^\flat \oplus R_1^\flat \oplus R_2^\flat$$
$$\cong \mathbb{F}_2 \oplus [R_1 \oplus \text{Span}_{\mathbb{F}_2}(\mathbf{Y})]$$
$$\oplus \left[\frac{R_2 \oplus R_1 \text{Span}_{\mathbb{F}_2}(\mathbf{Y})}{\text{Span}_{\mathbb{F}_2}(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \leq i < j \leq t)} \right].$$

(ii) *The ring $R^\flat$ is local with maximal ideal*

$$\mathfrak{m}^\flat = R_+^\flat = 0 \oplus R_1^\flat \oplus R_2^\flat.$$

(iii) *For each non-unit $f \in R^\flat$, we have $f^2 = 0$.*

(iv) *For $1 \leq i \leq j \leq t$, we have $(X_i + Y_i)(X_j + Y_j) = 0$ in $R^\flat$.*

(v) $\dim_{\mathbb{F}_2}(R_1^\flat) = d + e$.

Proof. (i) The elements $X_i X_j + X_i Y_j + X_j Y_i \in R'$ are $\mathbb{Z}$-homogeneous of degree 2, so the quotient

$$R^\flat \cong R'/(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \leq i < j \leq t)$$

is $\mathbb{Z}$ graded with $\deg(X_i) = 1 = \deg(Y_j)$. The ring R' only has non-zero summands in degrees 0, 1, and 2. Since the elements $X_i X_j + X_i Y_j + X_j Y_i$ have degree 2,

the summands R'_p and $R^\flat_p$ are isomorphic (for $p = 0, 1$) via the natural surjection $R' \to R^\flat$. Since R'_2 is in $\mathrm{Soc}(R')$, the ideal generated by the $X_i X_j + X_i Y_j + X_j Y_i$ is just $\mathrm{Span}_{\mathbb{F}_2}(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \le i < j \le t)$. Hence, the desired descriptions of $R^\flat$ follow from Proposition 3.4 (i).

(ii) Since R' is local and $\mathrm{Span}_{\mathbb{F}_2}(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \le i < j \le t) \subseteq \mathfrak{m}'$, it follows that $R^\flat$ is local with maximal ideal

$$\mathfrak{m}^\flat = \mathfrak{m}' / \mathrm{Span}_{\mathbb{F}_2}(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \le i < j \le t).$$

(iii) Since every non-unit in R' is square-zero, the same is true of the homomorphic image $R^\flat$.

(iv) When $i = j$, this follows from part (iii). When $i < j$, we have

$$(X_i + Y_i)(X_j + Y_j) = X_i X_j + X_i Y_j + X_j Y_i + Y_i Y_j = X_i X_j + X_i Y_j + X_j Y_i = 0$$

in $R^\flat$ because $Y_i Y_j = 0 = X_i X_j + X_i Y_j + X_j Y_i$ by construction.

(v) This follows from the description of $R^\flat_1$ in part (i). □

Lemma 3.6. *Continue with the assumptions and notation of Construction* 3.1. *In* $R[\mathbf{Y}]$, *let* $l \in R_1$ *and* $m \in \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})$ *such that* $lm \in \mathrm{Span}_{\mathbb{F}_2}(X_i Y_j + X_j Y_i \mid 1 \le i < j \le t)$. *Then* $l = 0$ *or* $m = 0$.

Proof. Consider the polynomial ring $S = \mathbb{F}_2[\mathbf{X}]$ with the natural $\mathbb{Z}$-graded surjection $\tau : S \to R$. Note that τ_i is an isomorphism for $i = 0, 1$. It follows that the induced $\mathbb{Z}^2$-graded surjection $\tau[\mathbf{Y}] : S[\mathbf{Y}] \to R[\mathbf{Y}]$ is an isomorphism for multi-degrees (i, j) with $i \le 1$. (Here $\deg(X_i) = (1, 0)$ and $\deg(Y_j) = (0, 1)$.) Thus, the condition $lm \in \mathrm{Span}_{\mathbb{F}_2}(X_i Y_j + X_j Y_i \mid 1 \le i < j \le t)$ in $R[\mathbf{Y}]_{(1,1)} \cong S[\mathbf{Y}]_{(1,1)}$ implies that there are elements $\gamma_{i,j} \in \mathbb{F}_2$ such that $lm = \sum_{1 \le i < j \le t} \gamma_{i,j}(X_i Y_j + X_j Y_i)$ in $S[\mathbf{Y}]$. It follows that

$$lm \in I = I_2 \begin{pmatrix} X_1 & \cdots & X_t \\ Y_1 & \cdots & Y_t \end{pmatrix} \subseteq S[\mathbf{Y}]$$

where I is the ideal of $S[\mathbf{Y}]$ generated by the size-2 minors of the matrix of variables. Since I is generated by elements of degree $(1, 1)$, we have $I \cap S[\mathbf{Y}]_{(1,0)} = 0$ and $I \cap S[\mathbf{Y}]_{(0,1)} = 0$.

From [15, Theorem 2.10] we know that the ideal I' in $\mathbb{F}_2[X_1, \dots, X_t, Y_1, \dots, Y_t]$ generated by the size-2 minors of the matrix of variables is prime. It follows that the ideal $I = I'S[\mathbf{Y}]$ is prime in $S[\mathbf{Y}]$. Hence, either $l \in I \cap S[\mathbf{Y}]_{(1,0)} = 0$ or $m \in I \cap S[\mathbf{Y}]_{(0,1)} = 0$, as desired. □

Remark 3.7. Set $H = \mathrm{Span}_{\mathbb{F}_2}(X_i + Y_i \mid 1 \le i \le t) \subseteq R^\flat_1 = R'_1 = R[\mathbf{Y}]_1$. Given an element $f = \sum_{i=1}^d a_i X_i + \sum_{j=1}^e b_j Y_j \in R^\flat_1$, it is straightforward to show that $f \in H$ if and only if the following conditions are satisfied:

(i) $a_i = 0 = b_j$ for all i, $j > t$; and

(ii) $a_i = b_i$ for all $i \leq t$.

Furthermore, in the case $t = 1$, we have $H = 0$.

Proposition 3.8. *Continue with the assumptions and notation of Construction* 3.1 *and Remark* 3.7.

(i) *For all $l \in R_1 \setminus \{0\}$ and $m \in \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) \setminus \{0\}$, we have $lm \neq 0$ in $R^{\flat}$.*

(ii) $\mathrm{Soc}(R^{\flat}) = R_2^{\flat}$.

(iii) $\left| [R_1 \oplus \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})] \setminus [R_1 \cup \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) \cup H] \right| = 2^{d+e} - 2^d - 2^e - 2^t + 2$.

Proof. (i) Suppose by way of contradiction that $lm = 0$ in $R^{\flat}$. In the polynomial ring $R[\mathbf{Y}]$ we have $lm \in R[\mathbf{Y}]_{(1,1)}$. From the relations used to create $R^{\flat}$, it follows that

$$lm \in \mathrm{Span}_{\mathbb{F}_2}(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \leq i < j \leq t) \subseteq R[\mathbf{Y}].$$

It follows that there are elements $\gamma_{i,j} \in \mathbb{F}_2$ such that

$$lm = \sum_{1 \leq i < j \leq t} \gamma_{i,j}(X_i X_j + X_i Y_j + X_j Y_i)$$

$$= \sum_{1 \leq i < j \leq t} \gamma_{i,j} X_i X_j + \sum_{1 \leq i < j \leq t} \gamma_{i,j}(X_i Y_j + X_j Y_i)$$

in $R[\mathbf{Y}]$. The elements lm and $\sum_{1 \leq i < j \leq t} \gamma_{i,j}(X_i Y_j + X_j Y_i)$ are in $R[\mathbf{Y}]_{(1,1)}$, and the element $\sum_{1 \leq i < j \leq t} \gamma_{i,j} X_i X_j$ is in $R[\mathbf{Y}]_{(2,0)}$. It follows that $\sum_{1 \leq i < j \leq t} \gamma_{i,j} X_i X_j = 0$, and hence

$$lm = \sum_{1 \leq i < j \leq t} \gamma_{i,j}(X_i Y_j + X_j Y_i) \in \mathrm{Span}_{\mathbb{F}_2}(X_i Y_j + X_j Y_i \mid 1 \leq i < j \leq t) \subseteq R[\mathbf{Y}]$$

so Lemma 3.6 implies that $l = 0$ or $m = 0$, a contradiction.

(ii) Since $R_i^{\flat} = 0$ for all $i \geq 3$, the containment $\mathrm{Soc}(R^{\flat}) \supseteq R_2^{\flat}$ is routine. For the reverse containment $\mathrm{Soc}(R^{\flat}) \subseteq R_2^{\flat}$, we use the fact that the socle of $R^{\flat}$ is a $\mathbb{Z}$-graded ideal; this follows from the fact that $R^{\flat}$ is $\mathbb{Z}$-graded. Since $R_0^{\flat}$ consists of units, it suffices to show that the only elements of degree 1 in $\mathrm{Soc}(R^{\flat})$ are 0.

Let $f \in \mathrm{Soc}(R^{\flat})_1 \subseteq R_1^{\flat} = R_1 \oplus \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})$, and fix $l \in R_1$ and $m \in \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})$ such that $f = l + m$. The assumption $f \in \mathrm{Soc}(R^{\flat})$ implies that

$$0 = f Y_1 = l Y_1 + m Y_1 = l Y_1$$

since $(\mathbf{Y})^2 = 0$ in $R^\flat$. Thus, part (i) implies that $l = 0$. Thus, we have $f = m$, and it follows that

$$0 = X_1 f = X_1 m$$

so part (i) implies that $f = m = 0$, as desired.

(iii) Since R_1, $\mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})$, and H have pair-wise trivial intersection, the number of elements of $[R_1 \oplus \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})] \setminus [R_1 \cup \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) \cup H]$ is given by the formula $2^{d+e} - 2^d - (2^e - 1) - (2^t - 1)$. $\qquad\square$

Notation 3.9. Set $v = 2^{d+e} - 2^d - 2^e - 2^t + 2$. Write

$$[R_1 \oplus \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})] \setminus [R_1 \cup \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) \cup H] = \{f_1, \ldots, f_v\}$$

and let $0 \neq z \in \mathrm{Soc}(R)$.

Lemma 3.10. *Continue with the assumptions and notation of Construction* 3.1, *Remark* 3.7, *and Notation* 3.9. *Let* $l, p \in R_1$ *and* $m, q \in \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})$ *such that* $l, m \neq 0$. *Set* $f = l + m$ *and* $g = p + q$, *and assume that* $fg = 0$ *in* $R^\flat$.

(i) *If* $f \in H$, *then* $g \in H$.

(ii) *If* $f \notin H$, *then either* $g = 0$ *or* $g = f$.

Proof. If $p = 0 = q$, then $g = 0$ and we are done. Thus, we assume that either $p \neq 0$ or $q \neq 0$.

Suppose that $p = 0$ and $q \neq 0$. If follows that $g = q \in \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) \setminus \{0\}$. Since $l, m \neq 0$, we have $f = l + m \notin \mathrm{Ann}_{R^\flat}(q) = \mathrm{Ann}_{R^\flat}(g)$, contradicting the assumption $fg = 0$.

If $p \neq 0$ and $q = 0$, then we arrive at a similar contradiction. Thus, we assume for the rest of the proof that $p, q \neq 0$.

In $R^\flat$, we have

$$0 = fg = lp + lq + mp + mq = lp + lq + mp$$

since $(\mathbf{Y})^2 = 0$. It follows that

$$lp + lq + mp \in \mathrm{Span}_{\mathbb{F}_2}(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \leq i < j \leq t) \subseteq R[\mathbf{Y}].$$

It follows that there are elements $\gamma_{i,j} \in \mathbb{F}_2$ such that

$$lp + lq + mp = \sum_{1 \leq i < j \leq t} \gamma_{i,j}(X_i X_j + X_i Y_j + X_j Y_i) \qquad (3.10.1)$$

in $R[\mathbf{Y}]$. Fix elements $a_i, \alpha_i, b_j, \beta_j \in \mathbb{F}_2$ such that

$$l = \sum_{i=1}^{d} \alpha_i X_i, \quad p = \sum_{i=1}^{d} a_i X_i, \quad m = \sum_{j=1}^{e} \beta_j Y_j, \quad q = \sum_{j=1}^{e} b_j Y_j.$$

Substituting these expressions into (3.10.1) and collecting homogeneous components, we obtain the following:

$$\sum_{i=1}^{d}\sum_{j=1}^{d}\alpha_i a_j X_i X_j = \sum_{1\leq i<j\leq t}\gamma_{i,j}X_i X_j, \tag{3.10.2}$$

$$\sum_{i=1}^{d}\sum_{j=1}^{e}(\alpha_i b_j + a_i\beta_j)X_i Y_j = \sum_{1\leq i<j\leq t}\gamma_{i,j}(X_i Y_j + X_j Y_i). \tag{3.10.3}$$

The set $\{X_i Y_j \mid 1 \leq i \leq d, 1 \leq j \leq e\}$ is linearly independent over $\mathbb{F}_2$ since the X_i's are linearly independent. Thus, equation (3.10.3) yields the following system of equations in $\mathbb{F}_2$:

$$\alpha_i b_j + a_i\beta_j = \begin{cases}\gamma_{i,j} = \alpha_j b_i + a_j\beta_i & \text{for } 1 \leq i < j \leq t, \\ 0 & \text{otherwise.}\end{cases} \tag{3.10.4}$$

The assumption $l, m \neq 0$ implies that there are indices i_0, j_0 such that $\alpha_{i_0} = 1 = \beta_{j_0}$. Assume that i_0 and j_0 are the largest such indices.

Case 1: $i_0 > t$. (This is a special case of the case $f \notin H$.) In this case, equation (3.10.4) implies that $b_j = a_{i_0}\beta_j$ for $j = 1,\ldots,e$. It follows that $q = a_{i_0}m$, and thus $g = p + a_{i_0}m$. Consider the element

$$g + a_{i_0}f = p + a_{i_0}l \in R_1.$$

Since $fg = 0 = a_{i_0}f^2$, we have $f(g + a_{i_0}f) = 0$. Since $f \neq 0$, Proposition 3.11 (i) implies that $g + a_{i_0}f = 0$, that is, that $g = a_{i_0}f$. Since $a_{i_0} \in \mathbb{F}_2$ and $g \neq 0$, it follows that $g = f$, as desired.

Case 2: $j_0 \geq t$. (This is another special case of the case $f \notin H$.) As in Case 1, it follows that $g = f$, as desired.

Case 3: For all $i, j > t$ we have $\alpha_i = 0 = \beta_j$, and $f \in H$. If there is an index $i_1 > t$ such that $a_{i_1} = 1$, then we conclude that $f = g$ as in Case 1. Thus, we assume that $a_i = 0$ for all $i > t$ and, similarly, that $b_j = 0$ for all $j > t$.

Case 3A: $f \in H$. The condition $f \in H$ implies that $\beta_i = \alpha_i$ for $i = 1,\ldots,t$; see Remark 3.7. To show that $g \in H$, we need to show that $b_i = a_i$ for $i = 1,\ldots,t$. For each i, equation (3.10.4) implies that

$$\alpha_i b_i = a_i\beta_i = a_i\alpha_i.$$

If $\alpha_i = 1$, then it follows that $b_i = a_i$, as desired. Assume that $\alpha_i = 0$. It follows that $\beta_i = \alpha_i = 0$ and $\beta_{i_0} = \alpha_{i_0} = 1$, so equation (3.10.4) implies that

$$a_i = \alpha_i b_{i_0} + a_i\beta_{i_0} = \alpha_{i_0}b_i + a_{i_0}\beta_i = b_i$$

as desired.

Case 3B: $f \notin H$. It follows that there is an index $i_2 \leq t$ such that $\alpha_{i_2} \neq \beta_{i_2}$.

Case 3Bi: $\alpha_{i_2} = 1$ and $\beta_{i_2} = 0$. Equation (3.10.4) with $j = i_2$ yields

$$b_{i_2} = \alpha_{i_2} b_{i_2} = a_{i_2} \beta_{i_2} = 0.$$

For $j \neq i_2$, equation (3.10.4) implies that

$$b_j + a_{i_2} \beta_j = \alpha_{i_2} b_j + a_{i_2} \beta_j = 0.$$

Combining these displays, we find that $b_j = a_{i_2} \beta_j$ for $j = i, \ldots, t$. It follows that $q = a_{i_2} m$, and we deduce that $g = f$ as in Case 1.

Case 3Bii: $\alpha_{i_2} = 0$ and $\beta_{i_2} = 1$. Argue as in Case 3Bi to conclude that $g = f$.   □

Proposition 3.11. *Continue with the assumptions and notation of Construction* 3.1, *Remark* 3.7, *and Notation* 3.9. *For all* $l \in R_1 \setminus 0$ *and* $m \in \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) \setminus 0$, *we have*

(i) $\mathrm{Ann}_{R^\flat}(l) = 0 \oplus [\mathrm{Ann}_R(l)_1 \oplus 0] \oplus R_2^\flat$

(ii) $\mathrm{Ann}_{R^\flat}(m) = 0 \oplus [0 \oplus \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})] \oplus R_2^\flat$

(iii) $\mathrm{Ann}_{R^\flat}(l + m) = \begin{cases} 0 \oplus [\mathrm{Span}_{\mathbb{F}_2}(l+m)] \oplus R_2^\flat & \text{if } l + m \notin H, \\ 0 \oplus H \oplus R_2^\flat & \text{if } l + m \in H. \end{cases}$

Proof. (i) Since l is homogeneous of degree 1, the ideal $\mathrm{Ann}_{R^\flat}(l)$ is also $\mathbb{Z}$-graded. Thus, we need only check the equality $\mathrm{Ann}_{R^\flat}(l) = 0 \oplus [\mathrm{Ann}_R(l) \oplus 0] \oplus R_2^\flat$ for graded pieces. Since $R_0^\flat$ consists of units of $R^\flat$, the assumption $l \neq 0$ implies that $\mathrm{Ann}_{R^\flat}(l)_0 = 0$. Since $\mathrm{Soc}(R^\flat) = R_2^\flat$, it is straightforward to show that $\mathrm{Ann}_{R^\flat}(l)_2 = R_2^\flat$. In degree 1, the containment $\mathrm{Ann}_{R^\flat}(l)_1 \supseteq \mathrm{Ann}_R(l)_1$ is straightforward. For the reverse containment $\mathrm{Ann}_{R^\flat}(l)_1 \subseteq \mathrm{Ann}_R(l)_1$, let

$$f \in \mathrm{Ann}_{R^\flat}(l)_1 \subseteq R_1^\flat = R_1 \oplus \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})$$

and fix $p \in R_1$ and $q \in \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})$ such that $f = p + q$.

In the polynomial ring $R[\mathbf{Y}]$ we have $lf \in R[\mathbf{Y}]_{(2,0)} \oplus R[\mathbf{Y}]_{(1,1)}$. In light of the relations used to create $R^\flat$, it follows that

$$lf \in \mathrm{Span}_{\mathbb{F}_2}(X_i X_j + X_i Y_j + X_j Y_i \mid 1 \leq i < j \leq t) \subseteq R[\mathbf{Y}].$$

It follows that there are elements $\gamma_{i,j} \in \mathbb{F}_2$ such that

$$lf = \sum_{1 \leq i < j \leq t} \gamma_{i,j} (X_i X_j + X_i Y_j + X_j Y_i),$$

$$lp + lq = \sum_{1 \leq i < j \leq t} \gamma_{i,j} X_i X_j + \sum_{1 \leq i < j \leq t} \gamma_{i,j} (X_i Y_j + X_j Y_i)$$

in $R[\mathbf{Y}]$. The elements lp and $\sum_{1 \le i < j \le t} \gamma_{i,j} X_i X_j$ are in $R[\mathbf{Y}]_{(2,0)}$ and the elements lq and $\sum_{1 \le i < j \le t} \gamma_{i,j}(X_i Y_j + X_j Y_i)$ are in $R[\mathbf{Y}]_{(1,1)}$. It follows that

$$lp = \sum_{1 \le i < j \le t} \gamma_{i,j} X_i X_j, \tag{3.11.1}$$

$$lq = \sum_{1 \le i < j \le t} \gamma_{i,j}(X_i Y_j + X_j Y_i) \tag{3.11.2}$$

Since $l \ne 0$, equation (3.11.2) implies that $q = 0$ by Lemma 3.6. Thus, we have $f = p \in R_1 \cap \operatorname{Ann}_{R^\flat}(l) = \operatorname{Ann}_R(l)_1$, as desired.

(ii) Again, it suffices to show that $\operatorname{Ann}_{R^\flat}(m)_1 \subseteq \operatorname{Span}_{\mathbb{F}_2}(\mathbf{Y})$. Let $p \in R_1$ and $q \in \operatorname{Span}_{\mathbb{F}_2}(\mathbf{Y})$ such that $f = p + q \in \operatorname{Ann}_{R^\flat}(m)$. Since $(\mathbf{Y})^2 = 0$ in $R^\flat$, we have

$$0 = fm = pm + qm = pm$$

so Lemma 3.6 implies that $p = 0$. It follows that $f = q \in \operatorname{Span}_{\mathbb{F}_2}(\mathbf{Y})$, as desired.

(iii) Since $\operatorname{Ann}_{R^\flat}(l + m)$ is a $\mathbb{Z}$-graded ideal, it suffices to verify the equalities degree-by-degree. The degree 0 and degree 2 parts are straightforward since $l+m \ne 0$ and $\operatorname{Soc}(R^\flat) = R_2^\flat$. Since $H^2 = 0 = (l+h)^2$ by Proposition 3.5 (iii), (iv), the degree 1 parts follow from Lemma 3.10. $\qquad\square$

Theorem 3.12. *Continue with the assumptions and notation of Construction* 3.1, *Remark* 3.7, *and Notation* 3.9. *Assume that* $\operatorname{Soc}(R) = R_2$.

(i) *The number of distinct vertices in* $\Gamma_E(R^\flat)$ *is* $c^\flat = c + v + 2$.

(ii) $\Gamma_E(R^\flat)$ *is formed from* $\Gamma_E(R)$ *by adding* $v+2$ *vertices* $[f_1], \ldots, [f_v], [X_1 + Y_1]$, $[Y_1]$, *and* $v + 2$ *edges* $[z] - [Y_1], [z] - [f_1], \ldots, [z] - [f_v], [z] - [X_1 + Y_1]$.

(iii) $\Gamma_E(R^\flat)$ *is a star if and only if* $\Gamma_E(R)$ *is a star.*

Proof. (i) Proposition 3.8 (ii) says that $\operatorname{Soc}(R^\flat) = R_2^\flat$. As $z \in \operatorname{Soc}(R) = R_2 \subseteq R_2^\flat = \operatorname{Soc}(R^\flat)$, it follows that the vertex set of $\Gamma_E(R^\flat)$ consists of the socle vertex $[z]$ and the vertices $[u]$ where u ranges through the elements of $R_1^\flat$ with distinct annihilators.

The non-zero elements of $R_1^\flat$ are of the form l, m, and $l + m$ where $l \in R_1 \setminus 0$ and $m \in \operatorname{Span}_{\mathbb{F}_2}(\mathbf{Y}) \setminus 0$; see Proposition 3.5 (i). Using Proposition 3.11, we see that:

(i) the vertices $[l]$, $[m]$, and $[l + m]$ are all distinct in $\Gamma_E(R^\flat)$ since the annihilator ideals are all different;

(ii) given another element $l' \in R_1 \setminus 0$, we have $\operatorname{Ann}_{R^\flat}(l) = \operatorname{Ann}_{R^\flat}(l')$ if and only if $\operatorname{Ann}_R(l) = \operatorname{Ann}_R(l')$, so $[l] = [l']$ in $\Gamma_E(R^\flat)$ if and only if $[l] = [l']$ in $\Gamma_E(R)$;

(iii) given another element $m' \in \operatorname{Span}_{\mathbb{F}_2}(\mathbf{Y}) \setminus 0$, we have $\operatorname{Ann}_{R^\flat}(m) = \operatorname{Ann}_{R^\flat}(m')$, so $[m] = [m']$ in $\Gamma_E(R^\flat)$;

(iv) If $l+m \notin H$, then $\operatorname{Ann}_{R^\flat}(l+m) = \operatorname{Ann}_{R^\flat}(l'+m')$ if and only if $l+m = l'+m'$, so $[l + m] = [l' + m']$ in $\Gamma_E(R^\flat)$ if and only if $l + m = l' + m'$; and

(v) If $l + m \in H$, then $\mathrm{Ann}_{R^\flat}(l + m) = \mathrm{Ann}_{R^\flat}(l' + m')$ if and only if $l' + m' \in H \setminus \{0\}$.

Thus, the distinct vertices of $\Gamma_E(R^\flat)$ are the following:

(i') $[z]$;

(ii') $[l]$ where l ranges through the distinct vertices $[l] \neq [z]$ of $\Gamma_E(R)$;

(iii') $[Y_1]$;

(iv') $[l + m]$ where l and m range through $R_1 \setminus 0$ and $\mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) \setminus 0$, respectively, with $l + m \notin H$; and

(v') $[X_1 + Y_1]$

accounting for all the elements of H. In particular, the number of vertices in $\Gamma_E(R^\flat)$ is

$$c^\flat = 1 + (c - 1) + 1 + \left| [R_1 \oplus \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y})] \setminus [R_1 \cup \mathrm{Span}_{\mathbb{F}_2}(\mathbf{Y}) \cup H] \right| + 1$$
$$= c + 2 + 2^{d+e} - 2^d - 2^e - 2^t + 2$$
$$= c + v + 2$$

by Proposition 3.8 (iii).

(ii) Using the fact that $z \in \mathrm{Soc}(R^\flat)$ with Proposition 3.11, we see the following:

(i'') the vertices $[z]$ and $[f]$ are adjacent in $\Gamma_E(R^\flat)$ for every $0 \neq f \in R_1^\flat$;

(ii'') given $l, l' \in R_1 \setminus 0$, the vertices $[l]$ and $[l']$ are adjacent in $\Gamma_E(R^\flat)$ if and only if they are adjacent in $\Gamma_E(R)$; and

(iii'') the vertices $[Y_1]$, $[l + m]$, and $[X_1 + Y_1]$ are only adjacent to $[z]$ in $\Gamma_E(R^\flat)$.

Thus, the graph $\Gamma_E(R^\flat)$ has the desired form.

(iii) This follows from part (ii). □

Next, we deal with the case where $\mathrm{Soc}(R) \neq R_2$, that is, when $\mathrm{Soc}(R) \supsetneq R_2$. This case is slightly more complicated, but part (iii) gives us many more stars, using Theorem 3.12.

Theorem 3.13. *Continue with the assumptions and notation of Construction* 3.1*, Remark* 3.7*, and Notation* 3.9*. Assume that* $\mathrm{Soc}(R) \neq R_2$*, and assume that* $z \in \mathrm{Soc}(R) \setminus R_2$*. Let* $[l_1], \ldots, [l_{c-1}], [z]$ *be the distinct vertices of* $\Gamma_E(R)$*.*

(i) *The number of distinct vertices in* $\Gamma_E(R^\flat)$ *is* $c^\flat = c + v + 3$*.*

(ii) *The graph* $\Gamma_E(R^\flat)$ *is obtained from* $\Gamma_E(R)$ *by adding the following* $v+3$ *vertices* $[Y_1], [f_1], \ldots, [f_v], [zY_1], [X_1 + Y_1]$ *and the* $v + c + 2$ *edges* $[zY_1] - [X_1 + Y_1]$*,* $[zY_1] - [Y_1], [zY_1] - [f_1], \ldots, [zY_1] - [f_v], [zY_1] - [z], [zY_1] - [l_1], \ldots, [zY_1] - [l_{c-1}]$*.*

(iii) *The following conditions are equivalent:*

   (a) $\Gamma_E(R^\flat)$ *is a star;*

   (b) $\Gamma_E(R)$ *is a single vertex;*

   (c) $R_2 = 0$;

   (d) $\mathrm{Soc}(R) = R_1$; *and*

   (e) $c = 1$.

Proof. Parts (i) and (ii) are proved like the corresponding parts of Theorem 3.12. The only real difference is in the fact that $z \in R_1$ implies that $z \notin R_2^\flat = \mathrm{Soc}(R^\flat)$; see Proposition 3.8 (ii). Thus, the graph $\Gamma_E(R^\flat)$ has a new socle vertex $[zY_1]$.

   (iii) We first show that (e) $\Rightarrow$ (n) for $n = $ a–d. Assume that $c = 1$. It follows by definition that $[z]$ is the only vertex in $\Gamma_E(R)$. In other words, every non-unit $f \in R \setminus \{0\}$ has $\mathrm{Ann}_R(f) = \mathrm{Ann}_R(z) = \mathfrak{m}$ where $\mathfrak{m} = 0 \oplus R_1 \oplus R_2$. It follows that $R_2 = \mathfrak{m}^2 = 0$ and hence $\mathrm{Soc}(R) = \mathfrak{m} = R_1$. Finally, the description of $\Gamma_E(R^\flat)$ from part (ii) shows that $\Gamma_E(R^\flat)$ is a star in this case. This gives the desired implications.

   Next, we show $(n) \Rightarrow$ (e) for $n = $ a–d. We argue by contrapositive, so assume that $c \geq 2$. It follows by definition that $\Gamma_E(R)$ is not a single vertex. Thus, there is an element $f \in \mathfrak{m}$ such that $\mathrm{Ann}_R(f) \neq \mathrm{Ann}_R(z) = \mathfrak{m}$. That is, $\mathfrak{m}f \neq 0$, so $R_2 = \mathfrak{m}^2 \neq 0$. It follows that $\mathrm{Soc}(R) \neq R_1$ since $0 \neq R_2 \subseteq \mathrm{Soc}(R) \setminus R_1$. Finally, the description of $\Gamma_E(R^\flat)$ in part (ii) shows that $\Gamma_E(R^\flat)$ contains the cycle $[z] - [f] - [zY_1] - [z]$ so $\Gamma_E(R^\flat)$ is not a star in this case. This gives the desired implications. $\square$

   The example below uses the computations from Theorems 3.12 and 3.13.

Example 3.14. Start with $R = \mathbb{F}_2[\mathbf{X}]/(\mathbf{X})^2$ where $\mathbf{X} = X_1, \ldots, X_{d_1}$ is a sequence of indeterminates with $d = d_1 \geq 1$. Then $R_2 = 0$, $\mathrm{Soc}(R) = R_1$, and $\Gamma_E(R)$ is a single vertex; see Example 3.3 (i). Thus, Theorem 3.13 (iii) applies, and the graph $\Gamma_E(R^\flat)$ obtained using $e = e_1$ and $t = t_1$ is a star with number of vertices

$$c^\flat = 1 + v_1 + 3 = 2^{d_1 + e_1} - 2^{d_1} - 2^{e_1} - 2^{t_1} + 6.$$

For instance, when $e_1 = 1$ we must have $t_1 = 1$ and

$$c^\flat = 2^{d_1 + 1} - 2^{d_1} - 2^1 - 2^1 + 6 = 2^{d_1} + 2. \tag{3.14.1}$$

Some example graphs in this case are the following:

$$e_1 = 1 = t_1, \quad d_1 = 1:$$

$[X_1]$ $[X_1Y_1]$ $[X_1 + Y_1]$

$d_1 = 2$:

$d_1 = 3$:
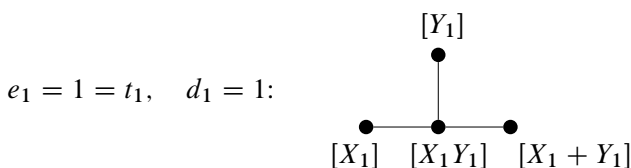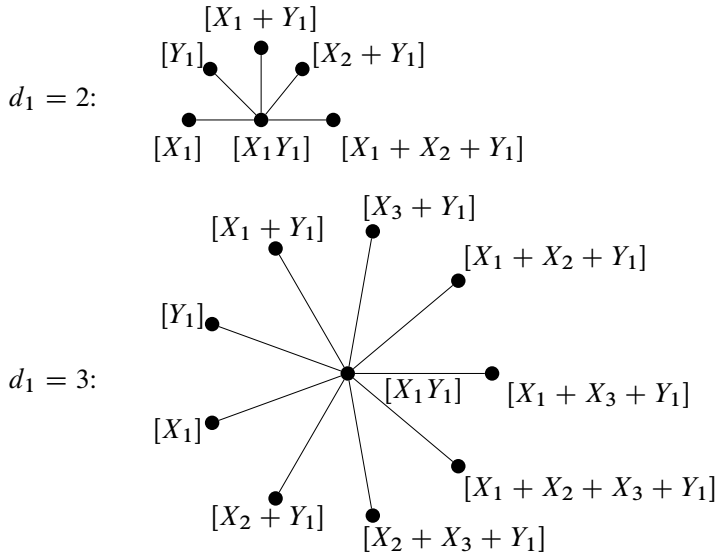
For instance, when $e_1 = 2$ we must have $t_1 = 1$ or 2, and in this case we have

$$c^\flat = \begin{cases} 2^{d_1} \cdot 3 & \text{if } t_1 = 1, \\ 2^{d_1} \cdot 3 - 2 & \text{if } t_1 = 2. \end{cases} \tag{3.14.2}$$

Note that the case $t_1 = 2$ above requires that $d_1 \geq 2$. However, when $d_1 = 1$, the formula yields $c^\flat = 4$, which is covered by the case $d_1 = e_1 = t_1 = 1$. Similarly, the values of (3.14.1) and (3.14.2) for $d_1 = 0$ can also be found.

The following table includes the values of $c^\flat$ for star graphs we can construct using this method with $c^\flat < 100$:

d_1	e_1	t_1	$c^\flat$	d_1	e_1	t_1	$c^\flat$	d_1	e_1	t_1	$c^\flat$
1	1	1	4	2	2	1	12	2	5	1	96
1	2	1	6	2	2	2	10	2	5	2	94
1	3	1	10	2	3	1	24	3	3	1	52
1	4	1	18	2	3	2	22	3	3	2	50
1	5	1	34	2	4	1	48	3	3	3	46
1	6	1	66	2	4	2	46				

Proposition 3.8 (ii) implies that $\operatorname{Soc}(R^\flat) = R_2^\flat$, so we can apply Theorem 3.12 to conclude that $\Gamma_E(R^{\flat\flat})$ is a star with $c^{\flat\flat}$ vertices where

$$c^{\flat\flat} = c^\flat + v_2 + 2,$$
$$= [2^{d_1 + e_1} - 2^{d_1} - 2^{e_1} - 2^{t_1} + 6] + [2^{d_2 + e_2} - 2^{d_2} - 2^{e_2} - 2^{t_2} + 2] + 2,$$
$$= [2^{d_1 + e_1} - 2^{d_1} - 2^{e_1} - 2^{t_1} + 6] + [2^{d_1 + e_1 + e_2} - 2^{d_1 + e_1} - 2^{e_2} - 2^{t_2} + 2] + 2,$$
$$= 2^{d_1 + e_1 + e_2} - 2^{d_1} - 2^{e_1} - 2^{t_1} - 2^{e_2} - 2^{t_2} + 10.$$

The tables in Appendix A include the values of c^{bb} for star graphs we can construct using this method with $c^{bb} < 100$. The next display gives some special cases of this formula:

$$c^{bb} = \begin{cases} 2^{d_1} \cdot 7 & \text{if } t_1 = e_1 = t_2 = 1 \text{ and } e_2 = 2, \\ 2^{d_1} \cdot 7 - 2 & \text{if } t_1 = e_1 = 1 \text{ and } t_2 = e_2 = 2, \\ 2^{d_1} \cdot 15 - 4 & \text{if } t_1 = 1 \text{ and } e_1 = t_1 = e_2 = 2, \\ 2^{d_1} \cdot 15 - 6 & \text{if } t_1 = e_1 = t_2 = e_2 = 2. \end{cases} \quad (3.14.3)$$

The case $t_1 = e_1 = t_2 = e_2 = 1$ is not included, as it repeats a previous formula.

This process can be repeated ad nauseum, but the number of vertices grows very quickly, even if one uses only one new variable at each iteration. See Appendix A.

For ease of reference, the list of even c-values with $c < 100$ we can produce with this method is 2–18, 22–34, 46–66, 94–98. (Note that $c = 2$ is achieved from the ring $\mathbb{F}_2[X]/(X^3)$.)

Example 3.15. Fix an integer $d = d_1 \geq 2$, and let $\mathbf{X} = X_1, \ldots, X_{d_1}$ be indeterminates. Consider the ring $R = \mathbb{F}_2[\mathbf{X}]/((X_1^2, \ldots, X_{d_1}^2) + (\mathbf{X})^3)$ from Example 3.3 (ii). The graph $\Gamma_E(R)$ is a star with 2^{d_1} vertices, and $\text{Soc}(R) = R_2$, so we may apply Construction 3.1 as in Example 3.14 to find that $\Gamma_E(R^b)$ is a star with number of vertices

$$c^b = 2^{d_1 + e_1} - 2^{e_1} - 2^{t_1} + 4.$$

Some special cases of this are listed next:

$$c^b = \begin{cases} 2^{d_1 + 1} & \text{if } t_1 = e_1 = 1, \\ 2^{d_1 + 2} - 2 & \text{if } t_1 = 1 \text{ and } e_1 = 2, \\ 2^{d_1 + 2} - 4 & \text{if } t_1 = e_1 = 2, \\ 2^{e_1} \cdot 3 + 2 & \text{if } d_1 = 2 \text{ and } t_1 = 1, \\ 2^{e_1} \cdot 3 & \text{if } d_1 = 2 \text{ and } t_1 = 2, \\ 2^{e_1} \cdot 7 + 2 & \text{if } d_1 = 3 \text{ and } t_1 = 1, \\ 2^{e_1} \cdot 7 & \text{if } d_1 = 3 \text{ and } t_1 = 2, \\ 2^{e_1} \cdot 7 - 4 & \text{if } d_1 = 3 \text{ and } t_1 = 3, \\ 2^{e_1} \cdot 15 + 2 & \text{if } d_1 = 4 \text{ and } t_1 = 1, \\ 2^{e_1} \cdot 15 & \text{if } d_1 = 4 \text{ and } t_1 = 2, \\ 2^{e_1} \cdot 15 - 2 & \text{if } d_1 = 4 \text{ and } t_1 = 3, \\ 2^{e_1} \cdot 15 - 4 & \text{if } d_1 = 4 \text{ and } t_1 = 4, \end{cases} \quad (3.15.1)$$

This yields a few more c-values to add from the list from Example 3.14:

$$c^\flat = \begin{cases} 20 & \text{if } d_1 = 2, e_1 = 3, \text{ and } t_1 = 1, \\ 44 & \text{if } d_1 = 2, e_1 = 4, \text{ and } t_1 = 1, \\ 42 & \text{if } d_1 = 2, e_1 = 4, \text{ and } t_1 = 2, \\ 92 & \text{if } d_1 = 2, e_1 = 5, \text{ and } t_1 = 1, \\ 90 & \text{if } d_1 = 2, e_1 = 5, \text{ and } t_1 = 2. \end{cases} \tag{3.15.2}$$

Thus, the list of even c-values with $c < 100$ we can produce with this method (combined with the values from Example 3.14 is 2–34, 42–66, 90–98. At this time, we do not know how to obtain the values 36–40, 68–88.

Next, we show how to build some star graphs with odd numbers of vertices.

Construction 3.16. Let R be a $\mathbb{Z}$-graded ring $R = \mathbb{F}_2 \oplus R_1 \oplus R_2$ generated over $\mathbb{F}_2$ by R_1. Let Y be an indeterminate, and set

$$R^\# = R[Y]/((\mathrm{Soc}(R)Y) + (R_1 Y^2) + (Y^3)).$$

Remark 3.17. Continue with the assumptions and notation of Construction 3.16. Once again, the ring R is local with maximal ideal $\mathfrak{m} = R_+ = 0 \oplus R_1 \oplus R_2$. Note that we are not assuming that $r^2 = 0$ for all $r \in R_1$.

The next result is proved like Propositions 3.4 and 3.5.

Proposition 3.18. *Continue with the assumptions and notation of Construction* 3.16.

(i) *The ring $R^\#$ is $\mathbb{Z}^2$-graded with*

$$R^\# = R^\#_{(0,0)} \oplus [R^\#_{(1,0)} \oplus R^\#_{(0,1)}] \oplus [R^\#_{(2,0)} \oplus R^\#_{(1,1)} \oplus R^\#_{(0,2)}]$$
$$\cong \mathbb{F}_2 \oplus [R_1 \oplus \mathrm{Span}_{\mathbb{F}_2}(Y)] \oplus \left[R_2 \oplus \frac{R_1 \, \mathrm{Span}_{\mathbb{F}_2}(Y)}{\mathrm{Soc}(R)_1 \, \mathrm{Span}_{\mathbb{F}_2}(Y)} \oplus \mathrm{Span}_{\mathbb{F}_2}(Y^2) \right].$$

(ii) *The ring $R^\#$ is local with maximal ideal*

$$\mathfrak{m}^\# = R^\#_+ = 0 \oplus [R^\#_{(1,0)} \oplus R^\#_{(0,1)}] \oplus [R^\#_{(2,0)} \oplus R^\#_{(1,1)} \oplus R^\#_{(0,2)}].$$

The element $Y \in R^\#$ is a non-unit such that $Y^2 \neq 0$. Contrast this with the behavior of the non-units in the rings R, R', and $R^\flat$.

The next results are proved like Propositions 3.8 and 3.11, and Theorem 3.12.

Proposition 3.19. *Continue with the assumptions and notation of Construction* 3.16.

(i) *For all $l \in R_1 \setminus \mathrm{Soc}(R)$ and $m \in \mathrm{Span}_{\mathbb{F}_2}(Y) \setminus \{0\}$, we have $lm \neq 0$ in $R^\#$.*

(ii) $\mathrm{Soc}(R^\#) = 0 \oplus [\mathrm{Soc}(R)_1 \oplus 0] \oplus R^\#_2.$

Proposition 3.20. *Continue with the assumptions and notation of Construction* 3.16. *For all $l \in R_1 \setminus 0$, we have*

(i) $\mathrm{Ann}_{R^{\#}}(l) = \begin{cases} \mathfrak{m}^{\#} = R_{+}^{\#} & \text{if } l \in \mathrm{Soc}(R), \\ 0 \oplus [\mathrm{Ann}_R(l)_1 \oplus 0] \oplus R_2^{\#} & \text{if } l \notin \mathrm{Soc}(R). \end{cases}$

(ii) $\mathrm{Ann}_{R^{\#}}(Y) = 0 \oplus [\mathrm{Soc}(R)_1 \oplus 0] \oplus R_2^{\#} = \mathrm{Ann}_{R^{\#}}(l + Y)$.

We break the description of $\Gamma_E(R^{\#})$ into three results.

Theorem 3.21. *Continue with the assumptions and notation of Construction* 3.16. *Let c denote the number of vertices in $\Gamma_E(R)$. Assume that there is an element $l \in R_1$ such that $\mathrm{Ann}_R(l) = \mathrm{Soc}(R)$.*

(i) *The number of distinct vertices in $\Gamma_E(R^{\#})$ is $c^{\#} = c$.*

(ii) *$\Gamma_E(R^{\#})$ is graph isomorphic to $\Gamma_E(R)$.*

(iii) *$\Gamma_E(R^{\#})$ is a star if and only if $\Gamma_E(R)$ is a star.*

Theorem 3.22. *Continue with the assumptions and notation of Construction* 3.16. *Let c denote the number of vertices in $\Gamma_E(R)$, and fix an element $z \in \mathrm{Soc}(R) \setminus 0$. Assume that $\mathrm{Ann}_R(l) \neq \mathrm{Soc}(R)$ for all $l \in R_1$.*

(i) *The number of distinct vertices in $\Gamma_E(R^{\#})$ is $c^{\#} = c + 1$.*

(ii) *$\Gamma_E(R^{\#})$ is formed from $\Gamma_E(R)$ by adding one vertex $[Y]$ and one edge $[z] - [Y]$.*

(iii) *$\Gamma_E(R^{\#})$ is a star if and only if $\Gamma_E(R)$ is a star.*

Corollary 3.23. *Continue with the assumptions and notation of Construction* 3.16. *Let c denote the number of vertices in $\Gamma_E(R)$, and fix an element $z \in \mathrm{Soc}(R) \setminus 0$. Assume that $\mathfrak{m}^2 \neq 0$ and that $r^2 = 0$ for all non-units $r \in R$.*

(i) *$\mathrm{Ann}_R(l) \neq \mathrm{Soc}(R)$ for all $l \in R_1$.*

(ii) *The number of distinct vertices in $\Gamma_E(R^{\#})$ is $c^{\#} = c + 1$.*

(iii) *$\Gamma_E(R^{\#})$ is formed from $\Gamma_E(R)$ by adding one vertex $[Y]$ and one edge $[z] - [Y]$.*

(iv) *$\Gamma_E(R^{\#})$ is a star if and only if $\Gamma_E(R)$ is a star.*

Proof. By Theorem 3.22, it suffices to show that $\mathrm{Ann}_R(l) \neq \mathrm{Soc}(R)$ for all $l \in R_1$. So, let $l \in R_1$ be given, and suppose that $\mathrm{Ann}_R(l) = \mathrm{Soc}(R)$. By assumption, we have $l \in \mathrm{Ann}_R(l) = \mathrm{Soc}(R)$, so $l\mathfrak{m} = 0$. This implies that $\mathfrak{m} \subseteq \mathrm{Ann}_R(l)$. The condition $\mathrm{Ann}_R(l) = \mathrm{Soc}(R)$ implies that $l \neq 0$, so we have $\mathfrak{m} = \mathrm{Ann}_R(l) = \mathrm{Soc}(R)$. It follows that $\mathfrak{m}^2 = 0$, a contradiction. $\square$

Example 3.24. We return now to the assumptions and notation of Construction 3.1. Proposition 3.4 implies that $(\mathfrak{m}^{\flat})^2 \neq 0$ and that $r^2 = 0$ for all non-units $r \in R^{\flat}$. Theorems 3.12–3.13 and Corollary 3.23 imply that $\Gamma_E(R^{\flat \#})$ is a star with $c + 1$ vertices.

Thus, for each star graph with an even number of vertices $c \geq 2$ we constructed in Examples 3.14 and 3.15, we obtain a star graph with an odd number of vertices $c + 1$. (Of course, the graph of the ring $\mathbb{F}_2[X]/(X^2)$ is a degenerate star with one vertex.) The list of odd c-values with $c < 100$ we can produce with this method is 1–35, 43–67, 91–99, while we do not know how to produce 37–41, 69–89.

Next, we indicate how we obtain the list of stars from the introduction.

Example 3.25. Let n be a non-negative integer.

$c = 2^n - 4$: If $n \geq 4$, then we may use equation (3.15.1) with $t_1 = e_1 = 2$ and $n = d_1 + 2$ to find a ring $R^\flat$ such that $\Gamma_E(R^\flat)$ is a star with $2^n - 4$ vertices. For the remaining values of n, the cases $n = 0, 1, 2$ imply that $2^n - 4 \leq 0$ (so we do not consider these); and the case $n = 3$ gives $c = 2^n - 4 = 4$ which we obtained explicitly in Example 3.14.

$c = 2^n - 3$: The rings produced in the previous paragraph all satisfy the hypotheses of Theorems 3.12–3.13 and Corollary 3.23, as in Example 3.24, so we obtain rings $R^{\flat\sharp}$ such that $\Gamma_E(R^{\flat\sharp})$ is a star with $2^n - 4 + 1$ vertices, when $n \geq 3$. For the remaining values of n, the cases $n = 0, 1$ imply that $2^n - 3 \leq 0$ (so we do not consider these); and the case $n = 2$ gives $c = 2^n - 3 = 1$ which we obtained explicitly in Example 3.24.

The remaining cases are derived similarly using the numbered equations from Examples 3.14 and 3.15, in conjunction with Example 3.24.

Example 3.26. Continue with the assumptions and notation of Construction 3.16. In the ring $R^\#$, the element Y satisfies $\text{Ann}_{R^\#}(Y) = 0 \oplus [\text{Soc}(R)_1 \oplus 0] \oplus R_2^\# = \text{Soc}(R^\#)$; see Propositions 3.19 (ii) and 3.20 (ii). Thus, Theorem 3.21 (ii) implies that $\Gamma_E(R^{\#\#})$ is graph isomorphic to $\Gamma_E(R^\#)$. Thus, one can not simply iterate this process to create rings with star graphs of any size.

Remark 3.27. Because they are needed for the proof of Proposition 5.8 we include three more examples of star graphs. These examples are instrumental to our argument that rings of length less than five must have a finite clique number. See Section 5.

Example 3.28. Let k be a field of characteristic 2, and set $R = k[X, Y]/(X^2, Y^2)$ where X and Y are indeterminates. Then R is a local ring with length 4 and maximal ideal $\mathfrak{m} = (x, y)R$ where x and y are the residues of X and Y in R.

We claim that $\Gamma_E(R)$ is a star with number of vertices equal to $2 + |k|$. The argument is similar to the proofs above, so we only outline the steps. We have the following:

$$\text{Soc}(R) = \mathfrak{m}^2 = (xy)R,$$

$$\text{Ann}_R(y) = (y)R + \mathfrak{m}^2 = (y)R,$$

$$\text{Ann}_R(x + ay) = (x + ay)R + \mathfrak{m}^2 = (x + ay)R \quad \text{for all } a \in k.$$

It follows that for all $b, c, d \in k$ such that $bx + cy + dxy \neq 0$, we have

$$[bx + cy + dxy] = \begin{cases} [xy] & \text{if } b = 0 = c, \\ [y] & \text{if } b = 0 \text{ and } c \neq 0, \\ [x + b^{-1}cy] & \text{if } b \neq 0, \end{cases}$$

and the distinct vertices in $\Gamma_E(R)$ are $[xy]$, $[y]$, and all classes of the form $[x + ay]$ where $a \in k$. No distinct vertices of the form $[y]$, $[x + ay]$, and $[x + a'y]$ are adjacent in $\Gamma_E(R)$, and all such vertices are adjacent to $[xy]$.

Example 3.29. Let k be a field of characteristic 2, and let $(Q, 2Q, k)$ be a discrete valuation ring. (Note that such a ring Q exists, e.g., as a ring of Witt vectors.) We set $R = Q[Y]/(4, Y^2)$ where Y is an indeterminate. Then R is a local ring with length 4 and maximal ideal $\mathfrak{m} = (2, y)R$ where y is the residue of Y in R. Since $4 = 0 = y^2$ in R, it follows that $\mathfrak{m}^2 = (2y)R$.

We claim that $\Gamma_E(R)$ is a star with number of vertices equal to $2 + |k|$. Because most of our previous examples contain a field, we include more details for this one. First, we observe that $R \cong (Q/4Q)[Y]/(Y^2)$, so R is a free $Q/4Q$-module of rank 2 with basis $1, y$. Units in R are of the form $\overline{q_0} + \overline{q_1}y$ where $q_0 \in Q \setminus 2Q$ and $q_1 \in Q$; here, for each element $q \in Q$, we write $\overline{q}$ for the residue of q in $Q/4Q$. Non-units in R are of the form $2\overline{q_0} + \overline{q_1}y$ where $q_0, q_1 \in Q$. Moreover, it is not difficult to see that every non-unit $r \in R$ satisfies $r^2 = 0$.

We claim that $\mathrm{Soc}(R) = \mathfrak{m}^2$. The containment $\mathrm{Soc}(R) \supseteq \mathfrak{m}^2$ follows from the fact that $\mathfrak{m}^3 = 0$. For the reverse containment, let $r \in \mathrm{Soc}(R)$, say $r = 2\overline{q_0} + \overline{q_1}y$ for elements $q_0, q_1 \in Q$. The equalities $0 = 2r = 4\overline{q_0} + 2\overline{q_1}y = 2\overline{q_1}y$ imply that $2\overline{q_1} = 0$ in $Q/4Q$; this uses the fact that R is free of rank 2 over $Q/4Q$ with basis $1, y$. Since Q is a discrete valuation ring with maximal ideal generated by 2, it follows that $q_1 \in 2Q$, so we have $q_1 = 2q_1'$ for some $q_1' \in Q$. Similarly, the equation $0 = yr$ implies that $q_0 = 2q_0'$ for some $q_0' \in Q$. Thus, we have

$$r = 2\overline{q_0} + \overline{q_1}y = 4\overline{q_0'} + 2\overline{q_1'}y = 2\overline{q_1'}y \in \mathfrak{m}^2$$

as desired.

Next, we claim that

$$\mathrm{Ann}_R(y) = (y)R + \mathfrak{m}^2 = (y)R.$$

The containment $(y)R + \mathfrak{m}^2 \subseteq (y)R$ follows from the fact that $\mathfrak{m}^2 = (2y)R \subseteq (y)R$ and the reverse containment is routine. The containment $\mathrm{Ann}_R(y) \supseteq (y)R$ is from the fact that $y^2 = 0$. For the reverse containment, let $r \in \mathrm{Ann}_R(y)$, where, since r is a non-unit, $r = 2\overline{q_0} + \overline{q_1}y$ for elements $q_0, q_1 \in Q$. Again, the equation $ry = 0$ implies that $\overline{q_0} = 2\overline{q_0'}$ for some $q_0' \in Q$. From this we have $r = \overline{q_1}y \in (y)R$, as desired.

Next, we claim that

$$\mathrm{Ann}_R(2 + \overline{q}y) = (2 + \overline{q}y)R + \mathfrak{m}^2 = (2 + \overline{q}y)R \tag{3.29.1}$$

for all $\overline{q} \in Q/4Q$. The equality $(2 + \overline{q}y)R + \mathfrak{m}^2 = (2 + \overline{q}y)R$ follows as in the previous paragraph because $2y = y(2 + \overline{q}y)$. The containment $\mathrm{Ann}_R(2 + \overline{q}y) \supseteq (2 + \overline{q}y)R + \mathfrak{m}^2$ is straightforward; thus, let $r \in \mathrm{Ann}_R(2 + \overline{q}y)$. Since r is a non-unit we have $r = 2\overline{q_0} + \overline{q_1}y$ for elements $q_0, q_1 \in Q$. Then we have

$$
\begin{aligned}
0 = r(2 + \overline{q}y) &= (2\overline{q_0} + \overline{q_1}y)(2 + \overline{q}y) \\
&= 4\overline{q_0} + (2\overline{q_0}\,\overline{q} + 2\overline{q_1})y + \overline{q_1}\,\overline{q}y^2 = (2\overline{q_0}\,\overline{q} + 2\overline{q_1})y.
\end{aligned}
$$

As before, this implies that $2\overline{q_0}\,\overline{q} + 2\overline{q_1} = 0$ in $Q/4Q$, and it follows that $-2\overline{q_0}\,\overline{q} + 2\overline{q_1} = 0$ in $Q/4Q$. Thus, we have $2\overline{q_1} = 2\overline{q_0}\,\overline{q}$ in $Q/4Q$, and it follows that $\overline{q_1} = \overline{q_0}\,\overline{q} + 2q_0'$ for some $q_0' \in Q$. From this we have

$$
r = 2\overline{q_0} + \overline{q_1}y = 2\overline{q_0} + (\overline{q_0}\,\overline{q} + 2q_0')y = \overline{q_0}(2 + \overline{q}y) + 2\overline{q_0'}y \in (2 + \overline{q}y)R + \mathfrak{m}^2
$$

as desired.

Next we claim that every vertex in $\Gamma_E(R)$ is of the form $[y]$, $[2y]$ or $[2 + \overline{q}y]$ for some $q \in Q$. Let $0 \neq r \in \mathfrak{m}$. If $r \in \mathfrak{m}^2 = \mathrm{Soc}(R)$, then $[r] = [2y]$ since $0 \neq 2y \in \mathfrak{m}^2 = \mathrm{Soc}(R)$. Assume then that $r \notin \mathfrak{m}^2$, and fix $q_0, q_1 \in Q$ such that $r = 2\overline{q_0} + \overline{q_1}y$. If $q_0 \in 2Q$, then $r = \overline{q_1}y$, and the fact that $r \notin \mathfrak{m}^2$ implies that $q_1 \in Q \backslash 2Q$; thus $\overline{q_1}$ is a unit in R and $[r] = [y]$. Assume then that $q_0 \notin 2Q$. It follows that q_0 is a unit in R, so $[r] = [2\overline{q_0} + \overline{q_1}y] = [2 + (\overline{q_0})^{-1}\overline{q_1}y]$ which is of the form $[2 + \overline{q}y]$, as desired.

The vertices $[2]$ and $[2y]$ are distinct since $y \in \mathrm{Ann}_R(2y)$, but $y \notin \mathrm{Ann}_R(2)$. Likewise, the vertices $[2y]$ and $[2 + \overline{q}y]$ are distinct for all $q \in Q$. The vertices $[y]$ and $[2 + \overline{q}y]$ are distinct for all $q \in Q$ since $y \in \mathrm{Ann}_R(y)$, but $y \notin \mathrm{Ann}_R(2 + \overline{q}y)$.

We claim that the vertices $[2 + \overline{q}y]$ and $[2 + \overline{q'}y]$ are equal if and only if $q - q' \in 2Q$, i.e., if and only if q and q' represent the same element in the field $Q/2Q \cong k$. For the first implication, assume that $q - q' \in 2Q$ and write $q - q' = 2q''$ where $q'' \in Q$. Then

$$
2 + \overline{q}y = 2 + \overline{q'}y + 2\overline{q''}y
$$

in R. Since $2\overline{q''}y$ is in $\mathfrak{m}^2$, by (3.29.1) it follows that $[2 + \overline{q}y] = [2 + \overline{q'}y]$.

For the converse, assume that $[2 + \overline{q}y] = [2 + \overline{q'}y]$ in $\Gamma_E(R)$. It follows that $2 + \overline{q}y \in \mathrm{Ann}_R(2 + \overline{q'}y) = (2 + \overline{q'}y)R$, so there are elements $q_0, q_1 \in Q$ where

$$
2 + \overline{q}y = (2 + \overline{q'}y)(\overline{q_0} + \overline{q_1}y) = 2\overline{q_0} + (\overline{q'q_0} + 2\overline{q_1})y. \tag{3.29.2}
$$

It follows that $2 = 2\overline{q_0}$ in $Q/4Q$, so $1 - q_0 = 2q''$ for some $q'' \in Q$. From the y coefficients in (3.29.2), we have

$$
\overline{q} = \overline{q'q_0} + 2\overline{q_1} = \overline{q'}(1 - 2q'') + 2\overline{q_1} = \overline{q'} + 2(\overline{q_1} - \overline{q'q''})
$$

in $Q/4Q$. It follows that $q - q' \in 2Q$, as desired. This ends the proof of the claim.

From the above claims, we conclude that $\Gamma_E(R)$ is a star with central vertex $[2y]$ and distinct ends $[y]$ and $[2 + \overline{q}y]$ where q ranges through a set of representatives of $Q/2Q \cong k$ in $Q/4Q$. Thus, the graph $\Gamma_E(R)$ is a star with $|k| + 2$ vertices.

Example 3.30. Let k be a field of characteristic 2, and let $(Q, 2Q, k)$ be a discrete valuation ring. We let X and Y be indeterminates and set

$$R = Q[\![X, Y]\!]/(4, X^2, Y^2, 2X, 2Y, 2 - XY)$$
$$\cong Q[X, Y]/(4, X^2, Y^2, 2X, 2Y, 2 - XY).$$

We show that the graph $\Gamma_E(R)$ is a star with $|k| + 2$ vertices.

The ring R is local with maximal ideal $\mathfrak{m} = (2, x, y)R = (x, y)R$ where x and y are the residues of X and Y in R; this is from the equation $2 = xy$ in R. Given the other equations determining R, we have $\mathfrak{m}^2 = (xy)R$. (Note that the element 4 in the ideal defining R is redundant since $4 = 2(2 - XY) + X(2Y)$ in $Q[\![X, Y]\!]$. We include it explicitly so that it is clear that $4 = 0$ in R.) Since $x^2 = 0 = y^2$ and $xy = 2$ in R, the elements of R all have the form $\bar{s} + \bar{p}x + \bar{q}y$, with $p, q, s \in Q$.

We claim that $\mathrm{len}(R) = 4$. To see this, note that the ring $Q[\![X, Y]\!]/(4, X^2, Y^2)$ has length 8, being a quotient of a regular local ring by the squares of the elements of a regular system of parameters. Modding out by a non-zero element of the socle reduces the length by 1. Thus, the ring $Q[\![X, Y]\!]/(4, X^2, Y^2, 2XY)$ has length 7, the ring $Q[\![X, Y]\!]/(4, X^2, Y^2, 2X)$ has length 6, the ring $Q[\![X, Y]\!]/(4, X^2, Y^2, 2X, 2Y)$ has length 5, and $Q[\![X, Y]\!]/(4, X^2, Y^2, 2X, 2Y, 2 - XY)$ has length 4.

Consider an element $r = \bar{s} + \bar{p}x + \bar{q}y \in R$, with $p, q, s \in Q$. We claim that $r = 0$ if and only if $p, q \in 2Q$ and $s \in 4Q$. One implication follows from the equalities $4 = 0 = 2x = 2y$ in R. For the converse, assume that $r = 0$. It follows that there are elements $f, f', g, g', h \in Q[\![X, Y]\!]$ such that

$$s + pX + qY = X^2 f + Y^2 g + 2Xf' + 2Yg' + (2 - XY)h. \qquad (3.30.1)$$

Write $f = \sum_{i,j \geq 0} f_{i,j} X^i Y^j$ with $f_{i,j} \in Q$, and similarly for f', g, g', h. Comparing constant terms and coefficients for x and y in this equation, we have

$$s = 2h_{0,0} \in 2Q, \quad p = 2f'_{0,0} + 2h_{1,0} \in 2Q, \quad q = 2g'_{0,0} + 2h_{0,1} \in 2Q$$

so it remains to show that $s \in 4Q$. To this end, compare coefficients for XY in (3.30.1) to find that

$$0 = 2f'_{0,0} + 2g'_{0,0} - h_{0,0} + 2h_{1,1}.$$

It follows that $h_{0,0} \in 2Q$, so $s = 2h_{0,0} \in 4Q$, as desired.

As a consequence of the previous paragraph, we find that the kernel of the natural map $Q \to R$ is precisely $4Q$.

Next, we note that an element $r = \bar{s} + \bar{p}x + \bar{q}y \in R$, with $p, q, s \in Q$, is a unit in R if and only if $s \notin 2Q$. Indeed, if $s \in 2Q$, then $r \in (2, x, y)R = \mathfrak{m}$. For the converse, assume that $s \notin 2Q$, that is, that s is a unit in Q. It follows that $s + pX + qY$ is invertible in $Q[\![X, Y]\!]$, say with inverse $\sum_{i,j \geq 0} a_{i,j} X^i Y^j$. Given the fact that $x^2 = 0 = y^2$ in R, it follows readily that $r^{-1} = \sum_{i=0}^{1} \sum_{j=0}^{1} \overline{a_{i,j}} x^i y^j$.

Given what we have shown, the following facts are readily verified. First, one has

$$\operatorname{Soc}(R) = \mathfrak{m}^2,$$
$$\operatorname{Ann}_R(x) = (x)R + \mathfrak{m}^2 = (x)R,$$
$$\operatorname{Ann}_R(y) = (y)R + \mathfrak{m}^2 = (y)R,$$
$$\operatorname{Ann}_R(x + \overline{q}y) = (x + \overline{q}y)R + \mathfrak{m}^2 = (x + \overline{q}y)R \quad \text{for all } q \in Q.$$

We have $2 \in \operatorname{Soc}(R)$, so every vertex $v \neq [2]$ in $\Gamma_E(R)$ has the form $[x]$, $[y]$ or $[x + \overline{q}y]$ for some unit $q \in Q$. Furthermore, we have $[x] \neq [y]$ and $[x] \neq [x + \overline{q}y] \neq [y]$ for each unit $q \in Q$. Also, given units $q, q' \in Q$, we have $[x + \overline{q}y] = [x + \overline{q'}y]$ if and only if $q - q' \in 2Q$ if and only if q and q' represent the same element in $Q/2Q \cong k$. From this, it follows that $\Gamma_E(R)$ is a star with central vertex $[2]$ and with $2 + |k|$ vertices.

4 Graph Homomorphisms and Graphs Associated to Modules

In this section we study *graph homomorphisms* $\Gamma_E(R) \to \Gamma_E(S)$ induced by ring homomorphisms $R \to S$. This allows us to produce an Artinian ring R of length 4 such that $\Gamma_E(R)$ is an infinite star. In addition, we introduce and study a "torsion graph" associated to an R-module M, which is used in Section 5 to produce an Artinian ring R of length 6 such that $\Gamma_E(R)$ has infinite clique number.

Proposition 4.1. *Given a flat ring monomorphism* $\varphi \colon R \hookrightarrow S$, *the graph* $\Gamma_E(R)$ *is isomorphic to an* induced subgraph *of* $\Gamma_E(S)$.

Proof. Let r be a zero divisor in R. Then $rr' = 0$ for some zero divisor $r' \in R$. Since φ is a ring monomorphism, it follows that $\varphi(r)$ and $\varphi(r')$ are non-zero elements of S such that $\varphi(r)\varphi(r') = 0$. Thus, $Z^*(R)$ maps into $Z^*(S)$. Moreover, if $r, r' \in Z^*(R)$ are equivalent, then $\varphi(r)$ and $\varphi(s)$ are equivalent in $Z^*(S)$: the equivalence of r and r' means that $\operatorname{Ann}_R(r) = \operatorname{Ann}_R(r')$, so the flatness of φ implies that $\operatorname{Ann}_S(\varphi(r)) = \operatorname{Ann}_R(r)S = \operatorname{Ann}_R(r')S = \operatorname{Ann}_S(\varphi(r'))$, as desired; see [28, Theorem 7.4 (iii)].

Moreover, if $\operatorname{Ann}(r_1) \neq \operatorname{Ann}(r_2)$, then $\operatorname{Ann}(\varphi(r_1)) \neq \operatorname{Ann}(\varphi(r_2))$ since $x \in \operatorname{Ann}(r_1) \setminus \operatorname{Ann}(r_2)$ implies $\varphi(x) \in \operatorname{Ann}(\varphi(r_1))$, but $\varphi(x)\varphi(r_2) \neq 0$ since $xr_2 \neq 0$. Thus, φ preserves equivalence classes. Also, we have already seen that edges in $\Gamma_E(R)$ correspond to edges in $\Gamma_E(S)$. This means that $\Gamma_E(R)$ is a subgraph of $\Gamma_E(S)$. Finally, to see that $\Gamma_E(R)$ is an induced subgraph, note that if there is an edge between $[\varphi(r_1)]$ and $[\varphi(r_2)]$ in $\Gamma_E(S)$, then there is an edge between $[r_1]$ and $[r_2]$ in $\Gamma_E(R)$ since $0 = \varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2)$ and φ is injective. □

A special case of the next result is stated without proof in [29, page 3552, lines 4–5]. It is worth noting that the analogous result for $\Gamma(R)$ is proved in [9, Theorem 2.2].

Proposition 4.2. *Let U be a multiplicatively closed subset, consisting of non-zero divisors, in the ring R. Then $\Gamma_E(R)$ and $\Gamma_E(U^{-1}R)$ are isomorphic as graphs.*

Proof. Let $\varphi : R \hookrightarrow U^{-1}R$. By Proposition 4.1, $\Gamma_E(R)$ is an induced subgraph of $\Gamma_E(U^{-1}R)$, therefore, we only need to show that there is a one-to-one correspondence between the vertices of $\Gamma_E(R)$ and those of $\Gamma_E(U^{-1}R)$. Let $[r/u] \in \Gamma_E(U^{-1}R)$. Then there exists a non-zero element $r'/u' \in U^{-1}R$ such that $rr'/uu' = 0$; i.e., there exists u'' such that $u''rr' = 0$ in R. However, since u'' is a non-zero divisor, we must have $rr' = 0$; so $r \in Z^*(R)$. Moreover, this shows that $r'/u' \in \mathrm{Ann}_{U^{-1}R}(r/u)$ if and only if $r' \in \mathrm{Ann}_R(r)$. It follows that $[r/u] = [r/1]$ in $\Gamma_E(U^{-1}R)$. $\square$

Corollary 4.3. *If $Z^*(R) \cup \{0\} = \mathrm{nil}(R)$, then $\mathrm{nil}(R)$ is a prime ideal and hence $\Gamma_E(R) \cong \Gamma_E(R_{\mathrm{nil}(R)})$; if R is also Noetherian, then $\Gamma_E(R) \cong \Gamma_E(A)$ where A is an Artinian local ring.*

As a tool for studying the clique numbers of $\Gamma_E(R)$, we introduce the "torsion graph" of a finitely generated R-module M. Note that our definition is different from those recently appearing in the literature [23].

Definition 4.4. To the pair R, M, we associate a **torsion graph**: (i) let $G^R(M)$ be the graph where every element of M is a distinct vertex; (ii) let $\Gamma^R(M)$ be the graph where each non-zero torsion element of M is represented by a distinct vertex; and (iii) let $\Gamma_E^R(M)$ be the graph whose vertices $[m]$ are the equivalence classes of non-zero torsion elements, where $m, n \in M$ are equivalent provided that $\mathrm{Ann}_R(m) = \mathrm{Ann}_R(n)$. For each of these graphs, join an edge between each pair of distinct vertices if and only if their annihilator ideals have a non-trivial intersection; i.e., if and only if $\mathrm{Ann}_R(m) \cap \mathrm{Ann}_R(n) \neq (0)$.

Example 4.5. Let $R = M = \mathbb{Z}/6\mathbb{Z}$. The graphs associated to M are shown below:

$$G^R(M) \qquad\qquad \Gamma^R(M) \qquad\qquad \Gamma_E^R(M)$$
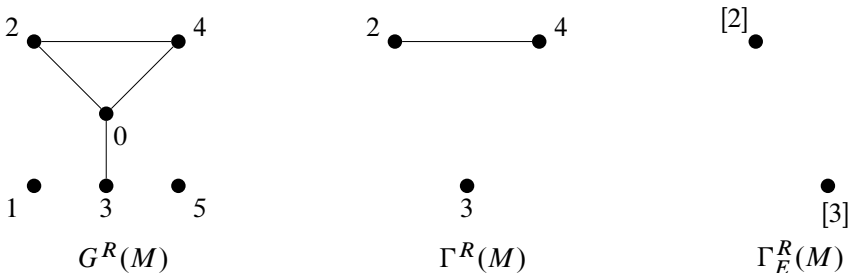
On the other hand, if we let $M = \mathbb{Z}/6\mathbb{Z}$, but change the ring to $R = \mathbb{Z}$, then $G^{\mathbb{Z}}(M) = K_6$, $\Gamma^{\mathbb{Z}}(M) = K_5$ (since 0 is omitted), and $\Gamma_E^{\mathbb{Z}}(M) = K_3$. For the last graph, note that there are now three classes determined by $\mathrm{Ann}_R(\bar{1}) = 6\mathbb{Z}$, $\mathrm{Ann}_R(\bar{2}) = 3\mathbb{Z}$, and $\mathrm{Ann}_R(\bar{3}) = 2\mathbb{Z}$.

Proposition 4.6. *If R is a domain or $\operatorname{Ann}_R(M) \neq (0)$, then $\Gamma_E^R(M)$ is complete.*

Proof. If R is a domain and M is torsion free, then the result holds vacuously; likewise, if the elements in the torsion submodule $\operatorname{Tor}(M)$ form a single equivalence class, then the result holds trivially. Thus, suppose $\operatorname{Tor}(M)$ contains at least two distinct classes $[m]$ and $[m']$. If R is a domain, there are $0 \neq r \in \operatorname{Ann}_R(m)$ and $0 \neq r' \in \operatorname{Ann}_R(m')$ such that $0 \neq rr' \in \operatorname{Ann}_R(m) \cap \operatorname{Ann}_R(m')$. Likewise, if $0 \neq r \in \operatorname{Ann}_R(M)$. $\hfill\square$

Remark 4.7. These examples and results show that many standard results for zero divisor graphs of rings do not hold for torsion graphs associated to modules, regardless of how the vertices are chosen. For example, all previous zero divisor graphs have been connected. Moreover, considering $\Gamma_E(R)$, cycle graphs and complete graphs with more than two vertices are not possible.

From a different perspective, given a ring R and R-module M, one can consider the graph $\Gamma_E(R \ltimes M)$, where $R \ltimes M$ is the **trivial extension** of R by M, also known as the "idealization" of M. (Another notation for this construction is $R(+)M$, as in the survey [5].) As an additive Abelian group, one has $R \ltimes M = R \oplus M$. The multiplication $(r, m) \cdot (r', m') = (rr', rm' + r'm)$ makes $R \ltimes M$ into a ring. The following results will be useful in studying infinite cliques in the next section.

Fact 4.8. Set $S = R \ltimes M$ and let $r \in R$ and $m \in M$. Then:

(i) $\operatorname{Ann}_S(r, 0) = \operatorname{Ann}_R(r) \oplus \operatorname{Ann}_M(r)$, where $\operatorname{Ann}_M(r) = \{m \in M \mid rm = 0\}$;

(ii) $\operatorname{Ann}_S(0, m) = \operatorname{Ann}_R(m) \oplus M$;

(iii) $\operatorname{Ann}_S(r, m) = \{(s, n) \mid s \in \operatorname{Ann}_R(r), n \in M \text{ with } rn + sm = 0\}$;

(iv) If R is a domain and $r \neq 0$, then $\operatorname{Ann}_S(r, 0) = \operatorname{Ann}_S(r, m) = 0 \oplus \operatorname{Ann}_M(r)$.

Proposition 4.9. *For any ring R and any R-module M, the graph $\Gamma_E^R(M)$ is a subgraph of $\Gamma_E(R \ltimes M)$; it is an induced subgraph if and only if $\Gamma_E^R(M)$ is complete.*

Proof. Fact 4.8 (ii) shows the following: (1) if m is a non-zero element of M, then $(0, m) \in R \ltimes M$ is a non-zero torsion element; and (2) two non-zero torsion elements $m, m' \in M$ are equivalent if and only if the elements $(0, m)$ and $(0, m')$ in $R \ltimes M$ are equivalent. This shows that $\Gamma_E^R(M)$ is a subgraph of $\Gamma_E(R \ltimes M)$. However, the classes $[(0, m)]$ in $\Gamma_E(R \ltimes M)$ form a complete subgraph, therefore $\Gamma_E^R(M)$ would need to be complete in order to be induced. $\hfill\square$

It is natural to ask whether the natural ring homomorphism $R \to R \ltimes M$ induces a well-defined graph homomorphism $\Gamma_E(R) \to \Gamma_E(R \ltimes M)$. Fact 4.8 (i) shows that this is equivalent to the following: for all $r, r' \in R$ if $\operatorname{Ann}_R(r) = \operatorname{Ann}_R(r')$, then $\operatorname{Ann}_M(r) = \operatorname{Ann}_M(r')$. Our next result gives a criterion guaranteeing that this condition is satisfied.

Proposition 4.10. *Assume that M satisfies one of the following conditions:*

(i) *M is an R-submodule of $\operatorname{Hom}_R(N, R)$ for some R-module N.*

(ii) *The natural "biduality" map $\delta_M \colon M \to \operatorname{Hom}_R(\operatorname{Hom}_R(M, R), R)$ is injective.*

(iii) *M is a submodule of a finite rank free R-module.*

Then the natural ring homomorphism $R \to R \ltimes M$ induces a well-defined graph monomorphism $\Gamma_E(R) \to \Gamma_E(R \ltimes M)$ making $\Gamma_E(R)$ into an induced subgraph of $\Gamma_E(R \ltimes M)$.

Proof. It is straightforward to show that (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i), so we assume that M satisfies condition (i). Let $r, r' \in R$ such that $\operatorname{Ann}_R(r) = \operatorname{Ann}_R(r')$. We claim that $\operatorname{Ann}_M(r) = \operatorname{Ann}_M(r')$. By symmetry, it suffices to show that $\operatorname{Ann}_M(r) \subseteq \operatorname{Ann}_M(r')$, so let $f \in \operatorname{Ann}_M(r)$. Then f is an R-module homomorphism $N \to R$ such that $rf = 0$, that is, such that $rf(n) = 0$ for all $n \in N$. It follows that $\operatorname{Im}(f) \subseteq \operatorname{Ann}_R(r) = \operatorname{Ann}_R(r')$, and similar reasoning implies that $f \in \operatorname{Ann}_M(r')$.

Using the claim, Fact 4.8 (i) implies that for all $r, r' \in R$ if $\operatorname{Ann}_R(r) = \operatorname{Ann}_R(r')$, then $\operatorname{Ann}_{R \ltimes M}(r, 0) = \operatorname{Ann}_{R \ltimes M}(r', 0)$. Thus, the rule of assignment $[r] \mapsto [(r, 0)]$ describes a well-defined function from the vertex set of $\Gamma_E(R)$ to the vertex set of $\Gamma_R(R \ltimes M)$. Moreover, Fact 4.8 (i) implies that for all $r, r' \in R$ if $\operatorname{Ann}_{R \ltimes M}(r, 0) = \operatorname{Ann}_{R \ltimes M}(r', 0)$, then $\operatorname{Ann}_R(r) = \operatorname{Ann}_R(r')$; hence this map is injective. Finally, it is straightforward to show that $(r, 0)(r', 0) = 0$ in $R \ltimes M$ if and only if $rr' = 0$ in R, so $\Gamma_E(R)$ is an induced subgraph of $\Gamma_E(R \ltimes M)$. $\qquad\square$

The next example shows that the natural ring homomorphism $R \to R \ltimes M$ does not necessarily induce a well-defined graph homomorphism $\Gamma_E(R) \to \Gamma_E(R \ltimes M)$. See also Example 5.2.

Example 4.11. Let $R = k[X, Y]/(X, Y)^2$ where k is a field, and set $M = R/XR$. Then we have $\operatorname{Ann}_R(X) = (X, Y)R = \operatorname{Ann}_R(Y)$, but $\operatorname{Ann}_M(X) = M \supsetneq YM = \operatorname{Ann}_M(Y)$. Thus, we have $[X] = [Y]$ in $\Gamma_E(R)$, but $[(X, 0)] \neq [(Y, 0)]$ in $\Gamma_E(R \ltimes M)$. It follows that the rule of assignment $[r] \mapsto [(r, 0)]$ does not describe a well-defined function from the vertex set of $\Gamma_E(R)$ to the vertex set of $\Gamma_R(R \ltimes M)$.

5 Cliques

One of our main motivations is the question of how pathological the behavior of $\Gamma_E(R)$ can be, and how one might avoid such pathologies by imposing mild conditions on R. As mentioned in the introduction, assuming that the ring is Noetherian or Artinian is not enough to ensure that the associated graph is finite or even has finite clique number. To construct a "small" ring R such that $\omega(\Gamma_E(R)) = \infty$, we begin by considering direct products of rings and reduce to the local case. Ultimately our construction yields an Artinian ring of length 6 with an infinite clique, but the question of whether such an example exists in length 5 is open.

Proposition 5.1. *Let R and S be rings.*

(i) $\Gamma_E(R \times S)$ *is infinite if and only if* $\Gamma_E(R)$ *or* $\Gamma_E(S)$ *is infinite.*

(ii) $\Gamma_E(R \times S)$ *has an infinite clique if and only if* $\Gamma_E(R)$ *or* $\Gamma_E(S)$ *has an infinite clique.*

(iii) $\omega(\Gamma_E(R \times S)) = \infty$ *if and only if* $\omega(\Gamma_E(R)) = \infty$ *or* $\omega(\Gamma_E(S)) = \infty$.

Proof. (i) The distinct vertices of $\Gamma_E(R \times S)$ have the form $[(1,0)]$, $[(0,1)]$, $[(r,1)]$, $[(1,s)]$, $[(r,0)]$, $[(0,s)]$, and $[(r,s)]$ where $r \in Z^*(R)$ and $s \in Z^*(S)$. (This holds even when R or S is a domain.) Thus, it is routine to show that

$$|\Gamma_E(R \times S)| = 2 + 2|\Gamma_E(R)| + 2|\Gamma_E(S)| + |\Gamma_E(R)||\Gamma_E(S)|,$$

and the result follows immediately.

(ii) If $\Gamma_E(R)$ has an infinite clique, then $\Gamma_E(R \times S)$ has an infinite clique with vertices of the form $[(r,0)]$; and similarly if $\Gamma_E(S)$ has an infinite clique.

Conversely, assume that $\Gamma_E(R \times S)$ has an infinite clique. Given the form of the vertices of $\Gamma_E(R \times S)$, it follows that $\Gamma_E(R \times S)$ has an infinite clique containing only vertices of one of the following forms: $[(r,1)]$, $[(1,s)]$, $[(r,0)]$, $[(0,s)]$, or $[(r,s)]$ where $r \in Z^*(R)$ and $s \in Z^*(S)$. No two vertices of the form $[(r,1)]$ or $[(1,s)]$ are adjacent, so the infinite clique must contain only vertices of one of the following forms: $[(r,0)]$, $[(0,s)]$, or $[(r,s)]$. If there is an infinite clique in $\Gamma_E(R \times S)$ with vertices of the form $[(r,0)]$, then the r-values for this clique yield an infinite clique in $\Gamma_E(R)$; and similarly if there is an infinite clique in $\Gamma_E(R \times S)$ with vertices of the form $[(0,s)]$.

Thus, we assume that $\Gamma_E(R \times S)$ contains a clique with infinitely many vertices of the form $[(r_i, s_i)]$ where $i = 1, 2, 3, \ldots$. Since these vertices are distinct, the ideals $\operatorname{Ann}_R(r_i) \oplus \operatorname{Ann}_S(s_i) = \operatorname{Ann}_{R \times S}(r_i, s_i)$ must be distinct. Thus, there are either infinitely many distinct ideals in the set $\{\operatorname{Ann}_R(r_i)\}_i$ or in the set $\{\operatorname{Ann}_S(s_i)\}_i$. Since $r_i r_j = 0$ and $s_i s_j = 0$ for all $i \neq j$, it follows that either the $[r_i]$ form an infinite clique in $\Gamma_E(R)$ or the $[s_i]$ form an infinite clique in $\Gamma_E(S)$.

(iii) Argue as in the proof of part (ii), showing that $\Gamma_E(R \times S)$ has arbitrarily large cliques if and only if $\Gamma_E(R)$ or $\Gamma_E(S)$ has arbitrarily large cliques. $\square$

With the next example we show that even the Artinian condition on a ring is not enough to prevent its graph of zero divisors from having an infinite clique.

Example 5.2. Let k be a field and set $R = k[X,Y]/(X,Y)^2$. Let x and y be the residues in R of the variables X and Y. As a k-vector space, the ring R has rank 3 with basis $1, x, y$. Moreover, this basis imposes a $\mathbb{Z}^2$-graded structure on R that is

represented by the following diagram.

$$R$$
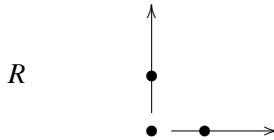
Set $M = E_R(k)$, the injective hull of k, in other words, the graded canonical module of R, which is given as $M = \operatorname{Hom}_{k[X,Y]}(R, k[X,Y])$. As a k-vector space, the module M has rank 3 with basis e, x^{-1}, y^{-1}, where the R-module structure is described according to the following rules:

$$x \cdot e = 0, \quad x \cdot x^{-1} = e, \quad x \cdot y^{-1} = 0,$$
$$y \cdot e = 0, \quad y \cdot y^{-1} = e, \quad y \cdot x^{-1} = 0.$$

This basis imposes a $\mathbb{Z}^2$-graded structure on M, represented by the next diagram.

$$M$$
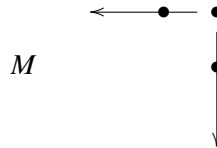
It is straightforward to verify the following computations where $a \in k$:

$$\operatorname{Ann}_R(e) = (x, y)R, \quad \operatorname{Ann}_R(y^{-1}) = xR, \quad \operatorname{Ann}_R(x^{-1} + ay^{-1}) = (ax - y)R.$$

In particular, the graph $\Gamma_E^R(M)$ has at least $|k| + 2$ distinct vertices. (In fact, these are exactly the distinct vertices of $\Gamma_E^R(M)$.) Thus, Proposition 4.9 implies that the graph $\Gamma_E(R \ltimes M)$ contains a clique with $|k| + 2$ distinct vertices. In particular, if k is infinite, then $\Gamma_E(R \ltimes M)$ contains an infinite clique. It is straightforward to show that $R \ltimes M$ has length 6.

We conclude the example by showing that the rule of assignment $[r] \mapsto [(r, 0)]$ does not describe a well-defined function from the vertex set of $\Gamma_E(R)$ to the vertex set of $\Gamma_R(R \ltimes M)$. (Contrast this with Proposition 4.10.) As in Example 4.11, this follows from the next equalities

$$\operatorname{Ann}_R(x) = (x, y)R = \operatorname{Ann}_R(y)$$
$$\operatorname{Ann}_M(x) = (e, y^{-1})R \neq (e, x^{-1})R = \operatorname{Ann}_M(y)$$

by Fact 4.8 (i).

It is natural to ask whether the previous example is minimal, that is, if one can construct a ring R of length 5 or less such that $\Gamma_E(R)$ contains an infinite clique. Accordingly, we next characterize all graphs $\Gamma_E(R)$ such that $\operatorname{len}(R) \leq 3$, and we show that $\Gamma_E(R)$ cannot contain an infinite clique if $\operatorname{len}(R) \leq 4$. The length 5 case is still open; see Question 5.9 and Remark 5.10.

Proposition 5.3. *If* $\operatorname{len}(R) \leq 3$*, then* $\Gamma_E(R)$ *is finite. In particular:*

(i) *If* $\operatorname{len}(R) = 1$*, then* $\Gamma_E(R) = \emptyset$*.*

(ii) *If* $\operatorname{len}(R) = 2$*, then* $\Gamma_E(R)$ *is either a single edge or a single vertex.*

(iii) *If* $\operatorname{len}(R) = 3$*, then* $|\Gamma_E(R)| \leq 6$*; specifically, the graph* $\Gamma_E(R)$ *is*

    (a) *a triangle with three ends if R is a product of three fields;*

    (b) *a* path *of length 3 if R is a product of a field and a local ring of length 2, or*

    (c) *either a single edge or a single vertex if R is local.*

Proof. If $\operatorname{len}(R) = 1$, then R is a field and has no zero divisors. If $\operatorname{len}(R) = 2$, then R is either a product of two fields, or a local ring of length 2. If $R \cong K_1 \times K_2$, then $\Gamma_E(R)$ is the edge $[(1,0)] - [(0,1)]$. Otherwise, there is a complete discrete valuation ring (Q, τ) such that $R \cong Q/(\tau^2)Q$; in this case, every non-unit of R is a unit multiple of $\overline{\tau}$, so $\Gamma_E(R)$ is the single vertex $[\overline{\tau}]$.

Suppose $\operatorname{len}(R) = 3$. Then R is isomorphic to one of the following: (1) a product $K_1 \times K_2 \times K_3$ of three fields, (2) a product of a field K_1 with a local ring R_2 of length 2, or (3) a local ring.

(1) If $R \cong K_1 \times K_2 \times K_3$, then R has exactly eight ideals, including 0 and R itself, namely, the products of copies of 0 and the K_i's. Each of the six non-trivial ideals is the annihilator of an element (a, b, c) with $a, b, c = 0$ or 1. It is not difficult to see that the three vertices $[(1,0,0)]$, $[(0,1,0)]$, and $[(0,0,1)]$ are all adjacent, with ends $[(0,1,1)]$, $[(1,0,1)]$, and $[(1,1,0)]$, respectively; i.e., the graph is as described.

(2) Assume that $R \cong K_1 \times R_2$, where R_2 has length 2. Then there is a complete discrete valuation ring (Q, τ) such that $R \cong Q/(\tau^2)Q$, and $\Gamma_E(R)$ is the graph $[(0,1)] - [(1,0)] - [(0,\overline{\tau})] - [(1,\overline{\tau})]$.

(3) Assume that $(R, \mathfrak{m})$ is local of length 3, and let e be the embedding dimension of R, that is, the minimal number of generators of $\mathfrak{m}$. Since $\operatorname{len}(R) = 3$, we have $e = 1$ or $e = 2$. If $e = 1$, then there is a complete discrete valuation ring (Q, τ) such that $R \cong Q/(\tau^3)Q$, and $\Gamma_E(R)$ is the edge $[\overline{\tau}] - [\overline{\tau}^2]$. If $e = 2$, then the equalities $3 = \operatorname{len}(R) = \operatorname{len}(R/\mathfrak{m}) + \operatorname{len}(\mathfrak{m}/\mathfrak{m}^2) + \operatorname{len}(\mathfrak{m}^2)$ imply that $\mathfrak{m}^2 = 0$; it follows that $\operatorname{Soc}(R) = \mathfrak{m}$, and $\Gamma_E(R)$ is the single vertex $[x]$ for any $0 \neq x \in \mathfrak{m}$. $\qquad\square$

Remark 5.4. In general, if R is a product of n fields, then $\Gamma_E(R)$ will have $2^n - 2$ vertices and clique number n, corresponding to the n primes $K_1 \times \cdots \times \widehat{K_i} \times \cdots \times K_n$.

Proposition 5.5 (See [7, Theorem 3.8].). *If R is a reduced Noetherian ring, then* $\omega(\Gamma_E(R)) = |\operatorname{Ass}(R)| < \infty$.

Proof. Let R be a reduced Noetherian ring and let U be the set of non-zero divisors of R. Then $U^{-1}R$ is Noetherian and a finite product of fields $K_1 \times \cdots \times K_n$. Proposition 4.2 implies that $\Gamma_E(R) \cong \Gamma_E(U^{-1}R)$, so Remark 5.4 implies that $\omega(\Gamma_E(R)) = \omega(\Gamma_E(U^{-1}R)) = n = |\operatorname{Ass}(U^{-1}R)| = |\operatorname{Ass}(R)|$. □

Noting that a reduced ring contains no self-annihilating elements, we consider a relationship between clique size and self-annihilating elements.

Proposition 5.6. *Let S be clique in $\Gamma_E(R)$, and set $N = \{[r] \in S : r^2 \neq 0\}$ and $A = \{[a] \in S : a^2 = 0\}$. If $|S| \geq 3$ and $|N| \geq 2$, then $|\Gamma_E(R)| \geq |A| + 2^{|N|} - 1$.*

Proof. Suppose S is a clique in $\Gamma_E(R)$, and $X = \{x_1, \ldots x_k\} \subsetneq S$ with $k \geq 2$. Consider the element $x = x_1 + \cdots + x_k$. For any $y \in S - X$ we have $xy = \sum_{i=1}^{k} x_i y = 0$, while for $x_i \in X$, we have $xx_i = (x_1 + \cdots + x_k)x_i = x_i^2$, since $x_i x_j = 0$ for $i \neq j$. If no element of X is self-annihilating, then $[x]$ is not adjacent to any vertex of X, while $[x]$ is adjacent to all other vertices of S. So each such choice of X determines a unique vertex $[x]$ such that $[x] \notin S$. Letting $|N| = n$, there are $2^n - n - 1$ subsets of N with at least two elements, so we have at least $2^n - n - 1$ vertices of $\Gamma_E(R)$ which are not elements of S.

We now see

$$|\Gamma_E(R)| \geq |S| + (2^n - n - 1) = |A| + |N| + (2^n - n - 1) = |A| + 2^n - 1. \quad □$$

Corollary 5.7. *If a clique of $\Gamma_E(R)$ contains infinitely many elements which are not self-annihilating, then R is uncountable.*

The next result uses the following facts: an Artinian ring R is isomorphic to a finite product of Artinian local rings, and the length of R is the product of the lengths of the factors. We note that, except for the case (v)(c), all the graphs turn out to be finite. Also, by the notation edim we mean the embedding dimension.

Proposition 5.8. *Let R be a ring of length* 4.

(i) *If R is a product of four fields, then $\omega(\Gamma_E(R)) = 4$.*

(ii) *If R is a product of two fields and a local ring of length 2, then $\omega(\Gamma_E(R)) = 3$.*

(iii) *If R is a product of two local rings of length 2, then $\omega(\Gamma_E(R)) = 3$.*

(iv) *If R is a product of a field and a local ring R_2 of length 3, then:*

    (a) *If $\operatorname{edim}(R_2) = 1$, then $\omega(\Gamma_E(R)) = 3$; and*

    (b) *If $\operatorname{edim}(R_2) = 2$, then $\Gamma_E(R)$ is a $K_{1,2}$ star graph and has clique number 2.*

(v) *If R is local, we have the following:*

    (a) *If* $\mathrm{edim}(R) = 1$*, then* $\Gamma_E(R)$ *is a* $K_{1,2}$ *star graph and has clique number 2;*

    (b) *If* $\mathrm{edim}(R) = 3$*, then* $\Gamma_E(R)$ *is a single vertex; and*

    (c) *If* $\mathrm{edim}(R) = 2$*, then* $\Gamma_E(R)$ *can be infinite, but* $\omega(\Gamma_E(R)) \leq 3$*.*

Proof. (i) This is from Remark 5.4.

(ii) Assume that $R \cong K_1 \times K_2 \times R_3$ where K_1 and K_2 are fields and R_3 is a local ring of length 2. Then there is a complete discrete valuation ring (Q, τ) such that $R_3 \cong Q/(\tau^2)Q$. Note that the only ideals of R_3 are R_3, $\overline{\tau} R_3$, and 0.

It is straightforward to see that $\Gamma_E(R)$ contains a clique with vertices $[(1, 0, 0)]$, $[(0, 1, 0)]$, and $[(0, 0, 1)]$. (There are several other cliques on three vertices.) To show that $\Gamma_E(R)$ does not have a clique on four vertices, it suffices to show that it does not have four vertices of degree at least 4.

We claim that this graph consists of the following:

- two vertices of degree 5, namely $[(1, 0, 0)]$ and $[(0, 1, 0)]$;

- four vertices of degree 3, namely $[(0, 0, 1)]$, $[(0, 0, \overline{\tau})]$, $[(1, 0, \overline{\tau})]$, $[(0, 1, \overline{\tau})]$;

- one vertex of degree 2, namely $[(1, 1, 0)]$; and

- three vertices of degree 1, namely $[(1, 0, 1)]$, $[(0, 1, 1)]$, and $[(1, 1, \overline{\tau})]$.

For instance, to check that all the vertices of $\Gamma_E(R)$ are listed, observe that R has exactly twelve ideals, each of the form $I_1 \times I_2 \times I_3$, where I_j is an ideal of R_j for $j = 1, 2, 3$. Each of the non-trivial ideals is the annihilator ideal of a zero-divisor. For instance we have $0 \times K_2 \times \overline{\tau} R_3 = \mathrm{Ann}_R(1, 0, \overline{\tau})$. Checking that each vertex has the given degree is tedious but not difficult. For instance, the vertices adjacent to $[(1, 0, \overline{\tau})]$ are $[(0, 1, 0)]$, $[(0, 0, \overline{\tau})]$, and $[(0, 1, \overline{\tau})]$.

(iii) Assume that $R \cong R_1 \times R_2$ where R_1 and R_2 are local rings of length 2. Then there are complete discrete valuation rings (Q_i, τ_i) such that $R_i \cong Q_i/(\tau_i^2)Q$ for $i = 1, 2$. Each ring R_i has exactly three ideals, namely R_i, $\overline{\tau_i} R_i$, and 0. This implies that R has exactly nine ideals. Each of the seven non-trivial ideals is the annihilator ideal of a zero-divisor.

It is straightforward to see that $\Gamma_E(R)$ contains a clique with vertices $[(0, \overline{\tau_2})]$, $[(\overline{\tau_1}, \overline{\tau_2})]$, and $[(\overline{\tau_1}, 0)]$. This is actually the only clique on three vertices, and there are no cliques on four vertices, as one can see from the following sketch of $\Gamma_E(R)$:
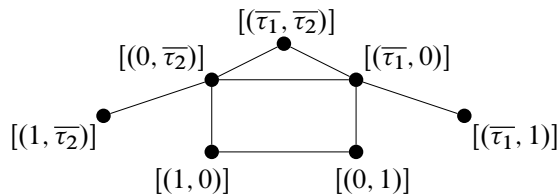
It follows readily that $\omega(\Gamma_E(R)) = 3$.

(iv) Assume that $R \cong K_1 \times R_2$ where K_1 is a field and R_2 is a local ring of length 3. Let e_2 be the embedding dimension of R_2, that is, the minimal number of generators of $\mathfrak{m}_2$. Since $\mathrm{len}(R_2) = 3$, we have $e_2 = 1$ or $e_2 = 2$.

If $e_2 = 1$, then there is a complete discrete valuation ring (Q, τ) such that $R_2 \cong Q/(\tau^3)Q$, and $\Gamma_E(R)$ is the following graph with $\omega(\Gamma_E(R)) = 3$:
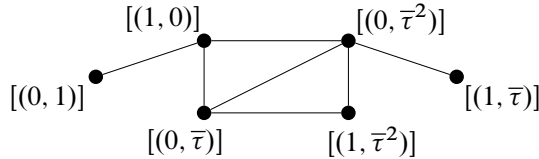
If $e_2 = 2$, then we have $\mathfrak{m}_2^2 = 0$, as in the proof of Proposition 5.3. It follows that $\mathrm{Soc}(R_2) = \mathfrak{m}_2$, so the graph $\Gamma_E(R)$ has the form $[(1,0)] - [(0,x)] - [(1,x)]$ for some (equivalently, any) $0 \neq x \in \mathfrak{m}_2$.

(v) Assume that R is local with $e = \mathrm{edim}(R)$. Since $\mathrm{len}(R) = 4$, we can have $e = 1, 2,$ or 3. If $e = 1$, then $R \cong Q/(\tau^4)$ where (Q, τ) is a discrete valuation ring; in this case, the graph $\Gamma_E(R)$ is $[\bar{\tau}] - [\bar{\tau}^3] - [\bar{\tau}^2]$. If $e = 3$, then $\mathfrak{m}^2 = 0$, as in the proof of Proposition 5.3; in this case, it follows that $\mathrm{Soc}(R) = \mathfrak{m}$ so $\Gamma_E(R)$ is the single vertex $[x]$ for some (equivalently, any) $0 \neq x \in \mathfrak{m}$.

Assume now that $e = 2$. The fact that $4 = \mathrm{len}(R) = \mathrm{len}(R/\mathfrak{m}) + \mathrm{len}(\mathfrak{m}/\mathfrak{m}^2) + \mathrm{len}(\mathfrak{m}^2/\mathfrak{m}^3) + \mathrm{len}(\mathfrak{m}^3)$ implies that $\mathfrak{m}^2$ is principal (and nonzero) and $\mathfrak{m}^3 = 0$.

We argue by cases.

Case 1: There is a generating sequence x, y of $\mathfrak{m}$ such that $x^2 \neq 0$, and $xy = y^2 = 0$. In this case, it follows readily that $\Gamma_E(R)$ is a single edge $[x] - [x^2]$, which has clique number 2.

Case 2: There is a generating sequence x, y of $\mathfrak{m}$ such that $x^2 \neq 0$, $y^2 \neq 0$, and $xy = 0$. In this case, we show that $\Gamma_E(R)$ can be infinite, but that $\omega(\Gamma_E(R)) = 3$.

Since $\mathfrak{m}^3 = 0$ and x^2, y^2 are non-zero, we conclude that x^2 and y^2 are each generators for the principal ideal $\mathfrak{m}^2$. It follows that there is a unit $u \in R$ such that $y^2 = ux^2$.

We claim that

$$\mathrm{Ann}_R(x^2) = \mathrm{Ann}_R(y^2) = \mathfrak{m}, \tag{5.8.1}$$

$$\mathrm{Ann}_R(x) = (y)R + \mathfrak{m}^2 = (y)R, \tag{5.8.2}$$

$$\mathrm{Ann}_R(y) = (x)R + \mathfrak{m}^2 = (x)R, \tag{5.8.3}$$

$$\mathrm{Ann}_R(x + ay) = (x - u^{-1}a^{-1}y)R + \mathfrak{m}^2 = (x - u^{-1}a^{-1}y)R, \tag{5.8.4}$$

where a is a unit in R.

(5.8.1) This follows from the fact that x^2 and y^2 are non-zero elements of $\mathfrak{m}^2$ and that $\mathfrak{m}^3 = 0$.

(5.8.2) Since $xy = 0$ and $\mathfrak{m}^2 = (y^2)R \subseteq (y)R$, it suffices to show that $\mathrm{Ann}_R(x) \subseteq (y)R + \mathfrak{m}^2$. Let $r \in \mathrm{Ann}_R(x)$. Since r is a non-unit, there are elements $s, t \in R$ such that $r = sx + ty$. Then we have

$$0 = xr = x(sx + ty) = sx^2.$$

If s were in $R \setminus \mathfrak{m}$, then s would be a unit, so the display would imply that $x^2 = 0$, a contradiction. Thus, we have $s \in \mathfrak{m}$ and so

$$r = sx + ty \in \mathfrak{m}x + (y)R \subseteq \mathfrak{m}^2 + (y)R$$

as desired.

(5.8.3) This is analogous to (5.8.2).

(5.8.4) First, we observe that

$$(x + ay)(x - u^{-1}a^{-1}y) = x^2 - u^{-1}y^2 = 0$$

since $y^2 = ux^2$. Next, we note that $x(x - u^{-1}a^{-1}y) = x^2$; it follows that $\mathfrak{m}^2 = (x^2)R \subseteq (x - u^{-1}a^{-1}y)R$. Thus, it remains to show the reverse containment. Let $r \in \mathrm{Ann}_R(x + ay)$, and write $r = sx + ty$ for $s, t \in R$. Then we have

$$0 = (x + ay)r = (x + ay)(sx + ty) = sx^2 + aty^2 = sx^2 + atux^2 = (s + atu)x^2.$$

It follows that $s + atu \in \mathrm{Ann}_R(x^2) = \mathfrak{m} = (x, y)R$, so there are elements $b, c \in R$ such that $s + atu = bx + cy$. We then have

$$sx + ty = -atux + bx^2 + cxy + ty = -atux + bx^2 + ty$$
$$= -tau(x - a^{-1}u^{-1}y) + bx^2 \in (x - u^{-1}a^{-1}y)R + \mathfrak{m}^2$$

as desired.

Next, we observe that the vertices of $\Gamma_E(R)$ are of the following form: $[x^2]$, $[x]$, $[y]$, or $[x + ay]$ for some unit $a \in R$. Let r be a non-zero non-unit of R. Then r is of the form $r = sx + ty$ with $s, t \in R$. If $s, t \in \mathfrak{m}$, then $r \in \mathfrak{m}^2 = \mathrm{Soc}(R)$, so we have $[r] = [x^2]$. If $s \in \mathfrak{m}$ and $t \in R \setminus \mathfrak{m}$, then $sx \in \mathfrak{m}^2 = \mathrm{Soc}(R)$ so $[r] = [sx + ty] = [ty] = [y]$ since t is a unit in R. Similarly, if $s \notin \mathfrak{m}$ and $t \in \mathfrak{m}$, then $[r] = [x]$. The last remaining case has $s, t \in R \setminus \mathfrak{m}$, that is, they are both units, so we have $[r] = [sx + ty] = [x + s^{-1}ty]$.

Since $\mathfrak{m}^3 = 0$, we see that every vertex $v \neq [x^2]$ is adjacent to $[x^2]$. Also, the vertices $[x]$ and $[y]$ are adjacent, so the vertices $[x^2]$, $[x]$, and $[y]$ form a triangle in $\Gamma_E(R)$, i.e., a clique of size 3. Thus, we need to show that $\Gamma_E(R)$ does not have a clique of size 4. To this end, it suffices to note that the equations (5.8.1)–(5.8.4) show that every vertex $v \neq [x^2]$ in $\Gamma_E(R)$ has degree at most 3, so this graph can not have a clique of size 4. This concludes the proof in Case 2.

Case 3: There is a generating sequence x, y of $\mathfrak{m}$ such that $x^2 \neq 0$ and $xy \neq 0$. In this case, a change of variables reverts back to Case 1 or 2. Specifically, since $\mathfrak{m}^2$ is principal and x^2, xy are non-zero, we have $(x^2)R = \mathfrak{m} = (xy)$. Write $xy = vx^2$ for some unit $v \in R$, and set $\tilde{y} = y - vx$. Then $x^2 \neq 0$ and $x\tilde{y} = xy - vx^2 = 0$, so we revert back to Case 1 or 2, depending on whether or not $(\tilde{y})^2 = 0$.

Case 4: Since all the previous arguments deal with the case where an element in a generating sequence is not square zero, we are reduced to the assumption that any element in a generating sequence *is* square zero. Moreover, if an element in $\mathfrak{m}$ is not a minimal generator, then as a member of $\mathfrak{m}^2$, its square is also zero since $\mathfrak{m}^3 = 0$. Thus, in this case we assume that $s^2 = 0$ for all $s \in \mathfrak{m}$. We will show that $\Gamma_E(R)$ is a *non-degenerate star*, in which case $\omega(\Gamma_E(R)) = 2$. Our assumptions imply that for any generating sequence x, y of $\mathfrak{m}$, we have $x^2 = y^2 = 0$, but $xy \neq 0$ since $\mathfrak{m}^2 \neq 0$. It follows that $\mathfrak{m}^2 = (xy)R$. Note that

$$0 = (x + y)^2 = x^2 + 2xy + y^2 = 2xy.$$

If 2 is a unit, then $xy = 0$, contradicting the fact that $0 \neq \mathfrak{m}^2 = (xy)R$. Thus, $2 \in \mathfrak{m}$, and hence $4 = 2^2 = 0$ in R. There are the following two possibilities:

Case 4a: $2 = 0$ in R. In this case, the ring R has characteristic 2, so R contains a field of characteristic 2. Since R is Artinian, it is complete, so it contains a subfield $k_0 \subseteq R$ such that $k_0 \cong k$. Cohen's structure theorem implies that there is a ring epimorphism $\tau \colon k_0[\![X, Y]\!] \twoheadrightarrow R$ given by $X \mapsto x$ and $Y \mapsto y$. Since $x^2 = 0 = y^2$, we conclude that $X^2, Y^2 \in \mathrm{Ker}(\tau)$, so there is an induced epimorphism $\tau' \colon k_0[\![X, Y]\!]/(X^2, Y^2) \twoheadrightarrow R$. Since $\mathrm{len}(k_0[\![X, Y]\!]/(X^2, Y^2)) = 4 = \mathrm{len}(R)$, the map τ' is an isomorphism $R \cong k_0[\![X, Y]\!]/(X^2, Y^2) \cong k_0[X, Y]/(X^2, Y^2)$. Example 3.28 implies that $\Gamma_E(R)$ is a non-degenerate star.

Case 4b: $2 \neq 0$ in R.

Case 4b(i): 2 is a minimal generator for $\mathfrak{m}$. In this case, Cohen's structure theorem implies that there is a complete discrete valuation ring $(Q, 2Q, k)$ and an epimorphism $\tau \colon Q[\![Y]\!] \twoheadrightarrow R$ such that $\mathfrak{m} = (2, \tau(Y))R$. Since $2^2 = 0 = \tau(Y)^2$ in R, it follows that $4, Y^2 \in \mathrm{Ker}(\tau)$. Thus, the induced epimorphism $\tau' \colon Q[\![Y]\!]/(4, Y^2) \twoheadrightarrow R$ is an isomorphism, as $\mathrm{len}(R) = 4 = \mathrm{len}(Q[\![Y]\!]/(4, Y^2))$. It follows that we have $R \cong Q[\![Y]\!]/(4, Y^2) \cong Q[Y]/(4, Y^2)$. Thus, Example 3.29 implies that $\Gamma_E(R) \cong \Gamma_E(Q[Y]/(4, Y^2))$ is a non-degenerate star.

Case 4b(ii): 2 is not a minimal generator for $\mathfrak{m}$. In this case, we have $2 \in \mathfrak{m}^2$. Cohen's structure theorem implies that there is a complete discrete valuation ring $(Q, 2Q, k)$ and an epimorphism $\tau \colon Q[\![X, Y]\!] \twoheadrightarrow R$ such that $\mathfrak{m} = (\tau(X), \tau(Y))R$. Set $x = \tau(X)$ and $y = \tau(Y)$. Since $x^2 = 0 = y^2 = 4$ in R, it follows that $2 \in \mathfrak{m}^2 = (xy)R$. Writing $2 = axy$ for some element $a \in R$, we see that a must be a unit in R; if not, then $a \in \mathfrak{m}$ and so $2 = axy \in \mathfrak{m}^3 = 0$, a contradiction. Define $\tau' \colon Q[\![X, Y]\!] \to R$ by sending $X \mapsto ax$ and $Y \mapsto y$. Then τ' is also a ring epimorphism with the added advantage of satisfying $2 = \tau'(X)\tau'(Y)$ in R.

It follows that $2 - XY \in \mathrm{Ker}(\tau')$. As $\tau'(X)^2 = 0 = \tau'(Y)^2 = 4$ in R, we have $X^2, Y^2, 4 \in \mathrm{Ker}(\tau')$. The facts $2 \in \mathfrak{m}^2$ and $\mathfrak{m}^3 = 0$ imply that $2\tau'(X) = 0 = 2\tau'(Y)$, so $2X, 2Y \in \mathrm{Ker}(\tau')$. In summary, we have $(4, X^2, Y^2, 2X, 2Y, 2 - XY) \subseteq \mathrm{Ker}(\tau')$. We conclude that $R \cong Q[\![X, Y]\!]/(4, X^2, Y^2, 2X, 2Y, 2 - XY)$, because $\mathrm{len}(Q[\![X, Y]\!]/(4, X^2, Y^2, 2X, 2Y, 2 - XY)) = 4$; see Example 3.30. From this example, we also know that $\Gamma_E(R)$ is a non-trivial star. $\qquad\square$

Question 5.9. Is there an Artinian ring R with $\mathrm{len}(R) = 5$ and $\omega(\Gamma_E(R)) = \infty$?

Remark 5.10. Working as in the proof of Proposition 5.8, one readily reduces Question 5.9 to the case where R is local with $\mathrm{edim}(R) = 2$ or 3.

6 Girth and Cut Vertices

Assume throughout this section that R is a Noetherian ring.

In this section we continue the investigation started in [35] into the graph theoretic properties satisfied by $\Gamma_E(R)$. One of our primary tools is the behavior of the associated primes of R as represented in $\Gamma_E(R)$; see Proposition 6.1 (ii). We prove that the *girth* of $\Gamma_E(R)$ is no more than 3 when finite. On the other hand, there is no similar bound on the *circumference* of $\Gamma_E(R)$. We also consider *cut vertices* in the graph.

6.1 Girth

We begin by listing several known results, some of which follow from direct proof on zero divisor graphs of rings, and others that are from results on semigroups. Some of the results in this section have a lot in common with work on Anderson and Livingston's graph $\Gamma(R)$. Therefore, where applicable, we point out the relevant papers.

Proposition 6.1.

(i) [17, Theorem 1]. *If $[x]$ and $[y]$ are non-adjacent vertices of $\Gamma_E(R)$, then the closed neighborhood of the vertex $[xy]$ contains the neighborhoods of $[x]$ and $[y]$; i.e., $\mathcal{N}([x]) \cup \mathcal{N}([y]) \subseteq \overline{\mathcal{N}([xy])}$.*

(ii) [35, Lemma 1.2]. *If $x, y \in R$ such that $\mathrm{Ann}_R(x)$ and $\mathrm{Ann}_R(y)$ are distinct associated primes of R, then $[x]$ and $[y]$ are adjacent in $\Gamma_E(R)$. If $[v]$ is a vertex of $\Gamma_E(R)$, then either $\mathrm{Ann}_R(v) \in \mathrm{Ass}(R)$ or there is a vertex $[w]$ adjacent to $[v]$ such that $\mathrm{Ann}_R(w) \in \mathrm{Ass}(R)$.*

(iii) [19, Theorem 1.6; 29, (2.4)]. *If $[v] \in \Gamma_E(R)$ is contained in a cycle, then it is contained in a cycle of length 3 or 4. In particular, if $\mathrm{girth}(\Gamma_E(R))$ is finite, then $\mathrm{girth}(\Gamma_E(R)) \leq 4$.*

(iv) [18, Theorem 1.5]. *If $\mathrm{girth}(\Gamma_E(R)) < \infty$, then each $[v] \in \Gamma_E(R)$ is either an end or is contained in some cycle.*

Proposition 6.2. (Compare to [1, Remark 2.7].) *Any vertex* $[x]$ *of* $\Gamma_E(R)$ *such that* $\mathrm{Ann}_R(x) \in \mathrm{Ass}(R)$ *dominates the edges of* $\Gamma_E(R)$. *That is, for every edge in* $\Gamma_E(R)$, *at least one end of that edge is in* $\overline{\mathcal{N}([x])}$. *Moreover, every vertex* $[y] \neq [x]$ *such that* y *is nilpotent is adjacent to* $[x]$.

Proof. This follows immediately from the fact that $yz = 0 \in \mathfrak{p}$ for all $\mathfrak{p} = \mathrm{Ann}(x) \in \mathrm{Ass}(R)$ forces y or z to be in $\mathrm{Ann}(x)$. $\qquad\qquad\qquad\qquad\square$

Corollary 6.3. *If* $|\Gamma_E(R)| > 3$ *and the graph has at least one vertex* $[x]$ *with two or more ends, then*

(i) $\mathrm{Ass}(R) = \{\mathrm{Ann}_R(x)\}$;

(ii) *every vertex* $[y] \neq [x]$ *must be adjacent to* $[x]$; *in particular,*

    (a) $\deg([x]) = |\Gamma_E(R)| - 1$ *if* $|\Gamma_E(R)|$ *is finite, and*

    (b) *no vertex other than* $[x]$ *can have an end.*

Proof. Let $[x]$ be a vertex of $\Gamma_E(R)$ that has (at least) two ends $[y_1], [y_2]$. Since $\Gamma_E(R)$ has at least four vertices, it follows from [35, Proposition 3.2] that $\mathrm{Ann}_R(y_1)$ and $\mathrm{Ann}_R(y_2)$ are not prime. Proposition 6.1 (ii) implies that there is an associated prime $\mathfrak{p} = \mathrm{Ann}_R(z)$ such that $[z] \in \mathcal{N}([y_1])$; since $[y_1]$ is an end for $[x]$, we have $[x] = [z]$, so $\mathrm{Ann}_R(x) = \mathfrak{p} \in \mathrm{Ass}(R)$.

Since $[y_1]$ and $[y_2]$ are ends for $[x]$, we conclude that either $y_1^2 = 0$ or $y_2^2 = 0$; if not, we would have $\mathrm{Ann}_R(y_1) = \mathrm{Ann}_R(y_2)$, contradicting the assumption $[y_1] \neq [y_2]$. Assume by symmetry that $y_1^2 = 0$.

Let $\mathrm{Ann}(w) \in \mathrm{Ass}(R)$. Proposition 6.2 implies that $[y_1]$ is adjacent to $[w]$, so the fact that $[y_1]$ is an end for $[x]$ implies that $[x] = [w]$, and so $\mathrm{Ann}(x) = \mathrm{Ann}(w)$. That is, we have $\mathrm{Ass}(R) = \{\mathrm{Ann}(x)\}$. This explains (i), and Proposition 6.1 (ii) implies that every vertex $[v] \neq [x]$ must be adjacent to $[x]$. From this, part (ii) is immediate. $\quad\square$

Proposition 6.4 (Compare to [19, Theorem 1.12].). *If* $\Gamma_E(R)$ *is acyclic, then it is a star graph or a path of length* 3.

Proof. If $|\mathrm{Ass}(R)| \geq 3$ then the clique of associated primes contains a cycle; see Proposition 6.1 (ii). Thus, we have $|\mathrm{Ass}(R)| \leq 2$. Since the graph is acyclic and each vertex is adjacent to some associated prime, every vertex not in $\mathrm{Ass}(R)$ must be an end. In the case that one of the associated primes has two ends, then by Corollary 6.3, we have $|\mathrm{Ass}(R)| = 1$, and hence every vertex in the graph is adjacent to a single central vertex; i.e., the graph is a star. In the case that each associated prime has at most one end, $\Gamma_E(R)$ is a path. (Note that if $|\Gamma_E(R)| < 4$, the path is also a star.) $\quad\square$

Proposition 6.5 (Compare to [1, Theorems 2.6 and 2.8, Corollary 2.2].).

(i) *If* $|\mathrm{Ass}(R)| = 1$, *then either* $\mathrm{girth}(\Gamma_E(R)) = \infty$ *or* $\mathrm{girth}(\Gamma_E(R)) = 3$. *Moreover,* $\mathrm{diam}(\Gamma_E(R)) \leq 2$.

(ii) *If* $|\mathrm{Ass}(R)| \geq 3$, *then* $\mathrm{girth}(\Gamma_E(R)) = 3$.

Proof. Note that (ii) follows immediately from Proposition 6.1 (ii) since all elements in $\text{Ass}(R)$ are adjacent. Thus, suppose $\mathfrak{p} = \text{Ann}(x)$ is the unique associated prime of R. Every vertex $[v] \neq [x]$ is adjacent to $[x]$ by Proposition 6.1 (ii), hence the diameter is at most 2. Moreover, $\Gamma_E(R)$ is either a star graph, in which case $\text{girth}(\Gamma_E(R)) = \infty$, or there is at least one additional edge, in which case $\text{girth}(\Gamma_E(R)) = 3$. $\qquad\square$

Theorem 6.6. *If the girth of $\Gamma_E(R)$ is finite, then it is 3.*

Proof. Applying Proposition 6.1 (iii), we assume that $\text{girth}(\Gamma_E(R)) = 4$ and obtain a contradiction. We claim that we may assume $|\Gamma_E(R)| \geq 6$. Zero divisor graphs with exactly five vertices are the subject of [25], where it is shown that in the four realizable graphs the girth is either infinite or 3. Likewise, of the six connected graphs on exactly four vertices, only three can be realized as $\Gamma_E(R)$ by [35, Propositions 1.5 and 1.7], and the girth is either infinite or 3. Clearly no graph with less than four vertices can have girth 4. Thus, assume $|\Gamma_E(R)| \geq 6$.

By Proposition 6.5, there are exactly two associated primes, say $\mathfrak{p}_1 = \text{Ann}_R(x_1)$ and $\mathfrak{p}_2 = \text{Ann}_R(x_2)$. Proposition 6.1 (ii) implies that $[x_1]$ and $[x_2]$ are adjacent. Quite a bit of information can be deduced from Proposition 6.2 since we are assuming that $\Gamma_E(R)$ has no three cycles.

For instance, we claim that no vertex in $\Gamma_E(R)$, except possibly $[x_1]$ or $[x_2]$, is represented by a self-annihilating element. To see this, let $[y] \in \Gamma_E(R) \setminus \{[x_1], [x_2]\}$ and suppose that $y^2 = 0$. Then $y \in \mathfrak{p}_1 \cap \mathfrak{p}_2$, i.e., $[y] \in \mathcal{N}([x_1]) \cap \mathcal{N}([x_2])$, resulting in the 3-cycle $[y] - [x_1] - [x_2] - [y]$.

Using similar reasoning, we show that no pair of distinct classes in $\mathcal{N}([x_i])$ can be adjacent. We argue for $i = 1$; the case $i = 2$ is by symmetry. Suppose that $[v]$ and $[w]$ are adjacent vertices in $\mathcal{N}([x_1])$. If $[v] \neq [x_2] \neq [w]$, then the condition $vw = 0$ implies that $v \in \mathfrak{p}_2$ or $w \in \mathfrak{p}_2$; hence, either $[v]$ or $[w]$ is in $\mathcal{N}([x_2])$, forming a 3-cycle with $[x_1]$ and $[x_2]$, a contradiction. Thus, either $[v]$ or $[w]$ is equal to $[x_2]$, say $[w] = [x_2]$. Then the condition $vw = 0$ implies that $v \in \text{Ann}_R(w) = \text{Ann}_R(x_2)$, so we have the 3-cycle $[v] - [x_1] - [x_2] - [v]$, another contradiction.

Next, we show that, given an edge $[a] - [b]$ such that $\{[a], [b]\} \cap \{[x_1], [x_2]\} = \emptyset$, we have a 4-cycle $[a] - [x_i] - [x_j] - [b]$. Since $[a] \notin \{[x_1], [x_2]\}$, Proposition 6.1 (ii) implies that $[a]$ is adjacent to $[x_i]$ for some i. Similarly $[b]$ is adjacent to either $[x_i]$ or $[x_j]$ where $j \neq i$. If $[b]$ is adjacent to $[x_i]$, then we would have the 3-cycle $[a] - [x_i] - [b]$, a contradiction. Thus $[b]$ is adjacent to $[x_j]$, and we have the 4-cycle $[a] - [x_i] - [x_j] - [b] - [a]$.

Next, we show that $\Gamma_E(R)$ has a 4-cycle containing $[x_1]$ and $[x_2]$. For this, it suffices to show that $\Gamma_E(R)$ contains an edge $[a] - [b]$ in $\Gamma_E(R)$ such that $\{[a], [b]\} \cap \{[x_1], [x_2]\} = \emptyset$, by the previous paragraph. Each $[x_i]$ has at most one end. Since $|\Gamma_E(R)| \geq 6$ this implies that there is a vertex $[a] \notin \{[x_1], [x_2]\}$ that is not an end. Proposition 6.1 (ii) implies that $[a]$ is adjacent to $[x_i]$ for some i. Since $[a]$ is not an end, there is a vertex $[b] \neq [x_i]$ adjacent to $[a]$. Note that $[b] \neq [x_j]$: if $[b] = [x_j]$,

then we would have the 3-cycle $[a] - [x_i] - [x_j] = [b] - [a]$, a contradiction. Thus, the edge $[a] - [b]$ provides the desired 4-cycle.

Note also that Corollary 6.3 implies that each $[x_i]$ can have at most one end $[v_i]$, which (by the third paragraph of this proof) necessarily satisfies $v_i^2 \neq 0$.

Next, consider the relationship between $\mathfrak{p}_1$ and $\mathfrak{p}_2$, and suppose $\mathfrak{p}_i \subsetneq \mathfrak{p}_j$. If there is some $[y] \in \mathcal{N}([x_i]) \setminus \{[x_j]\}$, then there is the 3-cycle $[y] - [x_1] - [x_2] - [y]$. Thus, all the remaining vertices must be in $\mathcal{N}([x_j]) \setminus \mathcal{N}([x_i])$. But this is impossible, since if $[y]$ and $[z]$ are two such vertices, then they can not be adjacent to one another or $[x_i]$, and hence must both be ends of $[x_j]$, contradicting Corollary 6.3. Thus, both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are maximal elements in the family of annihilator ideals of R.

Next, we show that each vertex in $\mathcal{N}([x_i]) \setminus \{[x_j]\}$ that is not an end must be part of a 4-cycle with the edge $[x_1] - [x_2]$ and some vertex in $\mathcal{N}([x_j]) \setminus \{[x_i]\}$. Indeed, let $[v] \in \mathcal{N}([x_i]) \setminus \{[x_j]\}$ such that $[v]$ is not an end. Since $[v]$ is adjacent to $[x_i]$, and $[v]$ is not an end, there is another vertex $[w] \neq [x_i]$ adjacent to $[v]$. If $[w] = [x_j]$, then we have a 3-cycle $[v] - [w] = [x_j] - [x_i] - v$, a contradiction. So we have $[w] \neq [x_j]$. Thus there is an edge $[v] - [w]$ such that $\{[v], [w]\} \cap \{[x_1], [x_2]\} = \emptyset$, so the fifth paragraph of this proof provides a 4-cycle $[v] - [x_i] - [x_j] - [w] - [v]$.

The diagram below summarizes the paragraphs above and demonstrates what general form $\Gamma_E(R)$ must take: (1) $[x_1]$ and $[x_2]$ are adjacent and are part of a 4-cycle with every edge disjoint from the edge $[x_1] - [x_2]$; (2) each $[x_i]$ has at most one end; (3) any vertex in $\mathcal{N}([x_i]) \setminus \{[x_j]\}$ that is not an end must be part of a 4-cycle with $[x_1], [x_2]$, and some vertex in $\mathcal{N}([x_j]) \setminus \{[x_i]\}$; and (4) there is at least one 4-cycle on the graph.
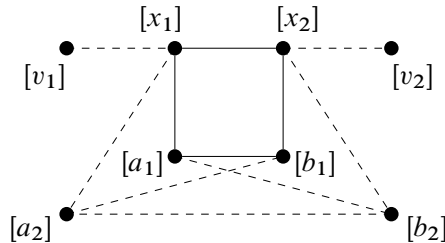
Let $\mathcal{A}$ be the set of all elements in $\mathcal{N}([x_1]) \setminus \{[x_2]\}$ which are not ends; i.e., each class $[a_i] \in \mathcal{A}$ is adjacent to some element(s) in $\mathcal{N}([x_2]) \setminus \{[x_1]\}$. Likewise, let $\mathcal{B}$ be the set of all elements $[b_j]$ in $\mathcal{N}([x_2]) \setminus \{[x_1]\}$ which are not ends.

Suppose there exist distinct classes $[a_1], [a_2] \in \mathcal{A}$. If $\mathcal{N}([a_1]) = \mathcal{N}([a_2])$, then a_1 and a_2 have the same annihilators, since $a_i^2 \neq 0$, so $[a_1] = [a_2]$, a contradiction. Assume by symmetry that we have $\mathcal{N}([a_2]) \not\subseteq \mathcal{N}([a_1])$, and let $[b_2] \in \mathcal{N}([a_2]) \setminus \mathcal{N}([a_1])$. Also, let $[b_1] \in \mathcal{N}([a_1])$. Thus, we have $[b_1], [b_2] \in \mathcal{B}$ such that $a_1 b_1 = 0 = a_2 b_2$ and $a_1 b_2 \neq 0$. Then $\mathcal{N}([a_1]) \cup \mathcal{N}([b_2]) \subseteq \mathcal{N}([a_1 b_2]) \subseteq \mathcal{N}([x_i])$ for some i, where the first containment is Proposition 6.1 (i), and the second follows from the fact that every annihilator ideal, in particular $\mathrm{Ann}_R(a_1 b_2)$, is contained in a maximal element of the family of annihilator ideals, hence either $\mathrm{Ann}_R(x_1)$ or $\mathrm{Ann}_R(x_2)$. Suppose $\mathrm{Ann}_R(a_1 b_2) \subseteq \mathrm{Ann}_R(x_1)$. Then $[b_1] \in \mathcal{N}([a_1]) \subseteq \mathcal{N}([x_1])$, translates into the 3-

cycle $[x_1] - [b_1] - [x_2] - [x_1]$, a contradiction. Likewise, if $\text{Ann}_R(a_1 b_2) \subseteq \text{Ann}_R(x_2)$, then $[a_2] \in \mathcal{N}([b_2]) \subseteq \mathcal{N}([x_2])$ translates into the 3-cycle $[x_1] - [a_2] - [x_2] - [x_1]$. Thus, assuming that $|\mathcal{A}| \geq 2$, which forces $|\mathcal{B}| \geq 2$, leads to a contradiction. By symmetry, assuming that $|\mathcal{B}| \geq 2$ forces $|\mathcal{A}| \geq 2$ and leads to a contradiction. Therefore, we must have $|\mathcal{A}| = |\mathcal{B}| = 1$, say $\mathcal{A} = \{[a_1]\}$ and $\mathcal{B} = \{[b_1]\}$, where $a_1 b_1 = 0$; i.e., there is exactly one 4-cycle in the graph. Next, recall that $|\Gamma_E(R)| \geq 6$. Based on the above arguments and assumptions, it follows that $|\Gamma_E(R)|$ must be exactly 6, and that $[x_1]$ and $[x_2]$ each have an end $[v_1]$, $[v_2]$, respectively.

Consider $v_1 v_2$, which is a zero divisor annihilated by x_1 and x_2. If $[v_1 v_2]$ is not $[x_1]$ or $[x_2]$, then the graph has the 3-cycle $[x_1] - [v_1 v_2] - [x_2] - [x_1]$, a contradiction. Thus, we have $[v_1 v_2] = [x_i]$ for some i. Without loss of generality, assume that $[v_1 v_2] = [x_1]$. Since $x_1 \in \text{Ann}_R(v_1 v_2) = \text{Ann}_R(x_1)$, it follows that $x_1^2 = 0$. Recall that $v_1^2, v_2^2 \neq 0$. In the graph we have $[v_1 v_2] = [x_1] - [v_1]$, so $v_1^2 v_2 = 0$ and $v_1^2 v_2^2 = 0$. However, since $[x_1] = [v_1 v_2]$ is not adjacent to $[v_2]$, we have $v_1 v_2^2 \neq 0$. Since $[v_2]$ is an end for $[x_2]$ and $v_1^2 v_2 = 0 \neq v_1^2$, we have $[v_1^2] = [x_2]$.

Now consider $a_1 + x_1$, which is annihilated by x_1, but not by $v_1, a_1, b_1,$ or x_2. Thus, $[a_1 + x_1] = [v_1]$. Note that $(a_1 + x_1)^2 = a_1^2$, hence $[a_1^2] = [v_1^2] = [x_2]$; this follows from the readily verified fact that $\text{Ann}_R(a_1) = \text{Ann}_R(v_1)$ implies that $\text{Ann}_R(a_1^2) = \text{Ann}_R(v_1^2)$. Thus, we have $a_1^2 v_2 = 0$, so $a_1 v_2$ is annihilated by $a_1, x_1, x_2,$ and b_1. As there is no such class and $a_1 v_2$ can not be zero, this is the final contradiction. □

Remark 6.7. To contrast the above results, note that Proposition 6.1 (iii) does not force every 5-cycle to have a chord. In fact, it does not preclude the existence of arbitrarily long cycles without chords. For example, for $n \geq 4$, the graph of the Noetherian ring $R = \mathbb{F}_2[X_1, \ldots, X_n]/(X_1 X_2, X_2 X_3, \ldots, X_{n-1} X_n, X_n X_1)$ has a C_n subgraph of $[X_1] - [X_2] - \cdots - [X_{n-1}] - [X_n] - [X_1]$ with no chord; i.e., circumference$(\Gamma_E(R)) \geq n$. On the other hand, girth$(\Gamma_E(R)) = 3$ by Theorem 6.6.

6.2 Cut Vertices

Cut vertices in Anderson and Livingston's graph $\Gamma(R)$ are investigated in [11].

Lemma 6.8. *If* $\text{Ass}(R) = \{\text{Ann}(v)\}$*, then* $v^2 = 0$*.*

Proof. The assumption $\text{Ass}(R) = \{\text{Ann}(v)\}$ implies that $\text{Ann}(v) = Z^*(R) \cup \{0\}$, hence $v \in \text{Ann}(v)$. □

In part (iii) of the next result, we employ the following terminology: Let A and B be disjoint sets of vertices of a graph G. We say that a vertex v of $G \setminus (A \cup B)$ *separates* A and B if for all $a \in A$ and all $b \in B$ every path from a to b in G passes through v.

Proposition 6.9. *Suppose* v *is a cut vertex in* $\Gamma_E(R)$*. Then* $\text{Ann}(v)$ *is an associated prime of R. Moreover,*

(i) *if v has at least two ends, then* $\mathrm{Ass}(R) = \{\mathrm{Ann}(v)\}$;

(ii) *if v does not have an end, then* $\mathrm{Ass}(R) = \{\mathrm{Ann}(v)\}$;

(iii) *if v separates subsets* $\{[a], [a']\}$ *and* $\{[b], [b']\}$ *where* $[a], [a'], [b], [b']$ *are distinct vertices satisfying* $aa' = 0$ *and* $bb' = 0$, *then* $\mathrm{Ass}(R) = \{\mathrm{Ann}(v)\}$.

Proof. Let $[v]$ be a cut vertex in $\Gamma_E(R)$, in which case there are at least three vertices in the graph. If $[v]$ has an end, then $\mathrm{Ann}(v)$ is an associated prime by [35, Corollary 3.3], and (i) follows from Corollary 6.3. If $[v]$ does not have an end, then it is straightforward to show that the hypotheses of part (iii) are satisfied. Thus, it remains to prove part (iii).

(iii) Assume that v separates subsets $\{[a], [a']\}$ and $\{[b], [b']\}$ where $[a], [a'], [b], [b']$ are distinct vertices satisfying $aa' = 0$ and $bb' = 0$. Suppose that there is an associated prime $\mathrm{Ann}(w) \neq \mathrm{Ann}(v)$. (Note that we do not yet know that $\mathrm{Ann}(v)$ is prime.) Since the elements of $\mathrm{Ass}(R)$ dominate the edges of the graph, at least one of $[a]$, $[a']$ is adjacent to $[w]$, and at least one of $[b]$, $[b']$ is adjacent to $[w]$. This provides a path from $[a]$ to $[b]$ via $[w]$ avoiding $[v]$, a contradiction. Thus, $\mathrm{Ann}(v)$ is the only ideal that might be an associated prime of R. Since R has an associated prime, the ideal $\mathrm{Ann}(v)$ is therefore the unique associated prime of R. $\square$

Corollary 6.10. *If* $[v]$ *satisfies the hypotheses of Proposition* 6.9 (iii)*, and* $|\Gamma_E(R)| < \infty$*, then* $\deg([v]) > \deg([u])$ *for all* $[u] \in \Gamma_E(R)$.

Proof. If $\Gamma_E(R)$ is finite with $n + 1$ vertices, then Propositions 6.1 (ii) and 6.9 (iii) show that $\deg([v]) = n$. (Recall that no vertex is adjacent to itself.) Given any other $[u] \in \Gamma_E(R)$, the cut vertex $[v]$ must separate $[u]$ from some vertex $[w]$. So $[u]$ is not adjacent to all other vertices, and hence $\deg([u]) < n$. $\square$

Example 6.11. The graph shown below on the left can not be the $\Gamma_E(R)$ for a ring R as per the Proposition; on the other hand, the graph on the right is $\Gamma_E(R)$ for $R = (\mathbb{Z}/3\mathbb{Z})[\![X, Y]\!]/(XY, X^3, Y^3, X^2 - Y^2)$, where lower case letters represent the cosets of the upper case letters in the quotient ring; see [35, Example 3.9].
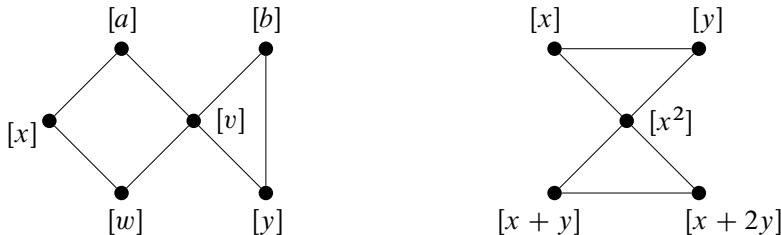
The converse to Proposition 6.9 is not true; i.e., an associated prime need not be a cut vertex, even when R is finite, as the next example shows.

Example 6.12. In the ring $R = \mathbb{F}_2[X, Y, Z]/(X^2, Y^2, Z^2)$, the ideal $\mathrm{Ann}_R(xyz) = (x, y, z)R$ is the unique associated prime ideal, but not a cut vertex. To see this,

note first that the only elements $v \in R$ such that $\operatorname{Ann}_R(v) = \operatorname{Ann}_R(xyz)$ are the non-zero scalar multiples of xyz. Write R as $A[Z]/(Z^2) \cong A \ltimes A$ where $A = \mathbb{F}_2[X, Y]/(X^2, Y^2)$. Let $r = f_0(x, y) + f_1(x, y) \cdot z$ and $s = g_0(x, y) + g_1(x, y) \cdot z$ be two non-equivalent zero divisors, where the constant coefficients of f_0, g_0 are necessarily zero. Assume that $[r] \neq [xyz] \neq [s]$. We show that $[r]$ and $[s]$ are connected by a path not containing $[xyz]$.

If both f_0 and g_0 have a linear term, then $[r]$ and $[s]$ are connected by the path $[r] - [f_0 z] - [g_0 z] - [s]$. Note that the assumptions on f_0 and g_0 imply that $[f_0 z] \neq [xyz] \neq [g_0 z]$. Also, the vertices $[f_0 z]$ and $[g_0 z]$ may be distinct or not, so this path has length 2 or 3.

If f_0 does not have a linear term (e.g., if $f_0 = 0$) and g_0 does have a linear term, then we use the path $[r] - [xz] - [g_0 z] - [s]$. If f_0 does have a linear term and g_0 does not have a linear term (e.g., if $g_0 = 0$), then we use the path $[r] - [f_0 z] - [xz] - [s]$. If f_0 and g_0 do not have linear terms, then we use the path $[r] - [xz] - [s]$.

7 Chromatic Numbers and Clique Numbers

Assume throughout this section that R is a Noetherian ring.

As mentioned in the survey, the origin of research in the theory of zero divisor graphs involved their chromatic numbers. It is important to note that D. D. Anderson and M. Naseer's [4] counterexample to Beck's conjecture that the chromatic and clique numbers of $G(R)$ are equal is not reduced and has clique number 5. When $\chi(G(R)) < 5$ or R is reduced and $\chi(G(R)) < \infty$, then Beck's conjecture is valid [12, Theorem 3.8 and §7]. In this section, we study smaller chromatic numbers for $\Gamma_E(R)$ as well as establish a version of Beck's conjecture when R is a reduced Noetherian ring, but ultimately prove that it does not hold in general, e.g., for the set of non-reduced rings or rings with clique number as small as 3.

We begin with a simple upper bound on the chromatic number:

Lemma 7.1. *Let Δ be the maximum degree of a vertex in $\Gamma_E(R)$. Then we have $\chi(\Gamma_E(R)) \leq \Delta$, except for the case $\Delta = 1$ where $\chi(\Gamma_E(R)) = 1$ or 2.*

Proof. By Brook's Theorem [22, Theorem 5.2.4], $\chi(\Gamma_E(R)) \leq \Delta$, unless the graph is complete or an odd cycle. However, when $\Gamma_E(R)$ has at least three vertices, it is never complete or a cycle, as per [35, Propositions 1.5 and 1.8]. The only exception is $|\Gamma_E(R)| = 2$, in which case $\chi(\Gamma_E(R)) = 2$, but $\Delta = 1$. □

Proposition 7.2. *If R is a reduced ring, then $\chi(\Gamma_E(R)) = \omega(\Gamma_E(R)) = |\operatorname{Ass}(R)|$.*

Proof. Recall Proposition 5.5, by which $|\operatorname{Ass}(R)| = \omega(\Gamma_E(R)) \leq \chi(\Gamma_E(R))$. Let $\operatorname{Min}(R) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. The fact that R is reduced implies that for each $x \in Z^*(R)$ there are indices i and j such that $x \in \mathfrak{p}_i$ and $x \notin \mathfrak{p}_j$. Define a coloring by $f([x]) = \min\{i : x \notin \mathfrak{p}_i\}$. If $f([x]) = k + 1$, then $x \in \mathfrak{p}_i$ for $1 \leq i \leq k$, but $x \notin \mathfrak{p}_{k+1}$.

If $[x]$ and $[y]$ are adjacent, then $y \in \mathfrak{p}_{k+1}$, by Proposition 6.2. Thus, $[x]$ and $[y]$ are assigned different colors. Hence, we have $\chi(\Gamma_E(R)) \leq |\mathrm{Min}(R)| = |\mathrm{Ass}(R)|$. $\qquad\square$

Following Beck's lead, we establish some results for rings with small chromatic numbers for $\Gamma_E(R)$. We note that D. F. Anderson, A. Frazier, A. Lauve, and P. S. Livingston [7, Section 3] have considered similar ideas for the Anderson and Livingston graph $\Gamma(R)$.

7.1 Chromatic/Clique Number 1

Since $\Gamma_E(R)$ is connected, we have $\chi(\Gamma_E(R)) = 1$ if and only if $\omega(\Gamma_E(R)) = 1$ if and only if $\Gamma_E(R)$ consists of a single vertex. Hence, when these conditions are satisfied, we have $xy = 0$ for every x, y in $Z^*(R)$. Thus, Anderson and Livingston's graph $\Gamma(R)$ is complete; see [10, Theorem 2.8]. We have the following characterization.

Proposition 7.3. *We have* $\chi(\Gamma_E(R)) = 1$ *if and only if* $\mathrm{Ass}(R) = \{\mathfrak{p}\}$ *such that* $\mathfrak{p}^2 = 0$. *When these conditions are satisfied, we have* $Q(R) = R_{\mathfrak{p}} \cong R_0 \ltimes V$, *where* $(R_0, \mathfrak{m}_0)$ *is a local ring such that* $\mathfrak{m}_0 = pR_0$ *where* $p = \mathrm{char}(R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}})$ *satisfies* $\mathfrak{m}_0^2 = 0$ *and* V *is a finite-dimensional vector space over* $R_0/\mathfrak{m}_0$.

Proof. Assume first that $\chi(\Gamma_E(R)) = 1$. Then

$$1 \leq |\mathrm{Min}(R)| \leq |\mathrm{Ass}(R)| \leq \chi(\Gamma_E(R)) = 1$$

so $\mathrm{Ass}(R) = \{\mathfrak{p}\}$ for some prime $\mathfrak{p}$. It follows that $Z^*(R) = \mathfrak{p} - \{0\}$. As we noted above, we have $xy = 0$ for every x, y in $Z^*(R) = \mathfrak{p} - \{0\}$, so $\mathfrak{p}^2 = 0$.

Conversely, assume that $\mathrm{Ass}(R) = \{\mathfrak{p}\}$ such that $\mathfrak{p}^2 = 0$. It follows that $xy = 0$ for every x, y in $Z^*(R) = \mathfrak{p} - \{0\}$, so $\Gamma_E(R)$ is a single vertex, hence $\chi(\Gamma_E(R)) = 1$.

Continue to assume that $\mathrm{Ass}(R) = \{\mathfrak{p}\}$ such that $\mathfrak{p}^2 = 0$. It follows that $Z^*(R) = \mathfrak{p} - \{0\}$, so $Q(R) = R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ such that $(\mathfrak{p}R_{\mathfrak{p}})^2 = 0$. The fact that $R_{\mathfrak{p}}$ has the desired form is probably well known; however, we do not know of an appropriate reference, so we include a proof here.

Replace R by $R_{\mathfrak{p}}$ to assume that R is a local ring with unique maximal ideal $\mathfrak{p}$ such that $\mathfrak{p}^2 = 0$. In particular R is a complete local ring. Set $k = R/\mathfrak{p}$.

If R contains a field, then Cohen's structure theorem provides a monomorphism $k \to R$ such that the composition $k \to R \to R/\mathfrak{p} = k$ is an isomorphism. It follows that R is the internal direct sum $R = k \oplus \mathfrak{p}$ as a k-vector space. From this, it is straightforward to show that $R \cong k \ltimes \mathfrak{p}$. Since $\mathfrak{p}$ is finitely generated such that $\mathfrak{p}^2 = 0$, we conclude that $\mathfrak{p}$ is a finite dimensional vector space over k.

Assume that R does not contain a field, and set $p = \mathrm{char}(k)$. In this case, Cohen's structure theorem provides a complete discrete valuation ring (A, pA, k) and a ring homomorphism $f: A \to R$ such that the induced map $k = A/pA \to R/\mathfrak{p} = k$ is an isomorphism. Since R does not contain a field and $\mathfrak{p}^2 = 0$, we conclude that $\mathrm{Ker}(f) = p^2 A$. In R we have $p \neq 0$ since R does not contain a field, and $p^2 = 0$

since $p^2 \in \mathfrak{p}^2 = 0$. In particular, we have $p \in \mathfrak{p} - \mathfrak{p}^2$, so $\mathfrak{p}$ has a minimal generating sequence of the form $p, x_1, \ldots, x_n$. The map $F \colon A[\![X_1, \ldots, X_n]\!] \to R$ given by $X_i \mapsto x_i$ is a well-defined ring epimorphism. Since we have chosen a minimal generating sequence for $\mathfrak{p}$, the fact that $\mathfrak{p}^2 = 0$ implies that $\mathrm{Ker}(F) = (p, X_1, \ldots, X_n)^2$. Thus, we have

$$R \cong A[\![X_1, \ldots, X_n]\!]/(p, X_1, \ldots, X_n)^2 \cong (A/p^2 A)[\![X_1, \ldots, X_n]\!]/(pX_i, X_i X_j).$$

From this description, it follows readily that $R \cong (A/p^2 A) \ltimes V$ where V is the finite dimensional vector space $V = (x_1, \ldots, x_n)R$ over $A/pA = k$. $\qquad\square$

Corollary 7.4. *If R is a finite ring such that $\chi(\Gamma_E(R)) = 1$, then R is local with maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^2 = 0$ and $\mathrm{char}(R) = p$ or p^2 where $p = \mathrm{char}(R/\mathfrak{m})$. Moreover, $R \cong R_0 \ltimes V$, where $(R_0, \mathfrak{m}_0)$ is either isomorphic to the finite field $R/\mathfrak{m}$ or a ring of order $|R/\mathfrak{m}|^2$ such that $\mathfrak{m}_0 = pR_0$ satisfies $\mathfrak{m}_0^2 = 0$, and V is a finite-dimensional vector space over $R_0/\mathfrak{m}_0$.*

7.2 Chromatic/Clique Number 2

The non-trivial star graphs in Section 3 have chromatic number 2, as does a path of length 3. Our next result says that these are the only ways to get chromatic number 2.

Proposition 7.5. *The following are equivalent:*

(i) $\omega(\Gamma_E(R)) = 2$;

(ii) $\chi(\Gamma_E(R)) = 2$;

(iii) $\Gamma_E(R)$ *is acyclic, with at least two vertices; and*

(iv) $\Gamma_E(R)$ *is a non-degenerate star or a path of length* 3.

Proof. If $\Gamma_E(R)$ is a single vertex, then $\omega(\Gamma_E(R)) = \chi(\Gamma_E(R)) = 1$, and all the conditions (i)–(iv) are false. Assume $\Gamma_E(R)$ has at least two vertices. Since it is connected, we have $\chi(\Gamma_E(R)) \geq \omega(\Gamma_E(R)) \geq 2$, hence (ii) $\Rightarrow$ (i). We have $\omega(\Gamma_E(R)) = 2$ if and only if $\Gamma_E(R)$ contains no cycle of length 3, since such a cycle is also a clique of size 3. By Theorem 6.6, $\Gamma_E(R)$ contains no cycle of length 3 if and only if it is acyclic. So (i) $\Leftrightarrow$ (iii). By [22, Proposition 1.6.1], we have $\chi(\Gamma_E(R)) = 2$ if and only if $\Gamma_E(R)$ contains no odd cycle. Thus, we have (iii) $\Rightarrow$ (ii). The equivalence (iv) $\Leftrightarrow$ (iii) is from Proposition 6.4. $\qquad\square$

7.3 Chromatic/Clique Number 3

Proposition 7.6. *If $\chi(\Gamma_E(R)) = 3$, then $\omega(\Gamma_E(R)) = 3$.*

Proof. If $\chi(\Gamma_E(R)) = 3$, then $\omega(\Gamma_E(R)) \leq 3$ and $\Gamma_E(R)$ has an odd cycle by [22, Proposition 1.6.1]. Consequently, $\omega(\Gamma_E(R)) = 3$ by Theorem 6.6. $\qquad\square$

The next example provides a finite local ring R such that $\omega(\Gamma_E(R)) = 3$ and $\chi(\Gamma_E(R)) = 4$. In particular, the converse of the previous result is false, as our example provides a negative answer to the question, motivated by Beck's original work, of whether or not $\omega(\Gamma_E(R)) = \chi(\Gamma_E(R))$.

Example 7.7. Let F be a field. Consider a sequence $\mathbf{X} = X_1, \ldots, X_5$ of indeterminates, and set

$$R = \frac{F[\mathbf{X}]}{(X_1 X_2, X_2 X_3, X_3 X_4, X_4 X_5, X_1 X_5) + (\mathbf{X})^3}.$$

Note that R is local and Artinian with maximal ideal $\mathfrak{m} = (\mathbf{X})R$ such that $\mathfrak{m}^3 = 0$.

To simplify computations, we perform arithmetic on subscripts modulo 5. For instance, we occasionally write X_{i+2} in place of X_{i-3} when $i \geq 4$. This allows us to consider expressions like $X_i X_{i+2}$ for $i = 1, \ldots, 5$ without worrying about separate cases for $i \leq 3$ and $i > 3$. For instance, this allows us to write $X_{i-1} X_i = 0 = X_i X_{i+1}$ in R for $i = 1, \ldots, 5$.

For $i = 1, \ldots, 5$ let $e_i \in \mathbb{Z}^5$ be the ith standard basis vector. The ring R is $\mathbb{Z}^5$-graded with $\deg(X_i) = e_i$ because the ideal defining R is a monomial ideal. It follows readily that

$$\mathrm{Soc}(R) = 0 \oplus 0 \oplus R_2 \tag{7.7.1}$$

where we use the naturally induced $\mathbb{Z}$-grading, and

$$\mathrm{Ann}_R(X_i) = 0 \oplus \mathrm{Span}_F(X_{i-1}, X_{i+1}) \oplus R_2. \tag{7.7.2}$$

It follows that

$$\mathrm{Ann}_R(X_1^2) = \mathrm{Soc}(R) = \mathrm{Ann}_R(q(\mathbf{X})) \tag{7.7.3}$$

for all nonzero quadratic forms $q(\mathbf{X}) \in R_2$.

Next, we claim that for $i = 1, \ldots, 5$ and for all non-zero elements $a, b \in F$ we have

$$\mathrm{Ann}_R(a X_i + b X_{i+2}) = 0 \oplus \mathrm{Span}_F(X_{i+1}) \oplus R_2. \tag{7.7.4}$$

The containment $\supseteq$ follows from the fact that $X_i X_{i+1} = 0 = X_{i+1} X_{i+2}$. For the reverse containment, let $l \in \mathrm{Ann}_R(a X_i + b X_{i+2})$. Since R is graded with $\mathrm{Soc}(R) = R_2$, we assume without loss of generality that $l \in \mathrm{Ann}_R(a X_i + b X_{i+2})_1$. There are (unique) elements $c_1, \ldots, c_5 \in F$ such that $l = \sum_{j=1}^5 c_j X_j$. The condition

$l \in \mathrm{Ann}_R(aX_i + bX_{i+2})$ implies that

$$0 = l(aX_i + bX_{i+2}) = \Big(\sum_{j=1}^{5} c_j X_j\Big)(aX_i + bX_{i+2}).$$

The coefficient of X_i^2 in the right-hand expression is $c_i a$; the $\mathbb{Z}^5$ grading implies that $c_i a = 0$, so $c_i = 0$ since a is a unit in the field F. (This uses the fact that X_i^2 is not in the ideal defining R.) Similarly, we have $c_{i+2} = 0$. The coefficient for $X_i X_{i+3}$ is $c_{i+3}a$, so the same reasoning implies that $c_{i+3} = 0$. Similarly, the $X_{i+2}X_{i+4}$ coefficient implies that $c_{i+4} = 0$. It follows that $l = c_{i+1}X_{i+1} \in \mathrm{Span}_F(X_{i+1})$, establishing the claim.

Note that the claim implies that

$$\mathrm{Ann}_R(aX_i + bX_{i+2}) = \mathrm{Ann}_R(X_i + X_{i+2}) \tag{7.7.5}$$

for $i = 1, \ldots, 5$ and for all non-zero elements $a, b \in F$. The same reason shows that all other linear forms have trivial annihilator; in other words:

$$l \in R_1 \setminus \bigcup_{i=1}^{5}(\mathrm{Span}_F(X_i) \cup \mathrm{Span}(X_i + X_{i+2}))$$
$$\Rightarrow \mathrm{Ann}_R(l) = R_2 = \mathrm{Ann}_R(X_1 + X_2).$$

Combining this with (7.7.2)–(7.7.5), we find that $\Gamma_E(R)$ is takes the form of a "pinwheel" and one edge, as shown below.
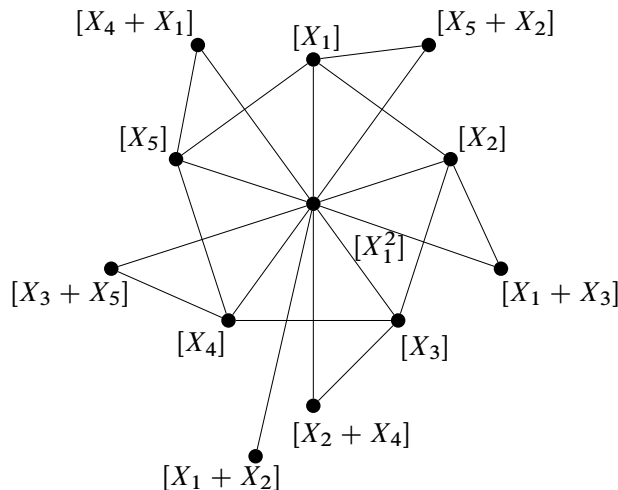
From the graph, it is easy to see that $\omega(\Gamma_E(R)) = 3$. However, $\chi(\Gamma_E(R)) = 4$ since the 5-cycle on $[X_i], 1 \leq i \leq 5$ requires 3 colors [22, Theorem 1.6.1] and the vertex $[X_1^2]$ is adjacent to every $[X_i]$ and hence requires a fourth color.

A Tables for Example 3.14

The following table includes the values of c^{bb} (with $c^{bb} < 100$) for star graphs we can construct using the method of Example 3.14.

d_1	e_1	t_1	d_2	e_2	t_2	c^{bb}
1	1	1	2	1	1	8
1	1	1	2	2	1	14
1	1	1	2	2	2	12
1	1	1	2	3	1	26
1	1	1	2	3	2	24
1	1	1	2	4	1	50
1	1	1	2	4	2	48
1	1	1	2	5	1	98
1	1	1	2	5	2	96
1	2	1	3	1	1	14
1	2	1	3	2	1	28
1	2	1	3	2	2	26
1	2	1	3	3	1	56
1	2	1	3	3	2	54
1	2	1	3	3	3	50
1	3	1	4	1	1	26
1	3	1	4	2	1	56
1	3	1	4	2	2	54
1	4	1	5	1	1	50
1	5	1	6	1	1	98
2	2	1	4	1	1	28
2	2	1	4	2	1	58
2	2	1	4	2	2	56
2	2	2	4	1	1	26
2	2	2	4	2	1	56
2	2	2	4	2	2	54
2	3	1	5	1	1	56
2	3	2	5	1	1	54

The next three iterations of the process are given below.

d_1	e_1	t_1	d_2	e_2	t_2	d_3	e_3	t_3	c^{bbb}
1	1	1	2	1	1	3	1	1	16
1	1	1	2	1	1	3	2	1	30
1	1	1	2	1	1	3	2	2	28
1	1	1	2	1	1	3	3	1	58
1	1	1	2	1	1	3	3	2	56
1	1	1	2	1	1	3	3	3	52
1	1	1	2	2	1	4	1	1	30
1	1	1	2	2	1	4	2	1	60
1	1	1	2	2	1	4	2	2	58
1	1	1	2	2	2	4	1	1	28
1	1	1	2	2	2	4	2	1	58
1	1	1	2	2	2	4	2	2	56
1	1	1	2	3	1	5	1	1	58
1	1	1	2	3	2	5	1	1	56
1	2	1	3	1	1	4	1	1	30
1	2	1	3	1	1	4	2	1	60
1	2	1	3	1	1	4	2	2	58
1	2	1	3	2	1	5	1	1	60
1	2	1	3	2	2	5	1	1	58
1	3	1	4	1	1	5	1	1	58
2	2	1	4	1	1	5	1	1	60
2	2	2	4	1	1	5	1	1	58

d_1	e_1	t_1	d_2	e_2	t_2	d_3	e_3	t_3	d_4	e_4	t_4	c^{bbbb}
1	1	1	2	1	1	3	1	1	4	1	1	32
1	1	1	2	1	1	3	1	1	4	2	1	62
1	1	1	2	1	1	3	1	1	4	2	2	60
1	1	1	2	1	1	3	2	1	5	1	1	62
1	1	1	2	1	1	3	2	2	5	1	1	60
1	1	1	2	2	1	4	1	1	5	1	1	62
1	1	1	2	2	2	4	1	1	5	1	1	60
1	2	1	3	1	1	4	1	1	5	1	1	62

d_1	e_1	t_1	d_2	e_2	t_2	d_3	e_3	t_3	d_4	e_4	t_4	d_5	e_5	t_5	c^{bbbbb}
1	1	1	2	1	1	3	1	1	4	1	1	5	1	1	64

B Graph Theory

Listed below are all the relevant definitions from Graph Theory. A good reference on the subject is [22] and for the material on zero divisor graphs, the papers [10], [2], and [1] provide a good background.

   (i) A graph is **acyclic** if it contains no cycles.

  (ii) A graph is **bipartite** (respectively, *r-partite*) if the vertices can be partitioned into two (resp., r) disjoint subsets so that every edge has one vertex in each subset (resp., every edge joins vertices in distinct subsets).

 (iii) A graph is **chordal** if every cycle with four or more vertices has a *chord*, or edge joining two vertices of the cycle that are not adjacent.

  (iv) The **circumference** of a graph is the maximum length of a cycle in the graph. If the graph is acyclic, then the circumference is zero.

   (v) A **clique** in a graph is a subset of vertices of the graph that are all pairwise adjacent; i.e. a vertex set which induces a complete subgraph.

  (vi) If a graph G contains a clique of size n and no clique has more than n elements, then the **clique number** of the graph is said to be n; if the clique size is unbounded, then the clique number is infinite. It is denoted by $\omega(G)$.

 (vii) The **closure of a neighborhood** of a vertex v in a graph is the neighborhood of v along with v itself; i.e., $\mathcal{N}(v) \cup \{v\}$. It is denoted by $\overline{\mathcal{N}(v)}$.

(viii) The **chromatic number** or **coloring number** of a graph G, denoted $\chi(G)$, is the minimal number of colors which can be assigned to the vertices of G such that no pair of adjacent vertices has the same color.

  (ix) A graph is **compact** if it is a simple connected graph satisfying the property that for every pair of non-adjacent vertices x and y, there is vertex z adjacent to every vertex adjacent to x and/or y.

   (x) A graph is said to be **complete** if every vertex in the graph is adjacent to every other vertex in the graph. The notation for a complete graph on n vertices is K_n.

  (xi) A **complete bipartite** is a bipartite graph such that every vertex in one partitioning subset is adjacent to every vertex in the other partitioning subset. If the subsets have cardinality m, and n, then this graph is denoted by $K_{m,n}$.

 (xii) A **complete r-partite** graph is an r-partite graph such that every vertex in any partitioning subset is adjacent to every vertex in every other partitioning subset.

(xiii) A graph is said to be **connected** if there is a path between every pair of vertices of the graph.

(xiv) A **cut vertex** in a connected graph G is a vertex whose removal from the vertex set of G results in a disconnected graph; v is said to **separate** vertices a and b if every path between the two includes v.

(xv) A **cycle** in a graph is a path of length at least 3 through distinct vertices which begins and ends at the same vertex.

(xvi) A **cycle graph** is an n-gon for some integer $n \geq 3$.

(xvii) The **degree** of a vertex is the number of vertices adjacent to it.

(xviii) The **diameter** of a connected graph is the supremum of the distances between any two vertices.

(xix) A **directed graph** is a pair (V, E) of disjoint sets (of vertices and edges) together with two maps init: $E \to V$ and ter: $E \to V$ assigning to every edge e an initial vertex init(e) and a terminal vertex ter(e). The edge e is said to be directed from init(e) to ter(e).

(xx) The **distance** between two vertices v and w in a connected graph is the length of the shortest path between them; if no path exists between a pair of vertices, then the distance is defined to be infinite.

(xxi) A vertex is an **end** if it has degree 1.

(xxii) The **girth** of a graph is the length of the shortest cycle in the graph; it is infinite if the graph is acyclic.

(xxiii) A **graph** consists of a set of vertices, a set of edges, and an incident relation, describing which vertices are adjacent (i.e., joined by an edge) to which.

(xxiv) Let $G = (V, E)$ and $G' = (V', E')$ be two graphs. A **homomorphism** $G \to G'$ is a function $\phi: V \to V'$ respecting adjacency, that is, such that for all $x, y \in V$ if $xy \in E$, then $\phi(x)\phi(y) \in E'$.

(xxv) An **induced subgraph** of a graph G is obtained by taking a subset U of the vertex set of G together with all edges which are incident in G only with vertices belonging to U.

(xxvi) Let $G = (V, E)$ and $G' = (V', E')$ be two graphs. An **isomorphism** $G \xrightarrow{\cong} G'$ is a bijection $\phi: V \to V'$ with $xy \in E$ if and only if $\phi(x)\phi(y) \in E'$ for all $x, y \in V$.

(xxvii) The **neighborhood** of a vertex v in a graph is the set of all vertices adjacent to v. It is denoted by $\mathcal{N}(v)$. [Note that for simple graphs, $v \notin \mathcal{N}(v)$.]

(xxviii) A **non-degenerate star graph** is a star graph with at least two vertices.

(xxix) A **path of length** n between two vertices v and w is a finite sequence of vertices $u_0, u_1, \ldots, u_n$ such that $v = u_0$, $w = u_n$, and u_{i-1} and u_i are adjacent for all $1 \leq i \leq n$.

(xxx) A graph is **perfect** if for every induced subgraph, including the graph itself, the chromatic number and clique numbers agree.

(xxxi) A graph is **planar** if it can be drawn in the plane with no crossings of edges.

(xxxii) A **regular** graph is one in which all the vertices have the same degree.

(xxxiii) A vertex v in a graph G is said to **separate** vertices a and b if every path between a and b includes v.

(xxxiv) A **simple graph** is one with no loops on a vertex and no multiple edges between a pair of vertices.

(xxxv) A **star graph** is a complete bipartite graph in which one of the partitioning subsets is a singleton set. The notation for this graph is $K_{1,n}$.

Bibliography

[1] Akbari, S., Maimani, H. R., Yassemi, S., When a zero-divisor graph is planar or a complete r-partite graph. J Algebra. 2003;270:169–180.

[2] Akbari, S., Mohammadian, A., On the zero-divisor graph of a commutative ring. J Algebra. 2004;274:847–855.

[3] ———, Zero-divisor graphs of non-commutative rings. J Algebra. 2006;296:462–479.

[4] Anderson, D. D., Naseer, M., Beck's coloring of a commutative ring. J Algebra. 1993; 159:500–514.

[5] Anderson, D. D., Winders, M., Idealization of a module. J Commut Algebra. 2009;1: 3–56.

[6] Anderson, D. F., Axtell, M. C., Stickles Jr, J. A., Zero-divisor graphs in commutative rings. In: Commutative algebra – Noetherian and non-Noetherian perspectives. New York: Springer; 2011. p. 23–45.

[7] Anderson, D. F., Frazier, A., Lauve, A., Livingston, P. S., The zero-divisor graph of a commutative ring. II. Proceedings, Ideal Theoretic Methods in Commutative Algebra; Columbia, MO, 1999. vol. 220 of Lecture notes in pure and applied mathematics. New York: Dekker; 2001. p. 61–72.

[8] Anderson, D. F., LaGrange, J. D., Commutative Boolean monoids, reduced rings, and the compressed zero-divisor graph. Preprint. 2011.

[9] Anderson, D. F., Levy, R., Shapiro, J., Zero-divisor graphs, von Neumann regular rings, and Boolean algebras. J Pure Appl Algebra. 2003;180:221–241.

[10] Anderson, D. F., Livingston, P. S., The zero-divisor graph of a commutative ring. J Algebra. 1999;217:434–447.

[11] Axtell, M., Baeth, N., Stickles, J., Cut vertices in zero-divisor graphs of finite commutative rings. Comm Algebra. To appear.

[12] Beck, I., Coloring of commutative rings. J Algebra. 1988;116:208–226.

[13] Belshoff, R., Chapman, J., Planar zero-divisor graphs. J Algebra. 2007;316:471–480.

[14] Bloomfield, N., Wickham, C., Local rings with genus two zero divisor graph. Comm Algebra. 2010;38:2965–2980.

[15] Bruns, W., Vetter, U., Determinantal rings. vol. 1327 of Lecture notes in mathematics. Berlin: Springer-Verlag; 1988.

[16] Chiang-Hsieh, H.-J., Smith, N. O., Wang, H.-J., Commutative rings with toroidal zero-divisor graphs. Houston J Math. 2010;36:1–31.

[17] DeMeyer, F., DeMeyer, L., Zero divisor graphs of semigroups. J Algebra. 2005;283:190–198.

[18] DeMeyer, F., McKenzie, T., Schneider, K., The zero-divisor graph of a commutative semigroup. Semigroup Forum. 2002;65:206–214.

[19] DeMeyer, F., Schneider, K., Automorphisms and zero divisor graphs of commutative rings. In: Commutative rings. Hauppauge, NY: Nova Sci. Publ.; 2002. p. 25–37.

[20] DeMeyer, L., D'Sa, M., Epstein, I., Geiser, A., Smith, K., Semigroups and the zero divisor graph. Bull Inst Combin Appl. 2009;57:60–70.

[21] DeMeyer, L., Greve, L., Sabbaghi, A., Wang, J., The zero-divisor graph associated to a semigroup. Comm Algebra. 2010;38:3370–3391.

[22] Diestel, R., Graph theory. 4th ed. vol. 173 of Graduate texts in mathematics. Heidelberg: Springer; 2010.

[23] Ghalandarzadeh, S., Malakooti Rad, P., Torsion graph over multiplication modules. Extracta Math. 2009;24:281–299.

[24] Halaš, R., Jukl, M., On Beck's coloring of posets. Discrete Math. 2009;309:4584–4589.

[25] Levidiotis, F., Spiroff, S., Five point zero divisor graphs determined by equivalence classes. Involve 2011;4(1):53–64.

[26] Lu, D., Wu, T., The zero-divisor graphs of posets and an application to semigroups. Graphs Combin. 2010;26:793–804.

[27] Maimani, H. R., Pournaki, M. R., Yassemi, S., Zero-divisor graph with respect to an ideal. Comm Algebra. 2006;34:923–929.

[28] Matsumura, H., Commutative ring theory. 2nd ed. vol. 8 of Studies in advanced mathematics. Cambridge: University Press; 1989.

[29] Mulay, S. B., Cycles and symmetries of zero-divisors. Comm Algebra. 2002;30:3533–3558.

[30] Nimbhokar, S. K., Wasadikar, M. P., DeMeyer, L., Coloring of meet-semilattices. Ars Combin. 2007;84:97–104.

[31] Redmond, S. P., An ideal-based zero-divisor graph of a commutative ring. Comm Algebra. 2003;31:4425–4443.

[32] _____, The zero-divisor graph of a non-commutative ring. In: Badawi, A., editor. Trends in commutative rings research. Hauppauge, NY: Nova Science Publishers; 2004. p. 203–211 [reprint of Int J Commut Rings. 2002;1(4):203–211].

[33] Smith, N. O., Planar zero-divisor graphs. Int J Commut Rings. 2003;2:177–186 [English, reprinted in Focus on commutative rings research. New York: Nova Sci. Publ.; 2006. p. 177–186].

[34] ⸻ , Infinite planar zero-divisor graphs. Comm Algebra. 2007;35:171–180.

[35] Spiroff, S., Wickham, C., A zero divisor graph determined by equivalence classes of zero divisors. Communications in Alg. 2011;39:2338–2348.

[36] Wickham, C., Classification of rings with genus one zero-divisor graphs. Comm Algebra. 2008;36:325–345.

Author Information

Jim Coykendall, Department of Mathematics, North Dakota State University, Fargo, ND, USA.
E-mail: `jim.coykendall@ndsu.edu`

Sean Sather-Wagstaff, Department of Mathematics, North Dakota State University, Fargo, ND, USA.
E-mail: `Sean.Sather-Wagstaff@ndsu.edu`

Laura Sheppardson, Department of Mathematics, University of Mississippi, Oxford, MS, USA.
E-mail: `sheppard@olemiss.edu`

Sandra Spiroff, Department of Mathematics, University of Mississippi, Oxford, MS, USA.
E-mail: `spiroff@olemiss.edu`

A Closer Look at Non-Unique Factorization via Atomic Decay and Strong Atoms

Scott T. Chapman and Ulrich Krause

Abstract. Let D be an integral domain and x an irreducible (or atom) of D. We call x a *strong atom* of D if every irreducible divisor of x^k, for k a positive integer, is an associate of x. If x is not a strong atom, then there is a factorization of x of the form $x^k = x_1 \cdots x_n$ where k is minimal and each x_i is irreducible and not associated to x. In this case we say that x admits *atomic decay* with respect to $x_1, \ldots, x_n$. In this paper, we consider various implications of atomic decay in integral domains. We characterize strong atoms in a general integral domain in terms of a separation property involving prime ideals. We then use two classic examples from algebraic number theory to illustrate how atomic decay effects factorization properties in general. While we show that atomic decay behaves in a relatively mild manner in $\mathbb{Z}[\sqrt{-5}]$, we also show that its effect is much more dramatic in the subring $\mathbb{Z}[5\imath]$ of the Gaussian integers $\mathbb{Z}[\imath]$.

Keywords. Non-unique Factorization, Algebraic Number Ring, Prime Ideals, Half-factoriality.

2010 Mathematics Subject Classification. 13F15, 11R04, 20D60.

1 Introduction

In a first course in Abstract Algebra (such as one taught from [5]), the theory of integral domains culminates with the study of the factorization of elements into products of irreducible elements. Of particular interest in such a discussion are two types of elements. If D is an integral domain and x is a nonzero nonunit of D, then

 (i) x is *prime* if whenever x divides yz with y and z in D, then either x divides y or x divides z;

 (ii) x is *irreducible* (or an *atom*) if whenever $x = yz$ with y and z in D, then either y or z is *unit* of D (a divisor of 1).

An elementary argument shows that a prime element must be irreducible, but the converse fails (see equation (∗) and its accompanying description in Section 4). Moreover, it is easy to verify that a prime element p has the nice property that any atom which divides a power p^k of p must be an associate of p. We call an atom which has this property a *strong atom* (in the literature, these atoms have also been called *absolutely irreducible* [1] or [6, Definition 7.1.3], or *completely irreducible* [12]). An atom which is not strong must have a power which is divisible by a nonassociated atom. That is, powers of atoms can decay into other atoms, a phenomenon we refer to as *atomic decay*. More precisely, we have the following definition.

Definition 1.1. Let D be an integral domain and x an atom of D. We call x a *strong atom* of D if each irreducible divisor of x^k (where k is a natural number) is an associate of x. If x is not a strong atom and $x^k = x_1 \cdots x_n$ where none of the atoms $x_1, \ldots, x_n$ are associates of x and $k, n \geq 2$, then we say that x admits *atomic decay* with respect to $x_1, \ldots, x_n$.

A prime element is, of course, a strong atom, but the converse fails (see Proposition 4.1). Both prime elements and strong atoms play their roles in regard to unique factorization in an integral domain D. Recall that D is a *unique factorization domain* (also called a *UFD* or a *factorial domain*) if each nonzero nonunit of D factors into a (finite) product of atoms which is unique up to order of associated factors. It is easily verified, for an *atomic domain* D (i.e., a domain where each nonzero nonunit is a product of atoms), that D is a UFD if and only if every atom is prime. Moreover, as we shall later see, the ring of integers of an algebraic number field is a UFD if and only if each atom is a strong atom. Therefore, for these rings, we can consider nonunique factorization as being rooted in atomic decay. We will demonstrate in this case that some power of any nonzero nonunit can be factored by atomic decay into strong atoms in a unique way (up to order and associates of factors). This can be viewed as a way of restoring uniqueness without leaving the domain or the level of elements.

We break the remainder of our paper into 5 Sections. In Section 2 we characterize for a general integral domain D strong atoms using a separation property involving prime ideals. This allows us to describe, under certain conditions, strong atoms by powers of prime ideals. Section 3 deals with the ring of integers of an algebraic number field for which the conditions in Section 2 are met. Using atomic decay, we obtain the above mentioned factorization of powers of elements into strong atoms which is essentially unique. From this we draw conclusions which characterize various factorization properties in terms of the decay rate of atoms. In Section 4 we discuss in detail an example within the domain $\mathbb{Z}[\sqrt{-5}]$, well known since the time of R. Dedekind, where unique factorization breaks down. Atomic decay works in a relatively mild manner in that all atoms admit a finite and unique decay. By taking squares, two different factorizations of an element reveal hidden uniqueness. We also relate strong atoms to the ideal numbers of E. E. Kummer as viewed by E. Hecke [7]. In Section 5 we consider the failure of uniqueness in the subring $\mathbb{Z}[5\iota]$ of the Gaussian integers $\mathbb{Z}[\iota]$ which appears at first seemingly simpler than $\mathbb{Z}[\sqrt{-5}]$. Atomic decay in this case, however, is much more dramatic. The decay of some atoms never reaches strong atoms and the powers of a single atom are divisible by infinitely many nonassociated atoms. In Section 6 we conclude with some remarks and questions. We ask, for example, if there is a direct way to check whether a given atom is strong. One goal in our paper is to use tools as elementary as possible. Hence, the examples presented are appropriate for students with a limited background in Abstract Algebra. To better facilitate this, we make use of algebraic number rings, where the reader need only have knowledge of the basic facts of ideal theory, which we explicitly state. Readers who desire a deeper or more technical analysis of the theory of nonunique factorizations, are directed to

the well-known monograph of Geroldinger and Halter-Koch [6]. The authors greatly acknowledge comments on an earlier draft of this paper by Alfred Geroldinger, Nathan Kaplan and William W. Smith.

2 Strong Atoms and Prime Ideals

To later describe atomic decay in algebraic number rings, we first analyze strong atoms within the common theory of ideals. We remind the reader of some basic notions. Let D be an integral domain. A subset I of D is called an *ideal* if I is an additive subgroup of D which is closed under the multiplication by elements from D. For $x \in D$, $(x) = \{rx \mid r \in D\}$ is the *principal ideal* generated by x. If $1 \in (x)$, then x is called a *unit*. If $(x) = (y)$, then the elements x and y are *associates*. An ideal P is called a *prime ideal* if $P \neq D$ and whenever $ab \in P$ for a and b in D, then either $a \in P$ or $b \in P$. An ideal M is called a *maximal ideal* if $M \neq D$ and the only ideals containing M are M and D. It is easy to show that a maximal ideal is a prime ideal, but not conversely [5, Theorems 14.3 and 14.4]. If I and J are two ideals of D, then

$$IJ = \left\{ \sum_i a_i b_i \mid a_i \in I \text{ and } b_i \in J \right\}$$

is another ideal of D called the *product* of I and J. The product I^n of n copies of the ideal I is the *nth power of I*. For an ideal I of D, the set

$$\mathrm{rad}(I) = \{x \in D \mid x^n \in I \text{ for some } n \in \mathbb{N}\}$$

is again an ideal called the *radical* of I.

For any integral domain D, the following lemma establishes relationships between strong atoms and prime ideals.

Lemma 2.1. *Let D be an integral domain and $x \in D$ an atom.*

  (i) *The atom x is a strong atom if and only if x can be separated from any non-associated atom y by a prime ideal P in the sense that $x \notin P$ but $y \in P$.*

 (ii) *If $(x) = M^k$ for some maximal ideal M and $k \in \mathbb{N}$, then x can be separated by a prime ideal from every non-associated atom y with (y) a product of prime ideals.*

(iii) *Let x be a strong atom and (x) a product of prime ideals such that for at least one prime factor P there exists an atom y such that $(y) = P^m$ for some $m \in \mathbb{N}$. Then $(x) = P^m$.*

Proof. (i) ($\Rightarrow$) Let x be a strong atom, $S = \{x^k \mid k \in \mathbb{N}_0\}$ and suppose $S \cap (y) \neq \emptyset$ for an atom y non-associated to x. Then there exists $r \in D$ and $k \in \mathbb{N}_0$ with $x^k = yr$. Since x is a strong atom it follows that x and y are associates. This is a contradiction

and we must have that $S \cap (y) = \emptyset$. By Zorn's Lemma, there exists an ideal P which is maximal with respect to $(y) \subseteq P$ and $S \cap P = \emptyset$. We show that P is a prime ideal. Suppose $a_1 a_2 \in P$ with $a_i \in D$ and $a_i \notin P$ for $i = 1, 2$. Then for the smallest ideal (P, a_i) containing P and a_i, we have for $i = 1, 2$ that $P \subsetneq (P, a_i)$ and $(P, a_i) \cap S \neq \emptyset$. Thus, there exist $s_i \in S$, $r_i \in D$ and $b_i \in P$ such that $s_i = b_i + r_i a_i$ for $i = 1, 2$. We obtain

$$s_1 s_2 = (b_1 + r_1 a_1)(b_2 + r_2 a_2) = b_1 b_2 + b_1 r_2 a_2 + b_2 r_1 a_1 + r_1 r_2 a_1 a_2.$$

Since $a_1 a_2 \in P$ it follows that $s_1 s_2 \in P$. Therefore $S \cap P \neq \emptyset$ which is a contradiction and hence P is a prime ideal. Obviously $y \in P$ and $x \notin P$ since $S \cap P = \emptyset$.

($\Leftarrow$) Assume x can be separated from every nonassociated atom y. Let $x^n = yz$ for some $n \in \mathbb{N}$ where y is an atom and $z \in D$. If y is not an associate of x, then $y \in P$ and $x \notin P$ for some prime ideal P. This implies $x^n \in P$ but $x \notin P$, a contradiction.

(ii) Suppose, for every prime ideal Q, $y \in Q$ implies $x \in Q$. We show that y must be associated to x. By assumption $(y) = P_1 \cdots P_l$ for prime ideals P_i. Since $y \in P_i$, we have $x \in P_i$ and, hence, $M^k = (x) \subseteq P_i$ for all i. If $p \in M$, then $p^k \in M^k \subseteq P_i$ and, hence, $p \in P_i$. That is, $M \subseteq P_i$ for all i. Since M is maximal we have $M = P_i$ for all i. Thus, $(x) = M^k$ and $(y) = M^l$. If $k \leq l$, then $(y) \subseteq (x)$ and if $k \geq l$, then $(x) \subseteq (y)$. In any case, since x and y are atoms, they must be associated.

(iii) Let x be a strong atom with $(x) = P_1 \cdots P_k$ and $P_i^m = (y)$ for some $i, m \in \mathbb{N}$ and atom y. If $y \in Q$ for some prime ideal Q then $P_i^m \subseteq Q$ and, hence, $P_i \subseteq Q$. Thus, $(x) \subseteq Q$ and $x \in Q$. Since x is a strong atom, y has to be associated to x by property (i). Therefore, $(x) = (y) = P_i^m$. □

As Lemma 2.1 indicates, there is a strong connection between the ideal theory of an integral domain and the factorization properties of its elements. We weigh this more carefully by considering three different ideal theoretic conditions on an integral domain D:

($\mathcal{A}$) For every atom $x \in D$ there exist prime ideals $P_1, \ldots, P_k$ of D such that $(x) = P_1 \cdots P_k$.

($\mathcal{B}$) For every nonzero prime ideal P of D, there exists a positive integer $m(P)$ such that $P^{m(P)} = (y)$ where y is an atom of D.

($\mathcal{C}$) Each nonzero prime ideal P of D is maximal.

Using these conditions, we obtain in Theorem 2.2 relationships between a strong atom x and its resulting principal ideal (x). In domains which satisfy conditions ($\mathcal{A}$), ($\mathcal{B}$), and ($\mathcal{C}$), the relationships will all be equivalent, a key fact for our work in Section 3.

Theorem 2.2. *For an atom x in an integral domain D consider the following properties.*

(a) *The ideal (x) is a power of a maximal ideal.*

(b) *The ideal* rad(x) *is a maximal ideal.*

(c) *The atom x is a strong atom.*

(d) *The ideal (x) is a power of a prime ideal.*

In an integral domain D the following relationships hold.

  (i) $(a) \Rightarrow (b)$.

 (ii) *If D satisfies $(\mathcal{C})$, then* (d) $\Rightarrow$ (a).

(iii) *If D satisfies $(\mathcal{A})$, then* (b) $\Rightarrow$ (a) $\Rightarrow$ (c).

(iv) *If D satisfies $(\mathcal{A})$ and $(\mathcal{B})$, then* (c) $\Rightarrow$ (d).

Hence, if D satisfies $(\mathcal{A})$, $(\mathcal{B})$ and $(\mathcal{C})$, then conditions (a)–(d) *are equivalent.*

Proof. (i) If $y \in \mathrm{rad}(x)$, then $y^m \in (x) = M^k \subseteq M$ for some maximal ideal M. Since M must be a prime ideal, we have that $y \in M$. Conversely, $y \in M$ implies $y^k \in M^k = (x)$ and, hence, $y \in \mathrm{rad}(x)$. Thus (a) $\Rightarrow$ (b).

The proof of (ii) is obvious.

(iii) Suppose that for each atom y there are prime ideals $P_1, \ldots, P_k$ such that $(y) = P_1 \cdots P_k$. We show that (b) $\Rightarrow$ (a) $\Rightarrow$ (c). Let $\mathrm{rad}(x) = M$ be a maximal ideal. By assumption, $(x) = P_1 \cdots P_k$ with prime ideals P_i. If $y \in M = \mathrm{rad}(x)$, then $y^n \in (x) \subseteq P_i$ and $y \in P_i$. Therefore $M \subseteq P_i$ for all $1 \le i \le k$. M a maximal ideal implies $P_i = M$ for all i and $(x) = M^k$. This proves (b) $\Rightarrow$ (a). Furthermore, let $(x) = M^k$ where M is a maximal ideal. From Lemma 2.1 (ii) and (i), it follows that x is a strong atom.

(iv) We note that (c) $\Rightarrow$ (d) follows from Lemma 2.1 (iii). The final statement now easily follows. $\qquad\square$

3 Atomic Decay in the Ring of Integers of an Algebraic Number Field

The relationship between strong atoms and ideals given in Theorem 2.2 for integral domains in general becomes particularly neat for the special class of algebraic number rings. First we review some basic notation. An (algebraic) *number field* is a field $K = \mathbb{Q}(\theta)$ obtained as the smallest field containing the rational numbers $\mathbb{Q}$ and a root θ of a polynomial with coefficients in $\mathbb{Z}$. The *ring of integers* of a number field K is the set of all elements in K which are roots of a monic polynomial with coefficients in $\mathbb{Z}$. To describe atomic decay within the ring of integers D of a number field, we will use the following well-known basic facts about the ideal theory in D. Proofs of these facts can be found in [10] or [11].

- **The Fundamental Theorem of Ideal Theory.** *Let I be an nonzero ideal of D with $I \ne D$. There exists a unique (up to order) sequence of prime ideals $P_1, \ldots, P_k$ of D such that $I = P_1 \cdots P_k$.*

- For each (nonzero) prime ideal P there exists $m(P) \in \mathbb{N}$ such that $P^{m(P)}$ is the principal ideal generated by an atom.

- Every (nonzero) prime ideal is a maximal ideal.

By these facts, the properties (a)–(d) in Theorem 2.2 are equivalent for a ring D of integers and strong atoms can be described in greater detail.

Theorem 3.1. *Let D be the ring of integers of a number field.*

(i) *An element $x \in D$ is a strong atom if and only if x is an atom and $\mathrm{rad}(x)$ is a prime ideal, or, equivalently, if (x) is a minimal power of a prime ideal.*

(ii) *For each nonzero nonunit $x \in D$, there exists a sequence $x_1, \ldots, x_k$ of strong atoms and a minimal $m \in \mathbb{N}$ such that*

$$x^m = x_1 \cdots x_k \tag{AD}$$

where this representation by atomic decay is unique up to ordering and associates for the $x_1, \ldots, x_k$.

Proof. (i) Follows from Theorem 2.2 according to the equivalence of (a)–(d). Hence, (x) is a minimal power of P if $(x) = P^{m(P)}$. (ii) By the Fundamental Theorem, $(x) = P_1 \cdots P_k$ for nonzero prime ideals $P_1, \ldots, P_k$ of D. Furthermore, $P_i^{m(P_i)} = (y_{P_i})$ for every prime ideal P_i, with $m(P_i) \in \mathbb{N}$ and, by (i), y_{P_i} a strong atom. Let $m = \mathrm{lcm}\{m(P_i) \mid 1 \le i \le k\}$ and for each i set $m = m(P_i)n(P_i)$. Then it follows that $(x)^m = (x^m) = \prod_{i=1}^{k} P_i^m = \prod_{i=1}^{k} (y_{P_i})^{n(P_i)}$. Therefore, there exist associates x_{P_i} of y_{P_i}, strong atoms again, such that $x^m = \prod_{i=1}^{k} x_{P_i}^{n(P_i)}$.

Concerning the uniqueness of this representation, assume $\prod_{i=1}^{k} v_i^{k_i} = \prod_{j=1}^{l} w_j^{l_j}$ for strong atoms v_i, w_j and $k_i, l_j \in \mathbb{N}$; the v_i, as well as the w_j are to be pairwise different. By property (i), we have $(v_i) = P_i^{n_i}$, $(w_j) = Q_j^{m_j}$ for nonzero prime ideals P_i and Q_j. Therefore

$$\prod_{i=1}^{k} P_i^{n_i k_i} = \prod_{j=1}^{l} Q_j^{m_j l_j}.$$

From the uniqueness property of the Fundamental Theorem we have $k = l$ and there is a permutation σ of $\{1, \ldots, k\}$ such that $Q_i = P_{\sigma(i)}$, $m_i = n_{\sigma(i)}$, $l_i = k_{\sigma(i)}$. Therefore, $(w_i) = (v_{\sigma(i)})$ and the representation is unique up to order and associates of factors. $\square$

The condition in Theorem 3.1 (ii) has been studied in general. In [4], the current authors define an integral domain D to be a *Cale domain* with base $B \subseteq D$ if a power of every nonzero nonunit of D can be written uniquely as a product of elements from B. For an algebraic ring of integers, the representation (AD) is known as the *Cale representation* of x. It is an interesting feature of (AD) that the representation as well as the definition of strong atoms is purely multiplicative. This is different for the unique representation according to the Fundamental Theorem of Ideal Theory, which does involve the addition operation of the ring. The reader interested in the general Cale concept may find a more technical discussion in [3] or [4].

As a further consequence, we obtain the following characterization of unique factorization into atoms for rings of algebraic integers.

Corollary 3.2. *The ring of integers D of a number field is a UFD if and only if D does not have atomic decay. That is, every atom is a strong atom.*

Proof. Using the norm function (see Section 4 or [10, 11]), it is easily argued that any element of D is a product of atoms. ($\Leftarrow$) If every atom is strong, then by Theorem 3.1 (ii) D is a UFD. ($\Rightarrow$) Assume D is a UFD. If x is an atom then

$$x^n = \underbrace{x \cdots x}_{n \text{ times}}$$

is the unique representation into atoms and any atom dividing x^n must be an associate of x. Hence, x is a strong atom. □

We note that Corollary 3.2 fails if the hypothesis that D is a ring of integers is dropped. While there are domains D with all atoms strong that are not UFDs, we are unaware of an elementary example. Many examples using the theory of Krull domains can be constructed using the main results of the recent paper [1].

If a ring of algebraic integers D is not a UFD, then D has atomic decay and the question arises how to arithmetically describe the different possible kinds of decay. A natural measure to consider is the *decay rate* of a nonzero nonunit $x \in D$, defined by

$$\vartheta(x) = \frac{k}{m}$$

where $x^m = x_1 \cdots x_k$ is the representation by decay (AD) according to Theorem 3.1 (ii). Notice that for any representation $x^n = y_1 \cdots y_l$ with strong atoms y_i one has that $\vartheta(x) = \frac{l}{n}$. Namely, $x^{mn} = (x_1 \cdots x_k)^n = (y_1 \cdots y_l)^m$ and by uniqueness $nk = ml$. The decay rate can be used to analyze two important invariants in the study of non-unique factorizations. If x is a nonzero nonunit of D, then the *elasticity* of x is defined by

$$\rho(x) = \sup\left\{ \frac{k}{l} \;\middle|\; x = a_1 \cdots a_k = b_1 \cdots b_l \text{ for atoms } a_1, \ldots, a_k, b_1, \ldots, b_l \text{ of } D \right\}$$

and the elasticity of D by

$$\rho(D) = \sup\{\rho(x) \mid x \text{ a nonzero nonunit of } D\}.$$

The elasticity of a ring of algebraic integers was first studied by Valenza [13]. Notice that if D is a UFD, then $\rho(x) = 1$ for each nonzero nonunit and hence $\rho(D) = 1$. The converse of this statement is false (see Corollary 4.2). Hence, an integral domain D with $\rho(D) = 1$ is known as a *half-factorial domain* or *HFD*. The following Corollary gives a relationship between the decay rate and elasticity.

Corollary 3.3. *Let D be the ring of integers of a number field.*

(i) $\vartheta(xy) = \vartheta(x) + \vartheta(y)$ *for nonzero nonunits* x, $y \in D$.

(ii) *D is half-factorial if and only if $\vartheta(x) = 1$ for all atoms x of D.*

(iii) *$\rho(D)$ is finite if and only if*

$$\sup\{\vartheta(x), \vartheta(x)^{-1} \mid x \text{ is an atom of } D\} < \infty.$$

Proof. (i) Let $x^m = x_1 \cdots x_k$, $y^n = y_1 \cdots y_l$ be the representations of x and y by atomic decay. Then

$$(xy)^{mn} = (x^m)^n (y^n)^m = (x_1 \cdots x_k)^n (y_1 \cdots y_l)^m.$$

From the uniqueness for the representations into strong atoms, we obtain

$$\vartheta(xy) = \frac{nk + ml}{mn} = \frac{k}{m} + \frac{l}{n} = \vartheta(x) + \vartheta(y).$$

(ii) ($\Rightarrow$) If D is half-factorial, then the representation $x^m = x_1 \cdots x_k$ implies $m = k$, that is, $\vartheta(x) = 1$. ($\Leftarrow$) If $x_1 \cdots x_k = y_1 \cdots y_l$ for atoms x_i y_j then by (i) it follows that

$$k = \sum_{i=1}^{k} \vartheta(x_i) = \sum_{j=1}^{l} \vartheta(y_j) = l.$$

(iii) ($\Rightarrow$) The representation $x^m = x_1 \cdots x_k$ implies $\frac{k}{m}$, $\frac{m}{k} \leq \rho(D)$ and hence if $C = \sup\{\vartheta(x), \vartheta(x)^{-1} \mid x \text{ an atom}\}$ then $C \leq \rho(D)$. ($\Leftarrow$) Let $x_1 \cdots x_k = y_1 \cdots y_l$ for atoms x_i, y_i. If $\vartheta(a) = \min \vartheta(x_i)$, $\vartheta(b) = \min \vartheta(y_j)$, then from (i) it follows that

$$k\vartheta(a) \leq \sum_{i=1}^{k} \vartheta(x_i) = \sum_{j=1}^{l} \vartheta(y_j) \leq l\vartheta(b).$$

Therefore, $\frac{k}{l} \leq \vartheta(b)\vartheta(a)^{-1}$ and C finite implies $\rho(D)$ is finite.   □

The point of Corollary 3.3 is that half-factoriality or finite elasticity can be checked for rings of algebraic integers by considering only special factorizations $a_1 \cdots a_k = b_1 \cdots b_l$ where on one side all the elements are equal. With the results thus far obtained, we consider more deeply in Section 4 the failure of nonunique factorization using an example which appears frequently in many entry level textbooks. We follow this in Section 5 with an even more striking example of non-uniqueness whose decay of atoms into strong atoms does not terminate.

4 The Fundamental Example of the Failure of Unique Factorization: $\mathbb{Z}[\sqrt{-5}]$

The ring

$$D = \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} \mid m, n \in \mathbb{Z}\}$$

is the ring of integers of the algebraic number field $\mathbb{Q}(\sqrt{-5})$. An example of non-unique factorization into atoms in D, is

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \qquad (*)$$

That the four elements involved are nonassociated atoms of D can be easily verified using the norm function

$$N(m + n\sqrt{-5}) = m^2 + 5n^2$$

which has the property that $N(xy) = N(x)N(y)$ for x, $y \in D$. For example, to see that $1 + \sqrt{-5}$ is an atom notice $N(1 + \sqrt{-5}) = 6$ and that $1 + \sqrt{-5} = xy$ implies $N(x), N(y) \in \{1, 2, 3, 6\}$. That $N(x) = 2$ or 3 is impossible and, hence, $N(x) = 1$ or 6. $N(x) = 1$ for $x \in D$ is an equivalent condition for x to be a unit of D. Therefore, x or y must be a unit which implies that $1 + \sqrt{-5}$ is an atom. Obviously, ± 1 are the units of D and, hence, $1 + \sqrt{-5}$ is not associated to any of the other factors of $(*)$. This non-unique factorization implies also that none of the four factors is a prime element of D. Obviously, for three of the factors, we have the following diagram outlining atomic decay.
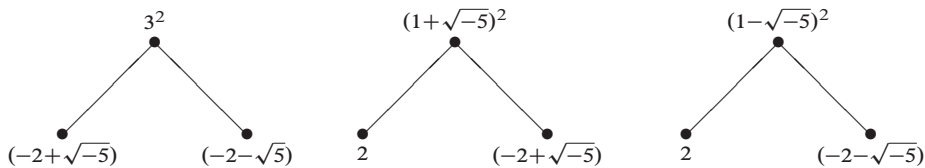
The factor 2 does not decay in a nontrivial way as shown by the following proposition.

Proposition 4.1. *The element* 2 *is a strong atom of* D *which is not prime in* D.

Proof. We have verified above that 2 is not prime in D. Suppose in D that an atom $x = m + n\sqrt{-5}$ divides a power 2^k. Then $N(x)$ must divide 2^{2k}, that is $m^2 + 5n^2 = N(x) = 2^l$ with $1 \leq l \leq 2k$. Consider this equation modulo 2. If exactly one of m and n is odd, then 2^l is odd, a contradiction. If m and n are both odd, then $m = 2m_1 + 1$ and $n = 2n_1 + 1$. Thus

$$(2m_1 + 1)^2 + 5(2n_1 + 1)^2 = 4w + 20v + 6 = 2^l$$

for integers w and v. Thus $2w + 10v + 3 = 2^{l-1}$ and $l = 1$. But $m^2 + 5n^2 = 2$ has no solutions in $\mathbb{Z}$. Thus, we must have that m and n are both even and, since x is an atom, it follows that $m = \pm 2$ and $n = 0$. Thus, any atom dividing a power of 2 in D must be equal to ± 2.   □

Below we will see that the other factors $-2 \pm \sqrt{-5}$ appearing in the diagram of atomic decay are strong atoms. Thus, by squaring the non-unique factorization $(*)$, we obtain a unique factorization of 6^2 into strong atoms (i.e., the representation of Theorem 3.1 (ii)). The decay diagram also shows that all atoms in $(*)$ have decay rate equal to 1. The common view of restoring uniqueness for equation $(*)$ is to use the Fundamental Theorem of Ideal Theory as follows (see [10, page 60]). The decompositions of the factors of $(*)$ into prime ideals are

$$(2) = P^2, \quad (3) = Q \cdot Q', \quad (1 + \sqrt{-5}) = P \cdot Q \quad \text{and} \quad (1 - \sqrt{-5}) = P \cdot Q'$$

with prime ideals

$$P = (2, 1 + \sqrt{-5}), \quad Q = (3, 1 + \sqrt{-5}) \quad \text{and} \quad Q' = (3, 1 - \sqrt{-5}).$$

Thus, by taking ideals in equation $(*)$, the non-uniqueness results from different groupings of the prime ideals P, Q and Q'. The above decompositions also show that the elements 2, $-2 \pm \sqrt{-5}$ are strong atoms. Namely, $(2) = P^2$ and $(2(-2 + \sqrt{-5})) = (1 + \sqrt{-5})^2 = P^2 Q^2$, hence, $(-2 + \sqrt{-5}) = Q^2$. Similarly, $(-2 - \sqrt{-5}) = Q'^2$. Therefore, according to Theorem 3.1 (i), 2 and $-2 \pm \sqrt{-5}$ are strong atoms. Thus, the representation by atomic decay (AD) according to Theorem 3.1 (ii) becomes for the element 6

$$6^2 = 2 \cdot 2 \cdot (-2 + \sqrt{-5})(-2 - \sqrt{-5}). \tag{$**$}$$

By using the Fundamental Theorem as above and some further techniques from [10] and [11] involving the *class group* of D, one can argue that the decay rate of all atoms in D is 1. Thus, using Corollary 3.3 and equation $(*)$, we obtain the following.

Corollary 4.2. *D is a half-factorial domain which is not a unique factorization domain.*

Carlitz [2] was the first to recognize that $\mathbb{Z}[\sqrt{-5}]$ is half-factorial. The interested reader can find many examples of half-factorial domains which are not UFD's as well as examples of domains exhibiting various values of elasticity in [6] and [8].

One is tempted to derive from $(**)$ a factorization of 6 itself by taking square roots. Of course, the complex roots obtained will in general not belong to D and are called *ideal numbers* with respect to D. More precisely, call a complex number α an *ideal prime number* for $\mathbb{Z}[\sqrt{-5}]$ if its square is a strong atom. Thus, complex numbers satisfying $\beta^2 = 2$, $\gamma^2 = -2 + \sqrt{-5}$ or $\delta^2 = -2 - \sqrt{-5}$ are ideal primes for $\mathbb{Z}[\sqrt{-5}]$. Taking roots with a positive sign, the square root of the (AD)-representation $(**)$ becomes $6 = \beta\beta\gamma\delta$. Of course, since by Theorem 3.1 (ii) the (AD)-representation is

unique up to units of D, that is ± 1, we obtain uniqueness for factorization into ideal primes only up to factors of fourth roots of 1. The non-unique factorization $(*)$ reads in ideal primes as

$$2 \cdot 3 = \beta\beta\gamma\delta = \beta\gamma \cdot \beta\delta = (1 + \sqrt{-5})(1 - \sqrt{-5}). \qquad (***)$$

Again, non-uniqueness results from different groupings, this time of ideal primes. The ideal primes can be described by ideals in D as follows. Consider for an ideal prime α the set

$$I(\alpha) = \{y \in D \mid y = \alpha\alpha', \alpha'^m \in D \text{ for some } m \in \mathbb{N}\}.$$

One verifies easily for $D = \mathbb{Z}[\sqrt{-5}]$ that $I(\beta) = \mathrm{rad}(2)$, $I(\gamma) = \mathrm{rad}(-2 + \sqrt{-5})$ and $I(\delta) = \mathrm{rad}(-2 - \sqrt{-5})$. Therefore, $I(\beta)$, $I(\gamma)$ and $I(\delta)$ are ideals in D given as radical ideals for strong atoms. By Theorem 3.1 (i), these 3 ideals are prime ideals. Indeed, one easily verifies that $I(\beta) = P$, $I(\gamma) = Q$ and $I(\delta) = Q'$. Ideal numbers were invented by E. E. Kummer (for the so called cyclotomic fields) prior to the invention of prime ideals by R. Dedekind. E. Hecke, who considered Kummer to be the creator of ideal theory ("Schöpfer der Idealtheorie," [7, page 87]) gave a construction of ideal numbers for the ring of integers of any number field. Though our definition of ideal prime numbers differs from Hecke's treatment, his discussion of another example seems quite similar [7, pages 83–86].

5 A More Striking Example

While factorization of elements into products of irreducible elements is not unique in $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[\sqrt{5}\iota]$, we were able to show for the example $(*)$ that atomic decay behaves in a finite manner. Namely, the decay of atoms reaches strong atoms just after one step, the decay rate equals 1 for all atoms and the elasticity of the domain equals 1. In this section, we construct an example of algebraic numbers where atomic decay is not as well mannered. The decay of the atoms involved will never end with strong atoms, infinitely many nonassociated atoms can divide the powers of a single atom and the elasticity $\rho(D)$ is infinite. Consider

$$\mathbb{Z}[5\iota] = \{m + 5n\iota \mid m, n \in \mathbb{Z}\}$$

which is a subdomain of $\mathbb{Z}[\iota]$, the domain of Gausssian integers. An example of non-unique factorization in $\mathbb{Z}[5\iota]$ is given by

$$5 \cdot 5 \cdot 5 = (5 + 10\iota)(5 - 10\iota). \qquad (\dagger)$$

All factors are nonassociated atoms in $\mathbb{Z}[5\iota]$ which is easily verified using the norm function $N(m + 5n\iota) = m^2 + 25n^2$ (see also Proposition 5.1 below). It is already clear from equation $(\dagger)$ that $\mathbb{Z}[5\iota]$ is neither factorial nor half-factorial. As for the example $(*)$ in $\mathbb{Z}[\sqrt{-5}]$, the factors in $(\dagger)$ further decay into atoms as can be seen from the following diagram.
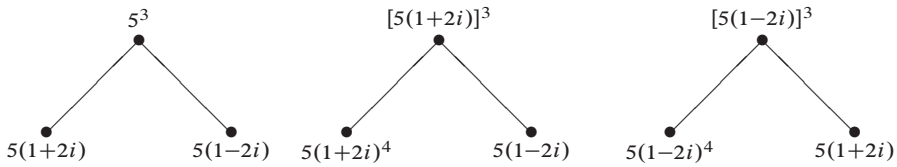
The equation (†) is just the decay of 5 in the above diagram. Thus, in a manner simpler than (∗), it is not necessary to square (†) to see that both sides of the equation contain the same atoms. In contrast to (∗), however, all the atoms created above by decay will decay further without reaching strong atoms. This will be demonstrated in Proposition 5.1 and is illustrated by the following diagram where all elements $a_k = 5(1 + 2\imath)^k$, $k \geq 0$, and their conjugates $\bar{a}_k$ are atoms.
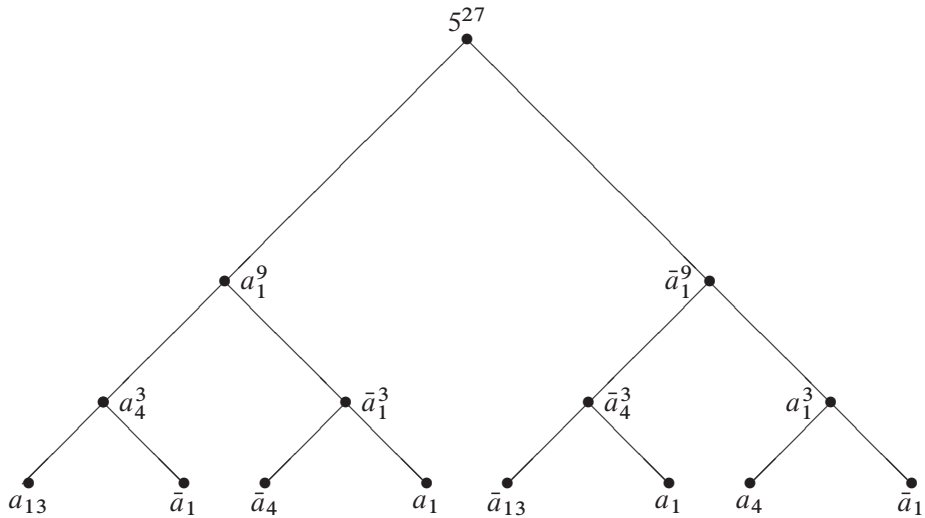
Proposition 5.1.   (i) *The elements $a_k = 5(1+2\imath)^k$, $k \geq 0$, are nonassociated atoms in $\mathbb{Z}[5\imath]$.*

(ii) *Any (proper) power of the atom a_k decays into exactly two nonassociated atoms, $a_k^p = a_{p(k+1)-2} \cdot \bar{a}_{p-2}$ for any $p \geq 2$, $k \geq 0$.*

(iii) *For each $k \geq 0$ the set of non-associated atoms dividing a_k^p for some $p \geq 0$ is infinite.*

(iv) *The elasticity of $\mathbb{Z}[5\imath]$ is infinite.*

Proof. (i) Using the Binomial Theorem we obtain

$$a_k = 5(1 + 2\imath)^k = \sum_{l=0}^{k} \binom{k}{l} 5(2\imath)^l$$

and hence $a_k \in \mathbb{Z}[5\imath]$. Obviously, $N(a_k) < N(a_l)$ for $k < l$ and, hence, the a_k are nonassociated. Suppose $5(1 + 2\imath)^k = (m + 5n\imath)(p + 5q\imath)$ is a factorization of a_k in $\mathbb{Z}[5\imath]$. Applying the norm function in $\mathbb{Z}[\imath]$ we obtain

$$N(5(1 + 2\imath)^k) = N(5) \cdot N(1 + 2\imath)^k = 5^{k+2} = (m^2 + 25n^2)(p^2 + 25q^2).$$

Therefore,

$$m^2 + 25n^2 = 5^a, \quad p^2 + 25q^2 = 5^b, \quad \text{and} \quad a + b = k + 2 \text{ for } a, b \in \mathbb{N}_0.$$

We shall show that either $a = 0$ or $b = 0$. Then $m + 5n\imath = \pm 1$ or $p + 5q\imath = \pm 1$ which proves that a_k is an atom. Suppose $a \geq 1$ and $b \geq 1$. Then $m = 5m'$, $p = 5p'$ and $5(1 + 2\imath)^k = 5(m' + n\imath)5(p' + q\imath)$. It follows that

$$(1 + 2\imath)^k = (1 + 2\imath)(1 - 2\imath)(m' + n\imath)(p' + q\imath).$$

Hence, $k \geq 2$ and

$$(1 + 2\imath)^{k-1} = (1 - 2\imath)(m' + n\imath)(p' + q\imath).$$

Now, we can write $1 + 2\imath = (1 - 2\imath)(-1 + \imath) - \imath$ to obtain by the Binomial Theorem

$$(1 + 2\imath)^{k-1} = (1 - 2\imath) \sum_{l=1}^{k-1} \binom{k-1}{l} (1 - 2\imath)^{l-1}(-1 + \imath)^l (-\imath)^{k-1-l} + (-\imath)^{k-1}.$$

Therefore, $(-\imath)^{k-1} = (1 + 2\imath)^{k-1} - (1 - 2\imath)\alpha$ with $\alpha \in \mathbb{Z}[\imath]$ and, combining we obtain

$$(-\imath)^{k-1} = (1 - 2\imath)(m' + n\imath)(p' + q\imath) - (1 - 2\imath)A = (1 - 2\imath) \cdot \beta$$

with $\beta \in \mathbb{Z}[\imath]$. Multiplying the two sides of this equation by its conjugate, we obtain $1 = 5 \cdot \beta\bar{\beta}$, which is impossible.

(ii) By definition

$$
\begin{aligned}
a_{p(k+1)-2} \bar{a}_{p-2} &= 5(1 + 2\imath)^{p(k+1)-2} 5(1 - 2\imath)^{p-2} \\
&= 5^2 [(1 + 2\imath)(1 - 2\imath)]^{p-2}(1 + 2\imath)^{pk} \\
&= 5^2 5^{p-2}(1 + 2\imath)^{pk} \\
&= a_k^p.
\end{aligned}
$$

(iii) Is immediate from (ii) and (i).
(iv) Is immediate from (ii) and the definition of elasticity. □

Putting $p = 3$ in Proposition 5.1 (ii), one obtains $a_k^3 = a_{3(k+1)-2} \cdot \overline{a}_1$ which is the formula that generates the atomic decay depicted in the diagram Figure 3. Though at first the domain $\mathbb{Z}[5\iota]$ may seem simpler than the domain $\mathbb{Z}[\sqrt{-5}]$, Proposition 5.1 shows that the opposite is the case with respect to atomic decay. In $\mathbb{Z}[5\iota]$, as in $\mathbb{Z}[\sqrt{-5}]$, each nonzero nonunit is a product of atoms, as can again be seen using the norm function. Also, there are strong atoms in $\mathbb{Z}[5\iota]$, for instance 2, as can be seen from the same argument used in Proposition 4.1. But $\mathbb{Z}[5\iota]$ differs from $\mathbb{Z}[\sqrt{-5}]$, as there are not enough strong atoms to represent all elements by atomic decay.

6 Concluding Remarks and Questions

In this paper, we argue that non-unique factorization into atoms descends from atomic decay. Of course, by its very definition an atom cannot be broken up into parts, but after taking powers of an atom, atomic decay can occur, in which case unique factorization fails. For the ring of integers of an algebraic number field, we proved using atomic decay, that for each nonzero nonunit element some power can be factored uniquely (up to order and associates of factors) into strong atoms. In this sense, unique factorization is restored by forcing atoms to decay into strong atoms which can no longer decay. In particular, unique factorization into atoms is possible precisely if each atom is a strong atom. Also, the properties of half-factoriality and finite elasticity descend from atomic decay and can be described by the decay rates of atoms. The decay behavior may differ very much for different rings of algebraic integers. In one example we found decay ending with strong atoms after finitely many steps. In another, the decay turned out to be much more drastic and never ended with strong atoms. As a tool we employed the Fundamental Theorem of Ideal Theory and some well-known related simple properties. Is it possible to obtain unique factorization into strong atoms in a more direct way, without these tools? One might think of "extracting" strong atoms out of atoms in finitely many steps. Can this be done in an elementary way? For an indirect and non-elementary example employing "extraction" see [3]. Also, is it possible to check if a given atom is strong in a direct way? That is, using the norm function but not ideal theory. We did this in the case $\mathbb{Z}[\sqrt{-5}]$ for the element 2, but for other elements we needed ideal theory. In such investigations, the interesting question arises whether for a (rational) prime number p a prime power p^l is of the form $m^2 + k n^2$ for given $k \in \mathbb{N}$. Finally, though we touched upon historical issues in the paper there are further interesting questions here. We mentioned Kummer's ideal numbers, as seen by Hecke, and connected these to strong atoms. It has been argued that Kummer's ideal numbers developed from the work of C. G. J. Jacobi (see the recent paper [9] and the references therein). Do Jacobi's "wahre complexe Primzahlen" (true complex prime numbers) connect in any way to the notion of strong atom?

Bibliography

[1] Baginski, P., Kravitz, R., A new characterization of half-factorial Krull domains. J Algebra Appl. 2010;9:825–837.

[2] Carlitz, L., A characterization of algebraic number fields with class number two. Proc Amer Math Soc. 1960;11:391–392.

[3] Chapman, S. T., Halter-Koch, F., Krause, U., Inside factorial monoids and integral domains. J Algebra. 2002;252:350–375.

[4] Chapman, S. T., Krause, U., Cale monoids, Cale domains and Cale varieties. In: Arithmetical properties of commutative rings and monoids. vol. 241 of Lecture notes in pure and applied mathematics. 2005. p. 142–171.

[5] Gallian, J., Contemporary abstract algebra. 7th ed. New York: Brooks Cole Publishing Company; 2009.

[6] Geroldinger, A., Halter-Koch, F., Non-unique factorizations: algebraic, combinatorial and analytic theory. vol. 278 of Pure and applied mathematics. Chapman & Hall/CRC; 2006.

[7] Hecke, E., Vorlesungen über die Theorie der Algebraischen Zahlen. New York: Chelsea Publishing Company; 1970 [1st ed. Leipzig; 1923].

[8] Kim, H., Examples of half-factorial domains. Canad Math Bull. 2000;43:362–367.

[9] Lemmermeyer, F., Jacobi and Kummer's ideal numbers. Abh Math Semin Univ Hamburg. 2009;79:165–187.

[10] Marcus, D. A., Number fields. New York: Springer-Verlag; 1977.

[11] Pollard, H., Diamond, H., The theory of algebraic numbers. vol. 9 of The Carus Mathematical Monographs. Providence, RI: The Mathematical Association of America; 1975.

[12] Rush, D. E., An arithmetic characterization of algebraic number fields with given class group. Math Proc Cambridge Philos Soc. 1983;94:23–28.

[13] Valenza, R., Elasticity of factorization in number fields. J Number Theory. 1990;36(2): 212–218.

Author Information

Scott T. Chapman, Department of Mathematics and Statistics, Sam Houston State University, Huntsville, TX, USA.
E-mail: scott.chapman@shsu.edu

Ulrich Krause, Fachberich Mathematik und Informatik, Universität Bremen, Bremen, Germany.
E-mail: krause@math.uni-bremen.de