Combinatorial and Homological Aspects of Monomial Algebras and Numerical Semigroups

Dylan Carl Beck

B.S., Mathematics with Honors, Missouri State University, 2016

M.A., Mathematics, University of Kansas, 2018

Submitted to the graduate degree program in the Department of Mathematics and the Graduate Faculty of the University of Kansas in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Committee members

Hailong Dao, Chairperson

Daniel Katz

Jeremy Martin

Emily Witt

Eileen Nutting, Philosophy

Date defended: 3 May 2022

The Thesis Committee for Dylan Carl Beck certifies
that this is the approved version of the following thesis:

Combinatorial and Homological Aspects of Monomial Algebras and Numerical Semigroups

Hailong Dao, Chairperson

Date approved: 10 May 2022

Abstract

Our aim throughout this thesis is to illuminate combinatorial and homological properties of algebraic structures arising in combinatorial commutative algebra, combinatorics, and additive number theory. We devote specific attention to Noetherian (standard graded) local rings (with infinite residue fields) that admit desirable properties, e.g., analytically unramified one-dimensional Cohen-Macaulay local rings and monomial algebras such as (i.) numerical semigroup rings, (ii.) edge rings of finite simple graphs, and (iii.) generalized two-dimensional Veronese subrings. We introduce two new classes of non-Gorenstein Cohen-Macaulay local rings — namely the Gorenstein canonical blow-up (GCB) rings and divisive numerical semigroup rings — in Chapter 3. We demonstrate that Arf rings, far-flung Gorenstein rings, nearly Gorenstein rings of minimal multiplicity, numerical semigroup rings of multiplicity at most three, and divisive numerical semigroup rings are GCB. We define two new invariants of Noetherian (standard graded) local rings in Chapter 4. We illustrate that these invariants refine the notion of embedding dimension and relate to reductions of the maximal ideal of reduction number one. We provide general bounds for these invariants and compute them explicitly in some cases. We offer a treatise on the invariants for standard graded algebras over fields and edge rings of finite simple graphs, and we demonstrate that these invariants give rise to subtle algebraic invariants of finite simple graphs. Last, in Chapter 5, we introduce a generalization of two-dimensional Veronese subrings — called pseudo-Veronese subrings — and we prove that their homological properties are determined by the underlying monomial generators.

Acknowledgements

To my best friend Michelle Pellegrino, I cannot thank you enough for your assistance, understanding, appreciation, and patience. Our consistent efforts to better each other have filled the past decade with cherished memories, unbridled joy, and moments of bittersweet humanity.

To our cats Gwen and Eve, thank you for the cuddles, affection, laughs, and smiles. One of the most fulfilling reasons to take a break from writing this thesis has been to give the two of you some attention, e.g., in the form of a conversation, a belly rub, or a game of hide-and-seek.

To my only sister Brittany Beck Kingery, I owe a large part of my success. Over the years, you have demonstrated confidence, expertise, and a genuine willingness and excitement to help — especially during the graduate school application process. I believe sincerely that you are rooting for me and that you are proud of what I have accomplished. We are very much the same.

To my nephews Charlie Knox and Kieran Beckett, I hope that you two will view the completion of this thesis as an endorsement of all that you are capable of accomplishing. I am very excited to continue to seek to understand, cherish, and support you both as you learn and grow.

To Souvik Dey, I extend my unceasing amazement, admiration, and appreciation. Enjoying first-hand your creativity and unparalleled brilliance, I learned how to conduct mathematical research; how to ask interesting questions; how to argue elegantly; and when to question the ostensibly obvious. Even more, I thank you for your kind affirmation, unfailing assistance, and humor.

To Ben Gershon, I tip my cap. I will always cherish the hilarity, absurdity, and simplicity you instilled in our office space together. Ever since we met, you have remained a trustworthy, compassionate, and dignified colleague, and I thank you for your support and confidence. Certainly, you have enriched my life with your friendship, and I hope that you would say the same of mine.

To Lucian Grand, I express my deepest gratitude and respect. Truly, your generosity knows no bounds, and I am consistently in awe of your tangible humanity — most notable in your inextri-

cable humor and palpable understanding of the bittersweet nature of life. I am forever indebted to you for your friendship and especially for your mentorship as a fellow teacher.

To John Portin, thank you for your genuine interest in and understanding of me as a human. Our conversations and outings as first-years provided comic relief from the stressful and sometimes dehumanizing conditions of graduate school. I will fondly remember the door bells that chimed at the House of Chá on Ninth and Vermont and the taste of taro-flavored bubble tea. Further, I appreciate your patience in introducing me to typesetting my assignments and papers in LaTeX.

To Lucas Schauer, I hold dear our friendship for all time, and I thank you for countless moments of levity and silliness during our marathon study sessions in our early years of graduate school. In the words of Lil Wayne, "You know you at the top when only Heaven's right above it. We on."

To Trevor Arrigoni, Debjit Basu, Monalisa Dutta, Ryan Hunter, Ritika Nair, Wayne Ng Kwing King, Enrique Salcido, and Christopher Wong, you are my academic family. I thank you for your attention and participation in the Graduate Student Algebra Seminar, and I hope that I have made a positive impact on each of you in some way — in your education and in your lives.

To Mark Denker, Conner Emberlin, and Jayan Mukherjee, I am honored that we could occupy the same time and space together. Mark, you have a warmth and an inviting enthusiasm for discourse that is contagious. Conner, your impeccable music taste and insatiable appetite for social justice propelled me to step out of my comfort zone and to use my privilege for the betterment of society. Jayan, your understated humor and humanity always brightened my afternoons.

To Ken Duna and Nick Ma, your expertise in matters of Bridge and navigating the often murky waters of obtaining a mathematics Ph.D. ensured that I did not fail along this journey.

To Promit Kundu, Debaditya Raychaudhury, and Prashanth Sridhar, I will always cherish the contagious laughter and rustic humor you brought to the various rooms of Snow Hall.

To Daniel James, I am eternally grateful to you for instilling in me the awareness, knowledge, and passion to continue to grow into an effective and thoughtful educator.

To Jeremy Martin, thank you for your consistent reassurance and your camaraderie. Early on, you convinced and reaffirmed to me that I belonged in the mathematics department at the

University of Kansas, but more importantly, you continued to provide assistance, patience, and an interested ear throughout my years as a graduate student. I cannot express my gratitude enough.

To Jila Niknejad, you are one of the most kind and genuine individuals I have ever known; your humility, humor, and humanity are inestimable. Over the years — during which I have had the repeated privilege and honor to collaborate and grow with you as an educator and a human — you have demonstrated the critical importance of grace and understanding as a teacher.

To Kerrie Brecheisen, Kate Pleskac, Gloria Prothe, and Lori Springs, thank you for your time and consideration. Everything I have accomplished throughout the years in the mathematics department at the University of Kansas has been in part due to your tireless organizational efforts.

To Hailong Dao, I confess my perpetual amazement and appreciation. Consistently, I stand in awe of your creativity and mathematical intuition. Crucially, you have provided countless fruitful ideas, comments, and suggestions without which this thesis would not be possible. Even more, your humor, charm, humanity, laughter, and reassurance never failed to uplift each moment.

To Daniel Katz, Eileen Nutting, and Emily Witt, I am honored to have you as members of my thesis committee. Thank you for your encouragement, interest, and service.

To Leslie Reid, Garrett Rucker, Kishor Shah, and Vera Stanojevic, I am eternally grateful for your thoughtful guidance and kind influence as my first mathematical mentors. Because of you all, the once latent spark of mathematical ability was ignited within me, and I felt the confidence and security grow into and identify as the vigorous mathematician that I am today.

I dedicate this to my grandparents **Frank and Gloria Beck** and **Carlo and Angelina Dellaquila**.

Contents

Chapter 1

Introduction

1.1 What Is Commutative Algebra?

Commutative algebra can be viewed literally as the study of objects for which addition and multiplication can be defined in a manner such that the order in which two things are added or multiplied is interchangeable. Put another way, commutative algebraists study any collection of objects R with the property that for every pair of elements $r, s \in R$, there are associative binary operations $+ : R \times R \to R$ and $\cdot : R \times R \to R$ that satisfy $r + s = s + r$ and $r \cdot s = s \cdot r$. Even more, we impose the additional requirements that there exist elements $0_R, 1_R \in R$ such that $0_R + r = r$ and $1_R \cdot r = r$ for any element $r \in R$, and for every element $r \in R$, there exists an element $-r \in R$ such that $-r + r = 0_R$. Under these conditions, one can show that the elements 0_R and 1_R are unique, and for any element $r \in R$, the element $-r$ is unique. Consequently, we distinguish these elements by name: 0_R is the **additive identity** of R; 1_R is the **multiplicative identity** of R; and $-r$ is the **additive inverse** of r. We refer to the set R as a **commutative unital ring**; the term "commutative" stems from the assumption that multiplication of any two elements of R "commutes," and the term "unital" is derived from the existence of the multiplicative identity (or "unity") 1_R. One can readily verify that the collection $\mathbb{R}[x]$ of polynomials in indeterminate x with real coefficients is an example of a commutative unital ring with additive identity 0 and multiplicative identity 1.

Understanding the fundamental and often subtle differences between two commutative unital rings forms a central problem in commutative algebra. One might recognize that the univariate polynomial ring with real coefficients $\mathbb{R}[x]$ and the univariate polynomial ring with complex coefficients $\mathbb{C}[x]$ are distinct commutative unital rings because the polynomial $x^2 + 1$ does not have a

nontrivial factorization in $\mathbb{R}[x]$ and yet $(x-i)(x+i)$ is a nontrivial factorization in $\mathbb{C}[x]$; however, the task of distinguishing two commutative unital rings from one another can be quite subtle even in familiar settings. For instance, the author is not immediately aware of a high school-level argument that the bivariate polynomial ring with real coefficients $\mathbb{R}[x,y]$ and the trivariate polynomial ring with real coefficients $\mathbb{R}[x,y,z]$ are distinct as commutative unital rings.

Consequently, it is natural to associate to a commutative unital ring R additional structures that allow us to differentiate between R and rings that are "fundamentally different" from R. We say that a nonempty set $I \subseteq R$ is an **ideal** of R if the associative binary operation $+ : R \times R \to R$ restricts to an associative binary operation $+ : I \times I \to I$ and the associative binary operation $\cdot : R \times R \to R$ restricts to an associative binary operation $\cdot : R \times I \to I$. Observe that if 1_R lies in I, then the second requirement implies that $r = r \cdot 1_R$ belongs to I for all elements $r \in R$, hence we say that I is a **proper** ideal if $1_R \notin I$. We refer to functions between commutative unital rings that preserve their ring structure as **ring homomorphisms**. Explicitly, a function $\varphi : R \to S$ between two commutative unital rings is a ring homomorphism if and only if $\varphi(r+s) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = \varphi(r)\varphi(s)$ hold for any elements $r,s \in R$ and $\varphi(1_R) = 1_S$. Even more, the study of commutative unital ring homomorphisms allows us to rigorously codify what is meant by "indistinguishable" commutative unital rings — namely, the commutative unital rings R and S are "indistinguishable" if there exists a bijective ring homomorphism $\varphi : R \to S$. We say in this case that R and S are **isomorphic** as commutative unital rings, and we write $R \cong S$. Using the theory of ideals and ring homomorphisms, one can rigorously demonstrate that $\mathbb{R}[x,y]$ and $\mathbb{R}[x,y,z]$ are "fundamentally different" commutative unital rings, i.e., they are not isomorphic. We will see in Chapter 2 that this is due, e.g., to the fact that $\mathbb{R}[x,y]$ and $\mathbb{R}[x,y,z]$ have different Krull dimension (cf. Definition 2.1.28 and Proposition 2.1.33), but an undergraduate student in abstract algebra could provide an even simpler proof.

Even more subtle questions than this require more sophisticated machinery and techniques. Case in point, if we restrict our attention to the real polynomials that can be constructed from the monomials x^4, x^5, and x^6, then the resulting commutative unital ring $\mathbb{R}[x^4,x^5,x^6]$ is distinct from the commutative unital ring $\mathbb{R}[x^4,x^5,x^7]$ obtained by restricting our attention to the real polynomials

that can be constructed from the monomials x^4, x^5, and x^7; however, the reason that these two commutative unital rings are "fundamentally different" is far from obvious to the author. Perhaps the simplest rationale is that the **numerical semigroup** $\langle 4,5,6\rangle$ is **symmetric** but the numerical semigroup $\langle 4,5,7\rangle$ is not symmetric (cf. Definition 2.4.16), but even this requires serious work.

Beneath the examples discussed in the previous paragraphs lies a very interesting and fundamental problem in commutative algebra: the classification of commutative unital rings. We learn in an undergraduate modern algebra course that certain commutative unital rings can be categorized as fields, Euclidean domains, principal ideal domains, or unique factorization domains in a manner such that each class of commutative unital rings constitutes a strict subclass of the subsequent class of rings — namely, this is the stratification of integral domains. One other fascinating classification problem is the stratification of Cohen-Macaulay local rings. Currently, it is well-known that any regular local ring is a local complete intersection; any local complete intersection is a Gorenstein local ring; any Gorenstein local ring is a Cohen-Macaulay local ring; and none of these implications can be reversed in general. One of the central focuses of this thesis is to examine the distinction between Gorenstein local rings and Cohen-Macaulay local rings. Explicitly, Chapter 3 investigates certain well-known classes of one-dimensional non-Gorenstein Cohen-Macaulay local rings and exhibits two generalizations of some of these classes to a larger family of rings.

On its own, commutative algebra hosts many interesting and challenging unresolved questions; however, the techniques inherent to the field can also be used to study objects arising in combinatorics, geometry, number theory, and topology. We invite the reader to peruse our discussions of Graph Theory and Semigroup Theory for two concrete examples illustrating these connections.

Ultimately, therefore, it is this desire to untangle and distinguish commutative unital rings that propels the bulk of this thesis forward; however, we will see along the way that these classification questions forge many delightful and sometimes surprising connections to neighboring fields.

1.2 Overview of the Main Results

Our goal throughout this thesis is to make our work understandable to any reader with only an understanding of undergraduate modern algebra. Bearing this in mind, Chapter 2 is devoted to providing the necessary tools to ensure that the subsequent materials lie within the scope of this document. Once we have discussed a modest amount of the requisite knowledge in commutative algebra, we turn our attention to the third, fourth, and fifth chapters. We point out that these consist of original work by the author and his co-authors. One can find the results of these chapters in the papers [BD22a], [BD22b], and [Bec22] that are now (or may later become) available on the arXiv.

We assume throughout Chapter 3 that $(R,\mathfrak{m},k)$ is an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k, total ring of fractions $Q(R)$, integral closure $\overline{R}$, and conductor $(R:\overline{R})$. Under these conventions, it is well-known that R enjoys many nice properties. Explicitly, we note that $\overline{R}$ is a regular ring that is finitely generated as an R-module (cf. Propositions 2.1.69, 2.1.163, and 2.1.162, respectively). Even more, every $\mathfrak{m}$-primary ideal of R admits a principal reduction (cf. [HS06, Corollary 8.3.9]). Crucially, R admits a canonical ideal ω_R that is regular of finite colength (cf. Propositions 2.2.66, 2.2.71, and 2.2.16, respectively).

Our objective in this chapter is to exhibit a natural generalization of several interesting classes of one-dimensional non-Gorenstein Cohen-Macaulay local rings. Barucci and Fröberg introduced and subsequently studied in 1997 a class of analytically unramified one-dimensional Cohen-Macaulay local rings called **almost Gorenstein** that are characterized by the existence of an R-module isomorphism $\mathfrak{m}\omega_R \cong \mathfrak{m}$ (cf. [BF97, Definition-Proposition 20]). Observe that if R is Gorenstein, then $\omega_R \cong R$ implies that $\mathfrak{m}\omega_R \cong \mathfrak{m}$, i.e., R is almost Gorenstein (cf. Theorem 2.2.67). Conversely, the numerical semigroup ring $k[\![x^4,x^7,x^9]\!]$ is almost Gorenstein but not Gorenstein.

Later, in 2019, a paper [HHS19] of Herzog, Hibi, and Stamate considered another class of Cohen-Macaulay local rings for which a canonical module exists. Let $M^* = \mathrm{Hom}_R(M,R)$ denote the collection of R-module homomorphisms from an R-module M to R. We define the **trace** $\mathrm{tr}(M)$

of M as the ideal of R generated by the homomorphic images of M in R, i.e., we have that

$$\operatorname{tr}(M) = \sum_{\varphi \in M^*} \varphi(M) = \{\varphi(x) \mid x \in M \text{ and } \varphi \in M^*\}.$$

We refer to $\operatorname{tr}(\omega_R)$ as the **canonical trace ideal**. One can verify that the canonical trace ideal of R controls the non-Gorenstein locus of R, i.e., R_P is not Gorenstein if and only if $P \supseteq \operatorname{tr}(\omega_R)$ (cf. [HHS19, Lemma 2.1]). Consequently, Herzog, Hibi, and Stamate refer to R as **nearly Gorenstein** if it holds that $\operatorname{tr}(\omega_R) \supseteq \mathfrak{m}$ (cf. [HHS19, Definition 2.2]). Observe that if R is almost Gorenstein, then the inclusions $\mathfrak{m} \subseteq \operatorname{tr}(\mathfrak{m}) = \operatorname{tr}(\mathfrak{m}\omega_R) = \mathfrak{m}\operatorname{tr}(\omega_R) \subseteq \operatorname{tr}(\omega_R)$ hold: indeed, the first inclusion is induced by $\mathfrak{m} \subseteq R$; the first equality holds by the isomorphism $\mathfrak{m}\omega_R \cong \mathfrak{m}$; and the second equality holds by the fact that any R-module homomorphism is R-linear. Conversely, the numerical semigroup ring $k[\![x^4, x^5, x^{11}]\!]$ is nearly Gorenstein but not almost Gorenstein. By [HHS19, Theorem 6.6], any nearly Gorenstein ring of minimal multiplicity is almost Gorenstein, hence the one-dimensional nearly Gorenstein and almost Gorenstein rings of minimal multiplicity coincide.

Even more recently, the notion of **far-flung Gorenstein** was introduced by Herzog, Kumashiro, and Stamate (cf. [HKS21, Definition 2.3]). Explicitly, a one-dimensional Cohen-Macaulay local ring R that admits a canonical module is far-flung Gorenstein if $\operatorname{tr}(\omega_R) = (R : \overline{R})$. Observe that a non-Gorenstein ring R that is both nearly Gorenstein and far-flung Gorenstein satisfies $(R : \overline{R}) \supseteq \mathfrak{m}$. Conversely, if $(R : \overline{R}) \supseteq \mathfrak{m}$, then the inclusions $(R : \overline{R}) \subseteq (R : C) \subseteq (R : C)C = \operatorname{tr}(C) = \operatorname{tr}(\omega_R)$ hold for any canonical module of R such that $R \subseteq C \subseteq \overline{R}$ (cf. the fifth part of [HKS21, Remark 2.1]).

Our main theorem of Chapter 3 is the following observation regarding the **canonical blow-up**

$$B(\omega_R) = \bigcup_{n \geq 0} (\omega_R^n : \omega_R^n) = \{\alpha \in Q(R) \mid \alpha\omega_R^n \subseteq \omega_R^n \text{ for some integer } n \geq 0\}.$$

Theorem 1.2.1 (Theorems 3.1, 3.3.15, and 3.4.4)**.** *Let $(R, \mathfrak{m}, k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k and canonical ideal ω_R. If any of the following hold, then $B(\omega_R)$ is Gorenstein, and we say that R is* **blow-up Gorenstein**.

(a.) *R is Arf.*

(b.) *R is nearly Gorenstein of minimal multiplicity.*

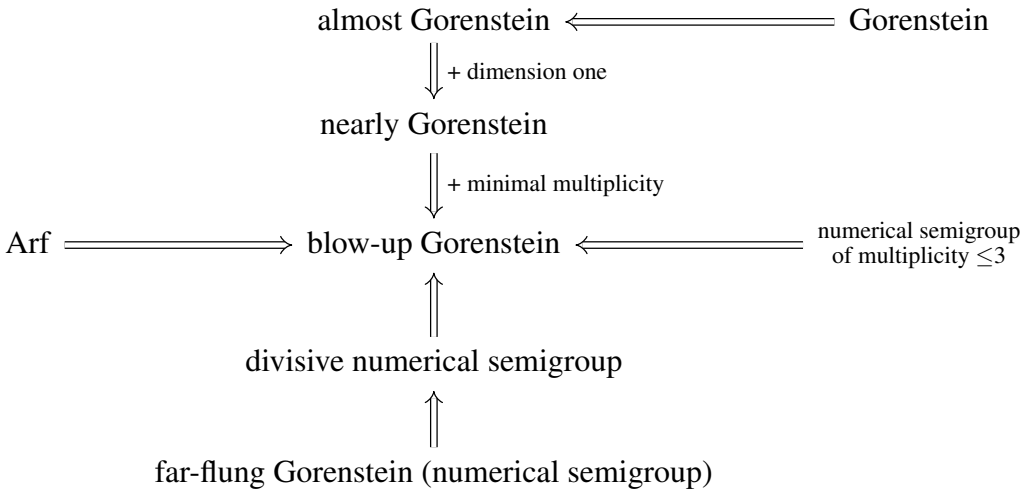
(c.) *R is almost Gorenstein of minimal multiplicity.*

(d.) *R is far-flung Gorenstein.*

(e.) *R is a numerical semigroup of multiplicity at most three.*

(f.) *R is a divisive numerical semigroup (cf. Definition 3.4.3).*

Essentially, our work illustrates that the family of analytically unramified one-dimensional rings for which the canonical blow-up of R is Gorenstein contains many interesting classes of singularities. One can perhaps best appreciate Theorem 1.2.1 in terms of the following diagram.



We prove moreover that the canonical blow-up $B(\omega_R)$ is itself an interesting construction that provides useful information about the singularities of the underlying ring R.

Theorem 1.2.2 (Theorem 3.2.21)**.** *Let $(R,\mathfrak{m},k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k and canonical ideal ω_R. The following conditions are equivalent.*

(i.) *R is regular.*

(ii.) *We have that $B(\omega_R) = \overline{R}$.*

(iii.) *We have that* $(R : B(\omega_R)) = (R : \overline{R})$.

(iv.) *We have that* $\omega_R^n \cong (R : \overline{R})$ *for some integer* $n \gg 0$.

Theorem 1.2.3 (Theorem 3.2.15)**.** *Let* $(R, \mathfrak{m}, k)$ *be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field* k *and canonical ideal* ω_R*. The following conditions are equivalent.*

(i.) *R is Gorenstein.*

(ii.) *We have that* $B(\omega_R) = R$.

(iii.) *We have that* $(R : B(\omega_R)) = R$.

Proposition 1.2.4 (Proposition 3.2.18)**.** *If* $(R, \mathfrak{m}, k)$ *is an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field* k *and canonical ideal* ω_R*, then R is almost Gorenstein if and only if* $(R : B(\omega_R)) \supseteq \mathfrak{m}$.

Ubiquitous in the study of analytically unramified one-dimensional Cohen-Macaulay local rings are the **numerical semigroup rings** (cf. Sections 2.4.2 and 2.4.3). Even though these objects are simple to describe and can be understood by undergraduate mathematics students, they exhibit subtle properties and provide a wealth of examples of non-Gorenstein Cohen-Macaulay local rings. Based on the work of Herzog in [Her69], it is well-known that a numerical semigroup ring is Gorenstein if and only if the corresponding numerical semigroup is **symmetric** (cf. Definition 2.4.16 and the subsequent propositions). Every numerical semigroup of embedding dimension two is symmetric, hence every numerical semigroup of **multiplicity** two is symmetric (cf. Proposition 2.4.19). Consequently, the condition that a numerical semigroup S is Gorenstein but not regular is equivalent to the condition that S has embedding dimension two. Extensive efforts in recent years have been made to understand certain classes of non-symmetric numerical semigroups (cf. [BF97], [MS21], and [HKS21]). Our work on numerical semigroups in Chapter 3 extends the results of the aforementioned authors to a new class of non-symmetric numerical semigroups we call **blow-up Gorenstein**; they form a natural generalization of the notion of symmetric in the following sense.

Theorem 1.2.5 (Proposition 3.3.15)**.** *Every numerical semigroup of multiplicity at most three is blow-up Gorenstein. Even more, a numerical semigroup is blow-up Gorenstein but not Gorenstein if and only if it has maximal embedding dimension three.*

Even more, we introduce the class of **divisive numerical semigroups** for which the canonical blow-up is regular (cf. Definition 3.4.3). By [HKS21, Proposition 6.1], it follows that the divisive numerical semigroups strictly contain the class of far-flung Gorenstein numerical semigroups defined by Herzog-Kumashiro-Stamate (cf. Proposition 3.4.2). Last, we completely classify all divisive numerical semigroups that (a.) are generated by an interval (cf. Proposition 3.4.12) or (b.) have maximal embedding dimension (cf. Proposition 3.4.14).

Chapter 4 is devoted to the introduction and study of two new invariants of Noetherian (standard graded) local rings that refine the notion of **embedding dimension** and provide insight into the **reductions** of the maximal ideal of reduction number one. We assume throughout the chapter that $(R,\mathfrak{m},k)$ is a Noetherian local ring with residue field k. If $R=\bigoplus_{i\geq 0}R_i$ is standard graded, then we impose the further conditions that R_0 is a field; $R=R_0[R_1]$ is an R_0-algebra that is finitely generated by elements of degree one; and $\mathfrak{m}=\bigoplus_{i\geq 1}R_i$ is the homogeneous maximal ideal of R. Our new invariants are related to the square of the maximal ideal and are defined as follows.

$$\operatorname{cs}(R)=\min\{\mu(I)\mid I \text{ is a (homogeneous) proper ideal of } R \text{ such that } I^2=\mathfrak{m}^2\} \text{ and}$$
$$\operatorname{ms}(R)=\min\{\mu(I)\mid I \text{ is a (homogeneous) proper ideal of } R \text{ such that } I\supseteq\mathfrak{m}^2\}.$$

One can verify immediately that the inequalities $\operatorname{ms}(R)\leq\operatorname{cs}(R)\leq\mu(\mathfrak{m})$ hold. Even more, by Krull's Height Theorem, we have that $\dim(R)=\operatorname{ht}(\mathfrak{m})=\operatorname{ht}(I)\leq\mu(I)=\operatorname{ms}(R)$ for any (homogeneous) proper ideal I that satisfies $I\supseteq\mathfrak{m}^2$ and $\mu(I)=\operatorname{ms}(R)$. We devote the second section of Chapter 4 to demonstrating that $\operatorname{cs}(R)$ and $\operatorname{ms}(R)$ are satisfied by sufficiently many (homogeneous) elements of $\mathfrak{m}\setminus\mathfrak{m}^2$ (cf. Propositions 4.2.2 and 4.2.3). Even more, these invariants enjoy many desirable properties with respect to ring operations that make their computation more tractable.

Proposition 1.2.6 (Propositions 4.2.10, 4.2.11, 4.2.15, 4.2.18, and 4.2.19)**.** *Let* $(R,\mathfrak{m})$ *and* $(S,\mathfrak{n})$

be Noetherian (standard graded) local ring. The following properties hold.

(1.) *If* $\varphi : R \to S$ *is a surjective (graded) homomorphism, then* $\operatorname{cs}(R) \geq \operatorname{cs}(S)$ *and* $\operatorname{ms}(R) \geq \operatorname{ms}(S)$.

(2.) *If* I *is a (homogeneous) proper ideal of* R, *then* $\operatorname{ms}(R/I) \leq \operatorname{ms}(R) \leq \operatorname{ms}(R/I) + \mu(I)$.

(3.) *If* R *is a standard graded algebra over its residue field and* $X_1, \ldots, X_n$ *are any indeterminates over* R, *then* $\operatorname{ms}(R[X_1, \ldots, X_n]) = \operatorname{ms}(R) + n$.

(4.) *If* R *is standard graded with homogeneous maximal ideal* $\mathfrak{m}$, *then* $\operatorname{ms}(R) = \operatorname{ms}(R_{\mathfrak{m}})$.

(5.) *If* $\widehat{R}$ *is the* $\mathfrak{m}$*-adic completion of* R, *then* $\operatorname{cs}(\widehat{R}) = \operatorname{cs}(R)$ *and* $\operatorname{ms}(\widehat{R}) = \operatorname{ms}(R)$.

General bounds and extremal equalities among the invariants $\dim(R) \leq \operatorname{ms}(R) \leq \operatorname{cs}(R) \leq \mu(\mathfrak{m})$ are explored in the third section of the chapter, where our main proposition is the following.

Proposition 1.2.7 (Proposition 4.3.3)**.** *Let* $(R, \mathfrak{m})$ *be a Noetherian (standard graded) local ring.*

(1.) *If* R *is regular, then the invariants* $\dim(R)$, $\operatorname{ms}(R)$, $\operatorname{cs}(R)$, *and* $\mu(\mathfrak{m})$ *are equal.*

(2.) *If* R *is a Cohen-Macaulay local ring with infinite residue field, then* $\operatorname{ms}(R) = \dim(R)$ *if and only if* R *has minimal multiplicity.*

(3.) *If* R *is Cohen-Macaulay, local, and* $\dim(R) > 0$, *then* $\operatorname{cs}(R) = \dim(R)$ *if and only if* R *is regular.*

(4.) *We have that* $\operatorname{ms}(R) = \mu(\mathfrak{m})$ *if and only if* $\mathfrak{m}I = \mathfrak{m}^2$ *implies* $I = \mathfrak{m}$ *for any ideal* I *of* R.

(5.) *We have that* $\operatorname{cs}(R) = \mu(\mathfrak{m})$ *if and only if* $I^2 = \mathfrak{m}^2$ *implies* $I = \mathfrak{m}$ *for any ideal* I *of* R.

We proceed subsequently to provide a thorough investigation of the invariants in the case that R is a hypersurface (cf. Corollaries 4.3.6 and 4.3.7) or $\mu(\mathfrak{m}^2)$ is small (cf. Propositions 4.3.12 and 4.3.13). One of the most useful bounds for $\operatorname{ms}(R)$ is established in Proposition 4.3.10, in which we demonstrate that $\operatorname{ms}(R) \leq r$ for any positive integer r such that $\mu(\mathfrak{m}^2) < \binom{r+2}{r}$. We also exhibit bounds on the invariants for **fiber products** of Noetherian local rings (cf. Proposition 4.3.14).

We devote the fourth section of the fourth chapter to the standard graded local case and the **Weak Lefschetz Property** (cf. Definition 4.4.5). Every Noetherian local ring $(R, \mathfrak{m})$ naturally

gives rise to a standard graded local ring $\mathrm{gr}_{\mathfrak{m}}(R)$ called the **associated graded ring** (cf. Proposition 2.1.136). We discuss the difficulties in passing information from the invariants of R to the invariants of $\mathrm{gr}_{\mathfrak{m}}(R)$ (cf. Proposition 4.4.1), and we establish that the associated graded ring of R provides information about $\mathrm{cs}(R)$ in the case that $\mathrm{gr}_{\mathfrak{m}}(R)$ has positive depth (cf. Proposition 4.4.4). If a standard graded local ring R enjoys the Weak Lefschetz Property, then $\mathrm{ms}(R)$ is simply the least number of linearly independent homogeneous elements of R of degree one for which the quadratic term of the Hilbert polynomial of the induced quotient ring vanishes (cf. Proposition 4.4.6). Consequently, we exploit this fact to deduce values of $\mathrm{ms}(R)$ in the case that R enjoys the Weak Lefschetz Property and either (a.) $\mathrm{ms}(R)$ is small or (b.) $\mu(\mathfrak{m})$ is small (cf. Propositions 4.4.7 and 4.4.8). Last, we provide bounds for or explicitly compute the invariants in the case that R is the nth **Veronese** subring of $k[x,y]$ (cf. Proposition 4.4.15 and Corollaries 4.4.18 and 4.4.19).

One of the most fruitful settings in which to consider the invariants of Chapter 4 is the case that R is a standard graded algebra over a field. Let k be the residue field of R, and let $x_1,\ldots,x_n$ be any indeterminates over k. We denote by $S = k[x_1,\ldots,x_n]$ the n-variate polynomial ring over k. We may write $R = S/I$ for some homogeneous ideal I of S. Crucially, we may assume that I is generated by polynomials of degree two (cf. Proposition 4.4.12), from which we obtain the following.

Proposition 1.2.8 (Proposition 4.5.1)**.** *Let R, I, and n be defined as in the above paragraph.*

(1.) *We have that* $\binom{n+1}{2} - \mu(I) \leq \binom{\mathrm{cs}(R)+1}{2}$.

(2.) *If there exists an integer* $0 \leq s \leq n-1$ *such that* $\mu(I) \leq \dfrac{(s+1)(2n-s)}{2}$, *then* $\mathrm{cs}(R) \geq n-s+1$.

(3.) *Even more, if* $\mu(I) \leq n-1$, *then* $\mathrm{cs}(R) = n$.

We work on a case-by-case basis in Section 4.5 to determine $\mathrm{cs}(R)$ and $\mathrm{ms}(R)$ when I admits a minimal generator that is not squarefree and either (a.) n is small or (b.) $\mu(I)$ is large. Conversely, by the **Stanley-Reisner Correspondence**, the quadratic squarefree monomial ideals of the n-variate polynomial ring S are in bijection with the finite simple graphs on n vertices (cf. Section 2.3.2). Consequently, if we assume moreover that the residue field k of R is infinite, then

these algebraic invariants give rise to graphical invariants in the following sense. Let G be a finite simple graph on n vertices. We may define the **edge ideal** $I(G) = (x_i x_j \mid \{i, j\}$ is an edge of $G)$ of the polynomial ring $S = k[x_1, \ldots, x_n]$; the quotient ring $k(G) = S/I(G)$ is the **edge ring** of G. Under these identifications, the invariants $\operatorname{ms}(G) = \operatorname{ms}(k(G))$ and $\operatorname{cs}(G) = \operatorname{cs}(k(G))$ measure the "connectivity" of G: we show that adjoining edges to G never increases $\operatorname{ms}(G)$, and the value of $\operatorname{ms}(G)$ depends only on the number of isolated vertices of G and $\operatorname{ms}(H)$, where H is the induced subgraph of G with no isolated vertices (cf. Proposition 4.6.8 and Corollary 4.6.10). Combining a famous result of Fröberg in [Frö90] on linear resolutions of edge ideals with work of Eisenbud-Huneke-Ulrich in [EHU06], we deduce that $\operatorname{ms}(G) = \alpha(G)$ in the case that $\overline{G}$ is **chordal**, where $\alpha(G)$ is the **independence number** of G and $\overline{G}$ is the **complement graph** of G (cf. Definitions 4.6.12 and 4.6.16 and Proposition 4.6.19). Consequently, the following statements hold.

Theorem 1.2.9 (Propositions 4.6.2, 4.6.7, 4.6.45, and 4.6.24)**.** *Let $n, n_1, \ldots, n_t$ be positive integers.*

(1.) *We have that* $\operatorname{ms}(K_n) = 1$ *and* $\operatorname{cs}(K_n) = \left\lceil \sqrt{2n + \frac{1}{4}} - \frac{1}{2} \right\rceil$ *for the complete graph K_n.*

(2.) *We have that* $\operatorname{ms}(K_{n_1,\ldots,n_t}) = \max\{n_1, \ldots, n_t\}$ *for the complete t-partite graph $K_{n_1,\ldots,n_t}$.*

(3.) *We have that* $\operatorname{ms}(S_n) = n - 1$ *and* $\operatorname{cs}(S_n) = n$ *for the star graph S_n.*

Unfortunately, many graphs do not satisfy the property that their complement $\overline{G}$ is chordal; even more, if the complement graph $\overline{G}$ admits an induced cycle of length four, then the upper bound on $\operatorname{ms}(G)$ provided in Proposition 4.6.19 does not yield any new information, hence we must turn our attention to computing $\operatorname{ms}(G)$ and $\operatorname{cs}(G)$ on a case-by-case basis.

Proposition 1.2.10 (Propositions 4.6.27, 4.6.29, and 4.6.47)**.** *Let n be a positive integer.*

(1.) *We have that* $\left\lceil \frac{n}{2} \right\rceil \leq \operatorname{ms}(P_n) \leq n - 1$ *and* $\operatorname{cs}(P_n) = n$ *for the path graph P_n.*

(2.) *We have that* $\left\lfloor \frac{n}{2} \right\rfloor \leq \operatorname{ms}(C_n) \leq n - 1$ *and* $n - 1 \leq \operatorname{cs}(C_n) \leq n$ *for the cycle graph C_n. If $n \leq 7$, then* $\operatorname{ms}(C_n) \leq \left\lceil \frac{n}{2} \right\rceil$*. If n is odd, then* $\operatorname{cs}(C_n) = n - 1$.

(3.) *We have that* $\left\lfloor \frac{n-1}{2} \right\rfloor \leq \operatorname{ms}(W_n) \leq n - 3$ *and* $n - 2 \leq \operatorname{cs}(W_n) \leq n$ *for the wheel graph W_n. If $n \leq 7$, then* $\operatorname{ms}(W_n) \leq \left\lceil \frac{n-1}{2} \right\rceil$*. If n is even, then* $\operatorname{cs}(W_n) \leq n - 1$.

We conclude Chapter 4 by reducing the study of $\mathrm{ms}(G)$ and $\mathrm{cs}(G)$ to finite simple graphs of **diameter** two and outlining a strategy to tackle the invariants in this case. Crucially, we prove that the edge ring of the **graph join** $G * H$ of finite simple graphs G and H is the fiber product of the respective edge rings of G and H (cf. Proposition 4.6.42 and the discussion preceding the proposition), hence we obtain automatic bounds for the invariants by Proposition 4.3.14. Consequently, for any finite simple graph G, we have that $\mathrm{ms}(G) = \mathrm{ms}(G * K_1)$, and $G * K_1$ has diameter two.

One of our central lingering questions regarding this chapter lies in understanding certain (vertex) **edge covers** of finite simple graphs of diameter two (cf. Question 4.6.38); its resolution would provide a nontrivial upper bound for $\mathrm{ms}(G)$ for any finite simple graph G. We are also curious about a possible connection between $\mathrm{ms}(\mathbb{R}(G))$ and another mysterious graphical invariant that appears in systems biology and bioinformatics called the **maximum likelihood threshold** (cf. the paragraph preceding Proposition 4.7.2, the proposition itself, and the subsequent Question 4.7.3).

Last, in Chapter 5, we turn our attention to the study of a family of two-dimensional monomial subrings that generalize the two-dimensional Veronese subrings of any degree. Given any integers $0 < n_s < \cdots < n_1 < a$, we may define a set $A = \{0, n_s, \ldots, n_1, a\} \subseteq [a] = \{0, 1, \ldots, a\}$; then, an ath **pseudo-Veronese** subring of $k[x,y]$ is any two-dimensional monomial subring of the form

$$k[x,y]^{(A)} = k[x^i y^{a-i} \mid i \in A] = k[x^a, x^{n_1} y^{a-n_1}, \ldots, x^{n_s} y^{a-n_s}, y^a].$$

Observe that if $A = [a]$, then we retrieve the ath Veronese subring $k[x,y]^{(a)}$. We demonstrate that the properties of $k[x,y]^{(A)}$ can be deduced from mild assumptions about the sumsets of A, i.e., the sets of finite sums of a fixed number of elements of A. Explicitly, if r is a positive integer, then the r-fold sumset $rA = \sum_{i=1}^{r} A = \{a_1 + \cdots + a_r \mid a_1, \ldots, a_r \in A\}$ controls certain aspects of the ath pseudo-Veronese subring of $k[x,y]$, e.g., its integral closure and the powers of its maximal ideal.

Proposition 1.2.11 (Propositions 5.3.1, 5.3.4, 5.3.5, and 5.3.6)**.** *Let $0 < n_s < \cdots < n_1 < a$ be integers, and let $A = \{0, n_s, \ldots, n_1, a\}$. Consider the monomial subring $k[x,y]^{(A)} = k[x^i y^{a-i} \mid i \in A]$.*

(1.) *If $n_s = 1$ or $n_1 = a - 1$, then the* **integral closure** *of $k[x,y]^{(A)}$ is $k[x,y]^{(a)}$.*

(2.) *The* **Hilbert function** *of* $k[x,y]^{(A)}$ *is* $|nA|$. *Consequently, if there exists a positive integer* r *such that* $rA = [ra]$, *then the* **multiplicity** *of* $k[x,y]^{(A)}$ *is* a.

(3.) *Let* $r > 0$ *be an integer. We have that* $(x^i y^{a-i} \mid i \in A)^r = (x^i y^{a-i} \mid i \in [a])^r$ *if and only if* $rA = [ra]$.

(4.) *If there exists an integer* $r > 0$ *such that* $rA = [ra]$, *then the* **Hilbert series** *of* $k[x,y]^{(A)}$ *is*

$$\sum_{n=0}^{r-1} |nA| t^n + \frac{at^r(1+r-rt)}{(1-t)^2} + \frac{(a-1)t^r}{1-t}.$$

Consequently, one can deduce that the ath pseudo-Veronese subrings are Cohen-Macaulay if and only if $A = [a]$ (cf. Proposition 5.3.9). Ultimately, we prove the following.

Theorem 1.2.12 (Proposition 5.3.12)**.** *Let* $A = \{0, n_s, \ldots, n_1, a\}$ *for some integers* $0 < n_s < \cdots < n_1 < a$. *Consider the monomial subring* $k[x,y]^{(A)} = k[x^i y^{a-i} \mid i \in A]$. *If there exists an integer* $r > 0$ *such that* $rA = [ra]$, *then the (Castelnuovo-Mumford)* **regularity** *of* $k[x,y]^{(A)}$ *is* r.

Other than the ath pseudo-Veronese subrings that they induce, the r-fold sumsets of A enjoy applications in signal processing and active imaging that make them worth investigating on their own (cf. [KKR18] for a discussion of the two-dimensional case). We say that A constitutes a **restricted additive basis** for the interval $[2a]$ if the two-fold sumset of A has the property that $A + A = [2a]$. Currently, it remains an open problem in additive number theory to establish a lower bound for the minimum cardinality of a restricted additive basis of $[2a]$, i.e., $\mu(a) = \min\{|A| : A \text{ is a restricted additive basis for } [2a]\}$ (cf. Proposition 5.2.6 and Remark 5.2.9). Generalizing the notion of restricted additive basis, we define the **regularity** of A to be the smallest positive integer r such that $rA = [ra]$; if such an integer does not exist, then we say that A has infinite regularity. We prove in Proposition 5.2.2 that A has finite regularity only if $A \supseteq \{0, 1, a-1, a\}$. Conversely, Propositions 5.2.14 and 5.2.15 together imply that this containment is sufficient to guarantee that A has finite regularity, and the regularity of any set A such that $A \supseteq \{0, 1, a-1, a\}$ is at most $a-2$.

Chapter 2

Background

2.1 Basic Properties and Invariants of Commutative Rings

2.1.1 Rings, Ideals, and Modules

Unless otherwise stated, we will assume throughout this thesis that R is a commutative unital ring with additive identity 0_R and multiplicative identity 1_R. Recall that an **ideal** I of R is a subgroup of $(R,+)$ that is closed under multiplication by elements of R, i.e., we have that $ri \in I$ for every element $r \in R$ and $i \in I$. We say that a proper ideal P of R is **prime** if and only if the quotient ring $R/P = \{r+P \mid r \in R\}$ is a **domain**. We say that a proper ideal M of R is **maximal** if and only if R/M is a **field**. By convention and for convenience, we make the following definitions, as well.

Definition 2.1.1. We denote by $\mathrm{Spec}(R)$ the collection of prime ideals of R, i.e.,

$$\mathrm{Spec}(R) = \{P \subseteq R \mid P \text{ is a prime ideal of } R\}.$$

Occasionally, we will write $\mathrm{MaxSpec}(R) = \{M \subseteq R \mid M \text{ is a maximal ideal of R }\}$. We refer to $\mathrm{Spec}(R)$ as the **spectrum** of R; likewise, $\mathrm{MaxSpec}(R)$ is the **maximal spectrum** of R. We define also the **Jacobson radical** $\mathrm{Jac}(R)$ of R as the intersection of all maximal ideals of R.

Example 2.1.2. Let $\mathbb{Z}$ denote the ring of integers. We have that $\mathrm{Spec}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ is prime}\} \cup \{0\}$ because $\mathbb{Z}$ is a Euclidean domain and $\mathrm{MaxSpec}(\mathbb{Z}) = \mathrm{Spec}(\mathbb{Z}) \setminus \{0\}$.

We note that $\mathrm{Spec}(R)$ can be viewed as a topological space with respect to the **Zariski topology**: the closed sets are denoted by $V(I) = \{P \in \mathrm{Spec}(R) \mid P \supseteq I\}$ for some ideal I of R, and the

open sets are denoted by $D(r) = \{P \in \operatorname{Spec}(R) \mid r \notin P\}$ for some element $r \in R$.

By the Fundamental Theorem of Arithmetic, every positive integer can be written as a product of positive powers of distinct primes. Consequently, given any integer n, there exist distinct primes $p_1, \ldots, p_k$ and positive integers $e_1, \ldots, e_k$ such that $n = \pm p_1^{e_1} \cdots p_k^{e_k}$. Every ideal of $\mathbb{Z}$ is principal, and we have that $a\mathbb{Z} \subseteq b\mathbb{Z}$ if and only if $b \mid a$, hence the ideal $n\mathbb{Z}$ induces a chain of ideals beginning with itself and ending with $p_i\mathbb{Z}$ for some prime p_i appearing in the prime factorization of n.

Generally, we use the following definition to describe this property of a ring.

Definition 2.1.3. We say that R is **Noetherian** if any of the following equivalent conditions hold.

(i.) Every ascending chain of ideals of R stabilizes. Explicitly, for every sequence of inclusions of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there exists an integer $n \gg 0$ such that $I_k = I_n$ for all integers $k \geq n$.

(ii.) Every nonempty collection of ideals has a maximal element with respect to inclusion.

(iii.) Every ideal I of R is finitely generated. Explicitly, there exist elements $x_1, \ldots, x_n \in I$ such that for every element $x \in I$, we have that $x = r_1x_1 + \cdots + r_nx_n$ for some elements $r_1, \ldots, r_n \in R$.

Theorem 2.1.4 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then $R[x]$ is Noetherian.*

Example 2.1.5. Let k be a field. Observe that the only ideals of k are $\{0_k\}$ and k: indeed, the ideals of k (or any commutative unital ring) are in one-to-one correspondence with the kernels of the unital ring homomorphisms $k \to S$ as S ranges over all commutative unital rings. Every nonzero element of k is a unit, so any unital ring homomorphism $\varphi : k \to S$ must be injective or identically zero, i.e., $\ker \varphi = \{0_k\}$ or $\ker \varphi = k$. Both of these are finitely generated ideals, as k is generated as an ideal by 1_k (as with any ring). Consequently, any field k is Noetherian by Definition 2.1.3. By Hilbert's Basis Theorem, any polynomial ring or finitely generated algebra over k is Noetherian.

Even more, Example 2.1.5 shows that the only maximal ideal of a field is the zero ideal.

Definition 2.1.6. We say that R is **local** if R admits a unique maximal ideal $\mathfrak{m}$. For emphasis, we write $(R, \mathfrak{m}, k)$ to denote the local ring R with unique maximal ideal $\mathfrak{m}$ and **residue field** $k = R/\mathfrak{m}$.

Proposition 2.1.7. *Let R be a commutative unital ring. The following conditions are equivalent.*

(i.) *R admits a unique maximal ideal, i.e., R is local.*

(ii.) *For every element $r \in R$, either r or $1_R + r$ is a unit.*

Particularly, the unique maximal ideal of a local ring R consists of all non-unit elements of R.

Example 2.1.8. Given a field k and indeterminate x, consider the quotient ring $S = k[x]/(x^2)$. We denote by $\bar{x}$ the class of x modulo (x^2). By the Correspondence Theorem, the ideals of S are in bijection with the ideals of $k[x]$ that contain (x^2) via the map that sends an ideal I of $k[x]$ to the ideal $I/(x^2)$ of S. Considering that $k[x]$ is a principal ideal domain, the ideals of S are (0_S), $(\bar{x})$, and S, corresponding to the ideals (x^2), (x), and $k[x]$, respectively. Of these, $(\bar{x})$ is maximal by the Third Isomorphism Theorem. Consequently, $(S, \mathfrak{m})$ is a local ring with maximal ideal $\mathfrak{m} = (\bar{x})$.

Using a process analogous to the construction of the rational numbers $\mathbb{Q}$ from the integers $\mathbb{Z}$, one can always obtain a local ring from a given ring. Recall that a set $S \subseteq R$ is **multiplicatively closed** if S contains 1_R and for any elements $s, t \in S$, we have that $st \in S$. Given any multiplicatively closed set $S \subseteq R$, one can construct an equivalence relation on $R \times S$ by declaring that $(r,s) \sim (r',s')$ if and only if there exists an element $t \in S$ such that $t(rs' - r's) = 0_R$. One need only check that if $(r,s) \sim (r',s')$ and $(r',s') \sim (r'',s'')$, then $(r,s) \sim (r'',s'')$. But in this case, there exist elements $t, t' \in S$ such that $t(rs' - r's) = 0_R$ and $t'(r's'' - r''s') = 0_R$, hence the product $s'tt'$ belongs to S and satisfies $s'tt'(rs'' - r''s) = 0_R$. Like with rational numbers, we denote by r/s the equivalence class of (r,s) modulo $\sim$. Consider the set of equivalence classes of $(R \times S)/\sim$, denoted by

$$S^{-1}R = \left\{ \frac{r}{s} : r \in R,\, s \in S, \text{ and } \frac{r}{s} = \frac{r'}{s'} \iff \text{there exists } t \in S \text{ such that } t(rs' - r's) = 0_R \right\}.$$

We refer to $S^{-1}R$ as the **localization** of R with respect to S. Observe that by definition, if $0_R \in S$, then $S^{-1}R = \{0_R\}$. Consequently, we will always assume that $0_R \notin S$.

Proposition 2.1.9. *Let R be a commutative unital ring with a multiplicatively closed subset S.*

(1.) *$S^{-1}R$ is a commutative unital ring with respect to* $\dfrac{r}{s}+\dfrac{r'}{s'}=\dfrac{rs'+r's}{ss'}$ *and* $\dfrac{r}{s}\cdot\dfrac{r'}{s'}=\dfrac{rr'}{ss'}$.

(2.) *There is a canonical ring homomorphism* $\lambda : R \to S^{-1}R$ *defined by* $\lambda(r)=\dfrac{r}{1_R}$.

(3.) *For any ideal I of R, we have that* $IS^{-1}R=\lambda(I)=\left\{\dfrac{i}{s} : i\in I \text{ and } s\in S\right\}$.

(4.) *For any ideal I of $S^{-1}R$, we have that* $\lambda^{-1}(I)S^{-1}R=\lambda(\lambda^{-1}(I))=I$.

(5.) *The canonical ring homomorphism* $\lambda : R \to S^{-1}R$ *induces a one-to-one correspondence between* $\operatorname{Spec}(S^{-1}R)$ *and the prime ideals of R such that* $P\cap S=\emptyset$ *as follows.*

$$\{P\in \operatorname{Spec}(R) \mid P\cap S=\emptyset\} \leftrightarrow \operatorname{Spec}(S^{-1}R)$$
$$P \mapsto \lambda(P)=PS^{-1}R$$

(6.) *(Existence of Local Maximal Ideals) If I is an ideal of R such that* $I\cap S=\emptyset$, *then there exists a prime ideal P of R such that* $P\cap S=\emptyset$ *and $S^{-1}P$ is a maximal ideal of $S^{-1}R$. Particularly, the prime ideal P is the largest (with respect to inclusion) ideal of R that is disjoint from S.*

(7.) *If P is a prime ideal of R, then* $W=R\setminus P$ *is a multiplicatively closed set. Further, the localization* $R_P=W^{-1}R$ *is a local ring with unique maximal ideal* PR_P.

Proof. We omit the proofs of properties (1.), (2.), (3.), and (4.), as they are routine to check.

(5.) We establish first that the map is well-defined, i.e., we show that if P is a prime ideal of R such that $P\cap S=\emptyset$, then the ideal $\lambda(P)=PS^{-1}R$ of $S^{-1}R$ is prime. Given any elements $a/s, b/t\in S^{-1}R$ such that $(a/s)(b/t)\in\lambda(P)$, we claim that either $a/s\in\lambda(P)$ or $b/t\in\lambda(P)$. By definition, we have that $(a/s)(b/t)=ab/st$ belongs to $\lambda(P)$ if and only if there exist some elements $c\in P$ and $u,v\in S$ such that $v(abu-stc)=0_R$ or $vabu=vstc$. By hypothesis that c belongs to P, we conclude that $vabu$ belongs to P. Considering that P is a prime ideal of R, one of the elements a,b,u, or v must belong to P. By construction, neither u nor v belongs to P, so either a or b belong to P. Consequently, either a/s or b/t belong to $\lambda(P)$, and we conclude that $\lambda(P)$ is prime.

Our previous paragraph establishes that the map is well-defined. We proceed to show that it has a well-defined inverse. Consider the map $P \mapsto \lambda^{-1}(P)$. If $PS^{-1}R$ is a prime ideal of $S^{-1}R$, then its contraction $\lambda^{-1}(P)$ is a prime ideal of R. Further, every element of S is mapped onto a unit by λ, hence if $\lambda^{-1}(P) \cap S$ were nonempty, then $P = \lambda(\lambda^{-1}(P))$ would be the entire ring $S^{-1}R$ — a contradiction. We conclude that the map $P \mapsto \lambda^{-1}(P)$ is well-defined. By property (2.) above, we have that $\lambda(\lambda^{-1}(P)) = P$ for all prime ideals P of $S^{-1}R$, hence the map $P \mapsto \lambda^{-1}(P)$ has a left-inverse. On the other hand, we claim that $\lambda^{-1}(\lambda(P)) = P$ so that the map $P \mapsto \lambda^{-1}(P)$ has a right-inverse. Clearly, it is always the case that $P \subseteq \lambda^{-1}(\lambda(P))$. Conversely, let x be an element of $\lambda^{-1}(\lambda(P))$. By definition, we have that $\lambda(x)$ belongs to $\lambda(P)$, hence there exist elements $s,t \in S$ and $p \in P$ such that $t(xs - p) = 0_R$. But this implies that txs belongs to the prime ideal P so that x belongs to P by assumption that $s,t \in S$ and $P \cap S = \emptyset$. We conclude that $\lambda^{-1}(\lambda(P)) = P$.

(6.) Observe that the collection $\mathscr{D} = \{I \subseteq R \mid I \text{ is an ideal of } R \text{ and } I \cap S = \emptyset\}$ is partially ordered by inclusion. Further, it is nonempty because it contains the zero ideal of R. Given any chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of ideals in $\mathscr{D}$, the union $\cup_{n=1}^{\infty} I_n$ is an ideal of R that is disjoint from S. Consequently, every chain in $\mathscr{D}$ has an upper bound in $\mathscr{D}$, hence $\mathscr{D}$ has a maximal element P by Zorn's Lemma. We claim that P is a prime ideal of R. Consider some elements $a,b \in R$ such that $ab \in P$. On the contrary, if neither $a \in P$ nor $b \in P$, then we would have that $P \subsetneq aR + P$ and $P \subsetneq bR + P$. By the maximality of P, there would exist elements $s \in (aR+P) \cap S$ and $t \in (bR+P) \cap S$. Observe that $(aR+P)(bR+P) \subseteq P$ so that $st \in (aR+P)(bR+P)$ belongs to P — a contradiction.

(7.) By definition, a prime ideal P of R is a proper ideal such that $ab \in P$ implies that $a \in P$ or $b \in P$. Equivalently, if neither $a \in P$ nor $b \in P$, then $ab \in R \setminus P$, i.e., $W = R \setminus P$ is multiplicatively closed. By properties (1.) and (5.), $\operatorname{Spec}(R_P)$ is in bijection with $\{Q \in \operatorname{Spec}(R) \mid Q \cap W = \emptyset\} = \{Q \in \operatorname{Spec}(R) \mid Q \subseteq P\}$. We conclude that PR_P is the unique maximal ideal of the local ring R_P. □

Proposition 2.1.10. *Every localization of a direct product of commutative unital rings $R_1 \times \cdots \times R_n$ at a prime ideal is isomorphic to the localization of some R_i at a prime ideal of R_i.*

Proof. Observe that the prime ideals of $R_1 \times \cdots \times R_n$ are of the form $P_1 \times \cdots \times P_n$, where P_i is a prime ideal of R_i for some integer $1 \leq i \leq n$ and $P_j = R_j$ for all integers $j \neq i$. We may assume

for simplicity that P_1 is a prime ideal of R_1, hence it suffices to prove the claim for the prime ideal $P = P_1 \times R_2 \times \cdots \times R_n$ of $R = R_1 \times \cdots \times R_n$. Observe that $R \setminus P = (R_1 \setminus P_1) \times R_2 \times \cdots \times R_n$, hence for any elements $(r_1, r_2, \ldots, r_n) \in R$ and $(s_1, s_2, \ldots, s_n) \in R \setminus P$, we have that

$$(1_{R_1}, 1_{R_2}, \ldots, 1_{R_n})[(r_1, r_2, \ldots, r_n)(s_1, 0_{R_2}, \ldots, 0_{R_n}) - (r_1, 0_{R_2}, \ldots, 0_{R_n})(s_1, s_2, \ldots, s_n)] = 0_R.$$

By definition, every element of R_P is of the form $\dfrac{(r_1, 0_{R_2}, \ldots, 0_{R_n})}{(s_1, 0_{R_2}, \ldots, 0_{R_n})}$ for some elements $r_1 \in R_1$ and $s_1 \in R_1 \setminus P_1$, hence we obtain a bijection $\varphi : R_P \to (R_1)_{P_1}$ that sends $\dfrac{(r_1, 0_{R_2}, \ldots, 0_{R_n})}{(s_1, 0_{R_2}, \ldots, 0_{R_n})} \mapsto \dfrac{r_1}{s_1}$. One can readily verify that φ is a well-defined ring homomorphism so that $R_P \cong (R_1)_{P_1}$, as desired. □

Generally, the set S of non-zero divisors of a commutative unital ring is multiplicatively closed; the resulting ring $Q(R) = S^{-1}R$ is the **total ring of fractions** of R. We demonstrate that the prime ideals of $Q(R)$ are in bijection with the prime ideals of R that consist of zero divisors.

Corollary 2.1.11. *Let R be a commutative unital ring with total ring of fractions $Q(R)$. The prime ideals of $Q(R)$ are in bijection with the prime ideals of R consisting of zero divisors.*

Proof. By Proposition 2.1.9, the canonical ring homomorphism $\lambda : R \to Q(R)$ induces a bijection between the prime ideals of $Q(R)$ and the prime ideals of R such that $P \cap S = \emptyset$, where S is the multiplicatively closed subset of R consisting of non-zero divisors of R and $Q(R) = S^{-1}R$. □

We will soon discuss further properties of $Q(R)$ in our section on Krull Dimension and Height. If D is an integral domain, then the structure of $Q(D)$ is especially simple. By definition, the zero ideal of D is prime. Consequently, we may construct the local ring $Q(D) = W^{-1}R$ for the multiplicatively closed set $W = D \setminus \{0_D\}$ consisting of non-zero divisors of D. We refer to $Q(D)$ as the **field of fractions** of D, and we write $\mathrm{Frac}(D)$: indeed, every nonzero element d/w of $\mathrm{Frac}(D)$ has multiplicative inverse w/d. Particularly, we have that $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. Our next proposition shows that this property holds even for integral domains obtained as quotient rings by prime ideals.

Proposition 2.1.12. *Let R be a nonzero commutative unital ring. For any prime ideal P of R, we have that* $\mathrm{Frac}(R/P) \cong R_P/PR_P$.

Proof. By definition, $\mathrm{Frac}(R/P)$ consists of ordered pairs $(r+P, s+P)$ such that $r \in R$ and $s \in R \setminus P$. Even more, we have that $(r+P, s+P) = (r'+P, s'+P)$ if and only if there exists an element $t \in R \setminus P$ such that $(t+P)[(r+P)(s'+P) - (r'+P)(s+P)] = 0_R + P$ if and only if there exists an element $t \in R \setminus P$ such that $t(rs' - r's) + P = 0_R + P$. Consequently, we may view $\mathrm{Frac}(R/P)$ as the ring of cosets $(r,s) + P$ of $R \times (R \setminus P)$ modulo P with the additional condition that $(r,s) + P = (r',s') + P$ if and only if there exists an element $t \in R \setminus P$ such that $t(rs' - r's) + P = 0_R + P$. Put another way, there exists a ring homomorphism $\pi : R_P \to \mathrm{Frac}(R/P)$ defined by $\pi\left(\frac{r}{s}\right) = \frac{r}{s} + P$. Observe that PR_P is a maximal ideal of R_P that is contained in $\ker \pi$. Considering that π is not identically zero, we conclude that $\ker \pi = PR_P$, hence the claim follows by the First Isomorphism Theorem. □

Other than the ideals of a commutative unital ring, the following definition introduces algebraic structures associated to R by which one may understand the properties of R.

Definition 2.1.13. We say that an abelian group $(M, +)$ is a (unital) R-**module** if there is a map $\cdot : R \times M \to M$ sending $(r,m) \mapsto r \cdot m$ such that for all elements $r, s \in R$ and $m, n \in M$, we have that

(i.) $r \cdot (m+n) = r \cdot m + r \cdot n$,

(ii.) $(r+s) \cdot m = r \cdot m + s \cdot m$,

(iii.) $r \cdot (s \cdot m) = (rs) \cdot m$, and

(iv.) $1_R \cdot m = m$.

Clearly, R is an R-module via its own multiplication. We will reserve the notation 0 for the zero element of M. Often, it will be convenient to write $r \cdot m$ as rm with the understanding that r is an element of R that is acting on the element m of the R-module M via the specified action.

Like with any algebraic structure, the substructures of a module are of central importance to its study. If M is an R-module, then $N \subseteq M$ is an R-**submodule** if N is closed under addition and R-scalar multiplication and $0 \in N$. By definition, the R-submodules of R are precisely its ideals.

If M and N are any R-modules, then an R-**module homomorphism** $\varphi : M \to N$ is a function such that $\varphi(m+m') = \varphi(m) + \varphi(m')$ and $\varphi(rm) = r\varphi(m)$ for all elements $m, m' \in M$ and $r \in R$. Equivalently, one could say that an R-module homomorphism is an R-linear transformation.

We say that M is **faithful** if $rm = 0$ implies that $r = 0_R$ for every nonzero element $m \in M$. Put another way, if the **annihilator** $\operatorname{ann}_R(M) = \{r \in R \mid rm = 0 \text{ for all elements } m \in M\}$ of M is zero, then M is a faithful R-module. One can immediately verify that $\operatorname{ann}_R(M)$ is an ideal of R.

Crucially, if M is an R-module and I is an ideal of M such that $IM = 0$, then M can be viewed as an R/I-module via the action $(r+I) \cdot m = rm$. Explicitly, if $r+I = s+I$, then $r-s$ belongs to I so that $rm - sm = (r-s)m = 0$. But this implies that $(r+I) \cdot m = rm = sm = (s+I) \cdot m$, and the action is well-defined. Particularly, if $\mathfrak{m}$ is a maximal ideal of R, then $R/\mathfrak{m}$ is a field. Further, if $\mathfrak{m}M = 0$, then M is an $R/\mathfrak{m}$-vector space, and it admits a basis. We will return to this idea soon.

We say that an R-module M is **finitely generated** if there exist elements $x_1, \ldots, x_n \in M$ such that for every element $x \in M$, there exist elements $r_1, \ldots, r_n \in R$ such that $x = r_1x_1 + \cdots + r_nx_n$. Put another way, the elements $x_1, \ldots, x_n \in M$ generate M as an R-module if $M = R\langle x_1, \ldots, x_n \rangle$. We state a fundamental result relating the finitely generated R-modules and prime ideals of R.

Lemma 2.1.14 (Prime Avoidance Lemma)**.** *[BH93, Lemma 1.2.2] Let R be a commutative unital ring with prime ideals $P_1, \ldots, P_n$. Let M be an R-module with $x_1, \ldots, x_n \in M$. Let $N = R\langle x_1, \ldots, x_n \rangle$. If $N_{P_i} \not\subseteq P_iM_{P_i}$ for any integer $1 \leq i \leq n$, then there exists an element $x \in N$ such that $x \notin P_iM_{P_i}$ for any integer $1 \leq i \leq n$. Particularly, if I is a finitely generated ideal of R such that $I \not\subseteq P_i$ for any integer $1 \leq i \leq n$, then there exists an element $r \in I$ such that $r \notin P_i$ for any integer $1 \leq i \leq n$.*

One of the most valuable results on finitely generated modules is the **Cayley-Hamilton Theorem**; the reader might be familiar with its use in linear algebra, but we state it in generality.

Theorem 2.1.15 (Cayley-Hamilton Theorem)**.** *Let R be a commutative unital ring. Let M be a finitely generated R-module. For any ideal I and any R-module homomorphism $\varphi : M \to M$ such that $\varphi(M) \subseteq IM$, there exists a monic polynomial $t^n + i_1t^{n-1} + \cdots + i_{n-1}t + i_n$ with $i_1, \ldots, i_n \in I$ such that $\varphi^n + i_1\varphi^{n-1} + \cdots + i_{n-1}\varphi + i_n \mathrm{id}_M$ is the zero homomorphism on M.*

Proof. Let $x_1, \ldots, x_n$ be a system of R-module generators of M. By hypothesis that $\varphi(M) \subseteq IM$, we may view M as an $R[t]$-module via the action $t \cdot x = \varphi(x)$. Considering that $M = R\langle x_1, \ldots, x_n \rangle$ and $\varphi(M) \subseteq IM$ by assumption, for each integer $1 \leq j \leq n$, there exist elements $i_{j,1}, \ldots, i_{j,n} \in I$ such that $t \cdot x_j = \varphi(x_j) = \sum_{k=1}^{n} i_{j,k} x_k$ or $\sum_{k=1}^{n} (\delta_{j,k} t - i_{j,k}) x_k = 0_R$, where $\delta_{j,k}$ is the Kronecker delta. Consider the matrix A whose jth row and kth column is $\delta_{j,k} s - i_{j,k}$. Observe that the previous identity shows that $A\mathbf{x} = \mathbf{0}$ for the column vector $\mathbf{x} = \langle x_1, \ldots, x_n \rangle^t$. Using the fact that $\operatorname{adj}(A)A$ is $\det(A)$ times the $n \times n$ identity matrix, we conclude that $\det(A)\mathbf{x} = \mathbf{0}$. Consequently, $\det(A)$ is a monic polynomial in t with coefficients in I that acts as the zero homomorphism on M. □

Every finitely generated module over a local ring $(R, \mathfrak{m})$ admits a unique number of minimal generators by **Nakayama's Lemma**. Considering its importance and ubiquity, we record it below.

Lemma 2.1.16 (Nakayama's Lemma)**.** *Let $(R, \mathfrak{m}, k)$ be a local ring with unique maximal ideal $\mathfrak{m}$ and residue field k. Let M be a finitely generated R-module. If the images of $x_1, \ldots, x_n$ modulo $\mathfrak{m}M$ form a basis of the k-vector space $M/\mathfrak{m}M$, then $M = R\langle x_1, \ldots, x_n \rangle$.*

One common variation of Nakayama's Lemma is presented in the following corollary. We omit the proof of the necessity of Nakayama's Lemma, but we do establish its sufficiency.

Corollary 2.1.17. *Let $(R, \mathfrak{m}, k)$ be a local ring. Let M be a finitely generated R-module. If I is a proper ideal of R and N is an R-submodule of M such that $M = IM + N$, then $M = N$.*

Proof. Let $x_1, \ldots, x_n$ denote a system of generators of M such that $x_1 + \mathfrak{m}M, \ldots, x_n + \mathfrak{m}M$ forms a basis for the k-vector space $M/\mathfrak{m}M$. By hypothesis that $M = IM + N$, for each integer $1 \leq i \leq n$, there exist elements $r_{i,1}, \ldots, r_{i,n} \in I$ and $y_i \in N$ such that $x_i = y_i + \sum_{j=1}^{n} r_{i,j} x_j$. Consequently, we have that $x_i + \mathfrak{m}M = y_i + \mathfrak{m}M$ so that $y_1 + \mathfrak{m}M, \ldots, y_n + \mathfrak{m}M$ forms a basis of $M/\mathfrak{m}M$. We conclude by Nakayama's Lemma that $M = R\langle y_1, \ldots, y_n \rangle$ so that $M = N$, as desired. □

We denote by $\mu(M) = \dim_k(M/\mathfrak{m}M)$ the unique number of minimal generators of M, as guaranteed by Nakayama's Lemma. Our next definition generalizes Definition 2.1.3.

Definition 2.1.18. We say that M is **Noetherian** if any of the following equivalent conditions hold.

(i.) Every ascending chain of R-submodules of M stabilizes.

(ii.) Every nonempty collection of R-submodules of M has a maximal element under inclusion.

(iii.) Every R-submodule of M is finitely generated.

If R is Noetherian, then the following condition is equivalent to the above conditions.

(iv.) The R-module M is finitely generated.

We describe two paramount results on Noetherian modules over Noetherian rings.

Lemma 2.1.19 (Artin-Rees Lemma)**.** *Let R be Noetherian. For any ideal I and finitely generated R-modules $N \subseteq M$, there exists an integer $k \geq 1$ such that $I^n M \cap N = I^{n-k}(I^k M \cap N)$ for all $n \geq k$.*

Theorem 2.1.20 (Krull's Intersection Theorem)**.** *Let R be a Noetherian ring. For any proper ideal I of R and any finitely generated R-module M, we have that $\bigcap_{n\geq 0} I^n M = I\big(\bigcap_{n\geq 0} I^n M\big)$. Even more, there exists an element $x \in I$ such that $(1_R - x)\bigcap_{n\geq 0} I^n M = 0$. If R is local, then $\bigcap_{n\geq 0} I^n M = 0$.*

Proof. Observe that $N = \bigcap_{n\geq 0} I^n M$ is a finitely generated R-submodule of M and $N = I^n M \cap N$ for all integers $n \geq 0$. By the Artin-Rees Lemma, there exists an integer $k \geq 1$ such that

$$N = I^n M \cap N = I^{n-k}(I^k M \cap N) = I^{n-k} N$$

for all integers $n \geq k$. We conclude that $N = IN$, i.e., we have that $\mathrm{id}_N(N) \subseteq IN$. By the Cayley-Hamilton Theorem, there exists a monic polynomial $t^n + i_1 t^{n-1} + \cdots + i_{n-1} t + i_n$ with $i_1, \ldots, i_n \in I$ such that $(1_R + i_1 + \cdots + i_{n-1} + i_n)\,\mathrm{id}_N$ is the zero endomorphism on N. Consequently, we find that $(1_R + i_1 + \cdots + i_{n-1} + i_n)N = 0$ so that $(1_R - x)N = 0$ with $x = -(i_1 + \cdots + i_{n-1} + i_n) \in I$.

Last, if R is local, then we conclude that $\bigcap_{n\geq 0} I^n M = N = 0$ by Corollary 2.1.17. □

We refer to a chain of R-modules $0 \subsetneq M_1 \subsetneq \cdots \subseteq M_{n-1} \subsetneq M$ as a **composition series** of M if there does not exist an R-submodule N of M such that $M_i \subsetneq N \subsetneq M_{i+1}$ for any integer $0 \leq i \leq n-1$.

Put another way, a composition series of M is a maximal ascending chain of R-submodules of M beginning with 0 and ending with M. One of the most important invariants of M is its **length**

$$\ell_R(M) = \inf\{n \geq 0 \mid M \text{ admits a composition series } 0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M\}.$$

If R is a field and M is an R-module, then M is an R-vector space, and its length coincides with its R-vector space dimension. Consequently, length is a generalization of vector space dimension to modules over commutative unital rings other than fields. Considering that finite-dimensional vector spaces exhibit pleasant properties, we are motivated to investigate length of general modules.

Definition 2.1.21. We say that M is **Artinian** if any of the following equivalent conditions hold.

(i.) Every descending chain of R-submodules of M stabilizes.

(ii.) Every nonempty collection of R-submodules of M has a minimal element under inclusion.

If R is Artinian, then the following condition is equivalent to the above conditions.

(iv.) The R-module M is finitely generated.

Proposition 2.1.22. *Let R be a commutative unital ring. The following are equivalent.*

(i.) *An R-module M is Noetherian and Artinian.*

(ii.) *An R-module M has finite length over R.*

Proof. Clearly, the claim holds if $M = 0$. We will assume henceforth that M is a nonzero R-module. (i.) If M is both Noetherian and Artinian, then we may construct a composition series of M as follows. By assumption that M is nonzero, there exists an R-submodule of M that strictly contains 0. By Definition 2.1.21, we may find a nonzero R-submodule M_1 of M that is minimal with respect to inclusion among all R-submodules of M that strictly contain 0. If $M_1 = M$, then we are done; otherwise, we may find a nonzero R-submodule M_2 of M that is minimal with respect to inclusion among all R-submodules of M that strictly contain M_1. Continuing in this manner yields a strictly

ascending chain of R-submodules $0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$. By hypothesis that M is Noetherian, this must be finite, hence we obtain a chain of R-submodules $0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M$ of M; it is by construction a composition series of M, hence we conclude that $\ell_R(M) \leq n$.

(ii.) Conversely, suppose that M has finite length n over R. We claim that every descending chain of R-submodules of M stabilizes. On the contrary, suppose that there exists an infinite descending chain $M_1 \supsetneq M_2 \supsetneq \cdots$ of R-submodules of M. Observe that the first $n+2$ terms of this chain yield a chain $M_{n+2} \subsetneq M_{n+1} \subsetneq \cdots \subsetneq M_2 \subsetneq M_1$. By hypothesis, M_{n+2} is nonzero, hence we may append M and the zero module to obtain a chain $0 \subsetneq M_{n+2} \subsetneq M_{n+1} \subsetneq \cdots \subsetneq M_2 \subsetneq M_1 \subseteq M$ of length at least $n+1$. Because we can refine this chain to a composition series of M of length larger than $\ell_R(M) = n$, we have reached a contradiction. Likewise, there cannot exist an infinite ascending chain of R-submodules of M. We conclude that M is Noetherian and Artinian. □

Corollary 2.1.23. *If M has finite length as an R-module, then M is finitely generated over R.*

Length is an especially important invariant over local rings. Our next proposition gives a useful equivalent condition for a module over a local ring to have finite length.

Proposition 2.1.24. *Let $(R, \mathfrak{m}, k)$ be a local ring. The following are equivalent.*

(i.) *A R-module M is Noetherian and admits an integer $n \geq 0$ such that $\mathfrak{m}^n M = 0$.*

(ii.) *An R-module M has finite length over R.*

Proof. (i.) By definition of length, it suffices to exhibit a finite composition series of M. By assumption that $\mathfrak{m}^n M = 0$ for some integer $n \geq 0$, there exists a chain of R-submodules

$$0 = \mathfrak{m}^n M \subsetneq \mathfrak{m}^{n-1} M \subsetneq \cdots \subsetneq \mathfrak{m} M \subsetneq M.$$

(We may assume without loss of generality that $\mathfrak{m}^{n-1} M$ is nonzero.) Observe that for each integer $0 \leq i \leq n-1$, we have that $M_i = \mathfrak{m}^i M / \mathfrak{m}^{i+1} M$ is a quotient of the Noetherian R-module $\mathfrak{m}^i M$, hence it is finitely generated. Each module M_i satisfies $\mathfrak{m} M_i = 0$, hence we may view each M_i as a k-vector

space. By our exposition preceding Definition 2.1.21, the length of each finite-dimensional k-vector space M_i is finite, hence each M_i admits a finite composition series. By the Correspondence Theorem, a finite composition series of M_i induces a strict chain of R-submodules of M beginning with $\mathfrak{m}^{i+1}M$ and ending with $\mathfrak{m}^i M$ such that each successive containment is minimal. Combining each chain successively from $i = n-1$ to $i = 0$ yields a composition series for M.

(ii.) By Proposition 2.1.22, if M has finite length over R, then M is a Noetherian R-module. On the contrary, assume that $\mathfrak{m}^n M$ is nonzero for each integer $n \geq 0$. By definition, for each integer $n \geq 0$, there exist elements $r_1, \ldots, r_n \in \mathfrak{m}$ and $m \in M$ such that $r_1 \cdots r_n m$ is nonzero. Consider the sequence of R-modules $0 \subseteq R(r_1 \cdots r_n m) \subseteq \cdots \subseteq R(r_1 m) \subseteq Rm \subseteq M$. We claim that each containment is strict; otherwise, there would exist an integer $0 \leq k \leq n-1$ and an element $s \in R$ such that $r_1 \cdots r_k m = s r_1 \cdots r_{k+1} m$. By rearranging, we would obtain $(1_R - s r_{k+1}) r_1 \cdots r_k m = 0$. By Proposition 2.1.7, we would find that $1_R - s r_{k+1}$ is a unit so that $r_1 \cdots r_k m = 0$ — a contradiction. Consequently, for each integer $n \geq 0$, we have constructed a composition series of M of length $n+1$. But this is impossible by assumption that M has finite length over R. □

Corollary 2.1.25. *Let $(R, \mathfrak{m}, k)$ be a local ring. If R is Artinian as an R-module, then R has finite length as an R-module. Particularly, every Artinian local ring is Noetherian.*

Proof. By hypothesis that R is Artinian, the descending chain of ideals $\mathfrak{m} \supsetneq \mathfrak{m}^2 \supsetneq \cdots$ stabilizes, hence we must have that $\mathfrak{m}^n = 0$ for some integer $n \geq 0$. By the proof of Proposition 2.1.24, there exist k-vector spaces $V_i = \mathfrak{m}^i/\mathfrak{m}^{i+1}$ for each integer $0 \leq i \leq n-1$. Every descending chain of k-vector subspaces of V_i corresponds to a descending chain of ideals of R. By hypothesis that R is Artinian, the k-vector spaces V_i must be finitely generated so that R admits a composition series of finite length as in the proof of Proposition 2.1.24. Last, R is Noetherian by Proposition 2.1.22. □

By the proof of Proposition 2.1.24, we obtain the following important and useful fact.

Proposition 2.1.26. *Let R be a commutative unital ring. Let M be an R-module such that $IM = 0$ for some ideal I of R. We have that $\ell_R(M)$ is finite if and only if $\ell_{R/I}(M)$ is finite.*

Proof. If $IM = 0$, then M is an R/I-module via the action $(r+I)\cdot M = rm$. Consequently, a composition series holds for M as an R-module if and only if it holds for M as an R/I-module. □

We define the **colength** of an R-submodule N of an R-module M to be the length of the quotient module M/N, i.e., the colength of N in M is $\ell_R(M/N)$. If I is an ideal of R with finite colength, then R/I is Artinian and Noetherian by Proposition 2.1.22. Conversely, if R is Noetherian and R/I is Artinian, then R/I is Noetherian and Artinian, hence I has finite colength.

We say that an ideal I of R is P-**primary** for a prime ideal P of R if $P = \sqrt{I}$. Observe that if $P^n \subseteq I \subseteq P$ for some integer $n \gg 0$, then $P = \sqrt{I}$ so that I is P-primary. We establish next a necessary and sufficient condition for ideals of finite colength in a Noetherian local ring.

Proposition 2.1.27. *Let $(R,\mathfrak{m})$ be a local ring. Let I be an ideal of R. If I has finite colength, then I is $\mathfrak{m}$-primary. Conversely, if R is Noetherian and I is $\mathfrak{m}$-primary, then I has finite colength.*

Proof. By definition, if I has finite colength, then R/I has finite length as an R-module. By Proposition 2.1.24, we have that $\mathfrak{m}^n(R/I) = 0$ for some integer $n \gg 0$ so that $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ and I is $\mathfrak{m}$-primary. Conversely, if I is $\mathfrak{m}$-primary, then $\mathfrak{m} = \sqrt{I}$. By hypothesis that R is Noetherian, this is equivalent to the condition that $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ for some integer $n \gg 0$, from which it follows that $\mathfrak{m}^n(R/I) = 0$. Even more, we have that $\dim(R/I) = 0$ so that R/I is Artinian by Proposition 6.1.2, from which it follows that R/I has finite length as an R-module, i.e., I has finite colength. □

2.1.2 Krull Dimension and Height

One of the most important invariants of a commutative unital ring is its dimension.

Definition 2.1.28. We define the **(Krull) dimension** of R to be the extended natural number

$$\dim(R) = \sup\{n \mid P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n \text{ and } P_0, P_1, \ldots, P_n \in \operatorname{Spec}(R)\},$$

i.e., $\dim(R)$ is the supremum of the lengths of strictly descending chains of prime ideals of R.

Example 2.1.29. Let k be a field. We have already seen in Example 2.1.5 that k is a Noetherian ring with $\mathrm{Spec}(k) = \{0_k\} = \mathrm{MaxSpec}(k)$. (By an abuse of notation, we use 0_k to denote both the zero element and the zero ideal of k.) Consequently, we have that $\dim(k) = 0$: indeed, 0_k is the only prime ideal of k, hence the only strictly descending chain of prime ideals of k is 0_k.

Example 2.1.30. By Example 2.1.2, we have that $\mathrm{Spec}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ is a prime}\} \cup \{0\}$. Consequently, every strictly descending chain of prime ideals of $\mathbb{Z}$ is of the form $p\mathbb{Z} \supsetneq \{0\}$ for some prime p. (We assume implicitly that a prime p is nonzero.) We conclude that $\dim(\mathbb{Z}) = 1$.

On the other hand, we note that $\mathbb{Z}$ is a principal ideal domain, hence every nonzero ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some integer $n > 0$. By the Fundamental Theorem of Arithmetic, we may write $n = p_1^{e_1} \cdots p_k^{e_k}$ for some distinct primes $p_1, \ldots, p_n$ and integers $e_1, \ldots, e_k \geq 0$, so any ascending chain of ideals beginning with $n\mathbb{Z}$ stabilizes in $\mathbb{Z}$. By Definition 2.1.3, $\mathbb{Z}$ is Noetherian.

Proposition 2.1.31. *A principal ideal domain has (Krull) dimension at most one.*

Proof. Every nonzero prime ideal of a principal ideal domain is maximal. Consequently, every maximal strictly descending chain of prime ideals consists of a nonzero prime (maximal) ideal and the zero ideal. We conclude that the (Krull) dimension of a PID is at most one. □

Corollary 2.1.32. *Let k be a field. We have that* $\dim(k[x]) = 1$.

One can show moreover that the n-variate polynomial ring over a field k has dimension n.

Proposition 2.1.33. *Let k be a field. We have that* $\dim(k[x_1, \ldots, x_n]) = n$.

Essentially, the idea is to proceed by induction: the base case has already been established by Corollary 2.1.32. Generally, the following result holds for polynomial rings over Noetherian rings.

Proposition 2.1.34. *Let R be a Noetherian ring. We have that* $\dim(R[x_1, \ldots, x_n]) = \dim(R) + n$.

Remark 2.1.35. There exist Noetherian rings of infinite Krull dimension (cf. [Tom16, Nagata's Example]). On the other hand, there exist commutative unital rings of finite Krull dimension that are not Noetherian (cf. [Suá12]). Both of these examples are quite involved, which illustrates

that such rings are more pathological than ubiquitous. Even more, we will soon see that every Noetherian local ring has finite Krull dimension (cf. Corollary 2.1.43).

Computing the dimension of an arbitrary commutative unital ring can be computationally burdensome. Our immediate aim is therefore to introduce several concepts and facts that can be used to simplify this procedure. We begin by describing the dimension of R in a different way.

Definition 2.1.36. We define the **height** of a prime ideal P of R to be the extended natural number

$$\mathrm{ht}(P) = \sup\{n \mid P \supsetneq P_1 \supsetneq \cdots \supsetneq P_n \text{ and } P_1, \ldots, P_n \in \mathrm{Spec}(R)\},$$

i.e., $\mathrm{ht}(P)$ is the supremum of the lengths of strictly descending chains of prime ideals contained in P. Given an arbitrary ideal I of R, we define $\mathrm{ht}(I) = \inf\{\mathrm{ht}(P) \mid P \supseteq I \text{ and } P \in \mathrm{Spec}(R)\}$.

Proposition 2.1.37. *We have that* $\dim(R) = \sup\{\mathrm{ht}(M) \mid M \in \mathrm{MaxSpec}(R)\}$. *Put another way, the (Krull) dimension of R is the supremum of the heights of the maximal ideals of R.*

Proof. Every strictly descending chain of prime ideals begins with (or can be extended to a strictly descending chain of prime ideals that begins with) a maximal ideal because every maximal ideal is prime and every (prime) ideal is contained in a maximal ideal. Consequently, every maximal strictly descending chain of prime ideals begins with a maximal ideal, and the inequality $\geq$ holds. Conversely, every strictly descending chain of prime ideals contained in a maximal ideal M gives rise to a strictly descending chain of prime ideals of R, and the inequality $\leq$ holds. □

Remark 2.1.38. There exist commutative unital rings in which two maximal ideals have different heights. In fact, there exist Hilbert domains with this property (cf. [Rob73]).

Example 2.1.39. By Proposition 2.1.37, for a local ring $(R, \mathfrak{m})$, we have that $\dim(R) = \mathrm{ht}(\mathfrak{m})$. Particularly, for any prime ideal P of R, we have that $\dim(R_P) = \mathrm{ht}(P)$ (cf. Proposition 2.1.9).

Our next two propositions show that height is a well-behaved invariant.

Proposition 2.1.40. *Let I and J be ideals of a commutative unital ring R.*

(1.) *If* $I \subseteq J$, *then* $\mathrm{ht}(I) \leq \mathrm{ht}(J)$.

(2.) *We have that* $\mathrm{ht}(I) = \mathrm{ht}(\sqrt{I})$, *where* $\sqrt{I}$ *is the* **radical** *of* I, *i.e.,*

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some integer } n \geq 1\}.$$

(3.) *We have that* $\mathrm{ht}(I) + \dim(R/I) \leq \dim(R)$.

(4.) *If* R *is an integral domain that is a finitely generated algebra over a field, then*

$$\mathrm{ht}(I) + \dim(R/I) = \dim(R).$$

Proof. (1.) Observe that any prime ideal P such that $P \supseteq J$ satisfies $P \supseteq I$, hence any prime ideal that satisfies $\mathrm{ht}(J) = \mathrm{ht}(P)$ must satisfy $\mathrm{ht}(I) \leq \mathrm{ht}(P) = \mathrm{ht}(J)$.

(2.) Observe that a prime ideal P satisfies $P \supseteq I$ if and only if it satisfies $P \supseteq \sqrt{I}$. One direction is clear in view of the fact that $I \subseteq \sqrt{I}$. Conversely, if $P \supseteq I$, then for any element $r \in \sqrt{I}$, we have that $r^n \in I$ implies that $r^n \in P$ so that $r \in P$ by the primality of P, i.e., $P \supseteq \sqrt{I}$.

(3.) Let P be a prime ideal of R such that $\mathrm{ht}(I) = \mathrm{ht}(P)$. If $\mathrm{ht}(P)$ is infinite, then we obtain an infinite strictly descending chain of prime ideals $P \supseteq P_1 \supseteq \cdots$, hence $\dim(R)$ is infinite. Otherwise, we obtain a strictly descending chain of prime ideals $P \supsetneq P_1 \supsetneq \cdots \supsetneq P_{n-1} \supsetneq P_n$. On the other hand, every strictly descending chain of prime ideals of R/I corresponds to a strictly descending chain of prime ideals of R such that the smallest (with respect to inclusion) prime ideal contains I. By construction, the longest among these ends with P, so we obtain a strictly descending chain of prime ideals $Q_m \supsetneq \cdots Q_1 \supsetneq P \supsetneq P_1 \cdots \supsetneq P_n$ of R. By definition, we have that

$$\mathrm{ht}(I) + \dim(R/I) = n + m \leq \dim(R).$$

We omit the proof of (4.) for the sake of simplicity. □

Before we move on, we record a short but important fact about radicals.

Proposition 2.1.41. *Let I and J be ideals of a commutative unital ring R.*

(1.) *If $J \subseteq \sqrt{I}$ is finitely generated, then $J^n \subseteq I$ for some integer $n \gg 0$.*

(2.) *If $\sqrt{I}$ is finitely generated, then $\left(\sqrt{I}\right)^n \subseteq I$ for some integer $n \gg 0$.*

Proof. (1.) Consider a finite system of generators $a_1, \ldots, a_j$ of J. By assumption that $J \subseteq \sqrt{I}$, for each integer $1 \leq i \leq j$, there exists an integer $n_i \geq 1$ such that $a_i^{n_i} \in I$. Observe that for any integer $k \geq 1$, the ideal J^k is generated by the products $a_1^{d_1} \cdots a_j^{d_j}$ such that $k = d_1 + \cdots + d_j$. By the Pigeonhole Principle, for the integer $n = n_1 + \cdots + n_j + 1$, we must have that $J^n \subseteq I$.

(2.) We note that this follows immediately from the first part of the proof with $J = \sqrt{I}$. □

Theorem 2.1.42 (Krull's Height Theorem)**.** *Let R be a commutative unital ring. Let I be a proper ideal of R. If I is finitely generated by at least n generators, then* $\mathrm{ht}(I) \leq n$.

Corollary 2.1.43. *Every Noetherian local ring has finite (Krull) dimension.*

Proof. If $(R, \mathfrak{m})$ is a Noetherian local ring, then $\dim(R) = \mathrm{ht}(\mathfrak{m})$ by Example 2.1.39. Even more, $\mathfrak{m}$ is finitely generated by Definition 2.1.3, hence $\mathrm{ht}(\mathfrak{m})$ is finite by Krull's Height Theorem. □

Corollary 2.1.44. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring with unique maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let $\mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$, where $\mathfrak{m}/\mathfrak{m}^2$ is viewed as a k-vector space.*

(1.) *We have that $\mu(\mathfrak{m})$ is the minimum number of generators of $\mathfrak{m}$.*

(2.) *We have that* $\dim(R) \leq \mu(\mathfrak{m})$.

Proof. Observe that (1.) holds by Nakayama's Lemma; (2.) holds by Krull's Height Theorem. □

On its own, the invariant $\mu(\mathfrak{m})$ of a Noetherian local ring $(R, \mathfrak{m})$ is of critical importance.

Definition 2.1.45. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring with residue field $k = R/\mathfrak{m}$. We refer to the invariant $\mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$ as the **embedding dimension** of R.

Definition 2.1.46. We say that a Noetherian local ring $(R, \mathfrak{m})$ is **regular** if $\dim(R) = \mu(\mathfrak{m})$. Generally, a Noetherian ring is regular if the local ring R_P is regular for each prime ideal P of R.

Example 2.1.47. By Example 2.1.29, every field is a regular local ring of dimension zero: the zero ideal is its unique maximal ideal. Conversely, every regular local ring of dimension zero is a field.

Later, in our discussion of regular local rings, we will require the following equivalent characterization of a unique factorization domain in terms of its height-one prime ideals. Our argument hinges upon the well-known fact that an integral domain R is a unique factorization domain if and only if every nonzero prime ideal of R contains a nonzero principal prime ideal of R.

Proposition 2.1.48. *Let R be a Noetherian integral domain. The following are equivalent.*

(1.) *R is a unique factorization domain.*

(2.) *Every prime ideal of R of height one is principal.*

Proof. Let P be a prime ideal of R such that $\text{ht}(P) = 1$. Observe that $\{0_R\}$ is the only height-zero prime ideal of R, hence P must be nonzero. If R is a unique factorization domain, then the nonzero ideal P contains a nonzero principal prime ideal pR. By Krull's Height Theorem, we have that $\text{ht}(pR) \leq 1$. Conversely, the chain of prime ideals $\{0_R\} \subsetneq pR \subseteq$ illustrates that $\text{ht}(pR) = 1$, from which we conclude that $P = pR$ is principal. Conversely, if every prime ideal of R of height one is principal, then every nonzero prime ideal P of R contains a principal prime ideal of R. Clearly, the claim holds trivially if $\text{ht}(P) = 1$; otherwise, we have that $\text{ht}(P) \geq 2$, hence P contains a prime ideal Q of height one. By hypothesis, Q is a nonzero principal prime ideal of R. □

We will soon demonstrate that regular local rings are the most "well-behaved" class of local rings. For instance, any regular local ring is a unique factorization domain (cf. Proposition 2.1.144). Even more, any complete commutative unital Noetherian local ring is the homomorphic image of a complete regular local ring (cf. the Cohen Structure Theorem).

Because we do not yet have the tools to establish these claims, we direct our attention instead to a thorough investigation of the height-zero prime ideals of a commutative unital ring.

Definition 2.1.49. We refer to a prime ideal P of R such that $\text{ht}(P) = 0$ as a **minimal prime** of R. Equivalently, P is a minimal prime of R if and only if for any prime ideal Q of R such that $Q \subseteq P$, we

have that $P = Q$. Equivalently, P is a minimal prime of R if and only if $\dim(R_P) = 0$. Occasionally, it will be convenient for us to denote $\text{MinSpec}(R) = \{P \subseteq R \mid P \text{ is a minimal prime ideal of } R\}$.

Crucially, every commutative unital ring admits a minimal prime ideal.

Proposition 2.1.50. *Let R be a commutative unital ring. Every proper ideal I of R is contained in a prime ideal of R that is minimal with respect to inclusion among all prime ideals of R that contain I. Conversely, every prime ideal of R contains a minimal prime ideal of R.*

Proof. Consider the collection $\mathscr{P} = \{P \in \text{Spec}(R) \mid P \supseteq I\}$. By Zorn's Lemma, the proper ideal I of R is contained in a maximal ideal M of R, hence $\mathscr{P}$ is nonempty. Our proof is complete if $M \supseteq I$ is a maximal chain of prime ideals containing I. Otherwise, there exists a descending chain of prime ideals $M = P_0 \supseteq P_1 \supseteq \cdots$ that contain I. Observe that $P = \bigcap_{i \geq 0} P_i$ is a prime ideal that is minimal with respect to the property that $P \supseteq I$. We conclude that I is contained in a prime ideal of R that is minimal with respect to inclusion among all prime ideals of R that contain I.

Last, for any prime ideal P of R, a similar argument as the above applied to the nonempty collection $\mathscr{Q} = \{Q \in \text{Spec}(R) \mid P \supseteq Q\}$ yields a minimal prime ideal of R that lies in P. □

Conversely, if R is Noetherian, then there are only finitely many minimal prime ideals of R.

Proposition 2.1.51. *Every Noetherian commutative unital ring R admits only finitely many minimal prime ideals. Put another way, we have that* $\text{MinSpec}(R)$ *is finite.*

Proof. (Daniel Katz) We will prove that there are only finitely many minimal prime ideals of the quotient ring R/I for any ideal I of R. Our claims holds by taking I to be the zero ideal.

By the Correspondence Theorem, the elements of $\text{MinSpec}(R/I)$ can be viewed as the prime ideals P of R such that $I \subseteq P$ is a maximal chain of prime ideals containing I. On the contrary, we will assume that $\text{MinSpec}(R/I)$ is infinite, i.e., there exist infinitely many primes P_i such that $I \subseteq P_i$ is a maximal chain of prime ideals containing I. By hypothesis, the collection

$$\mathscr{J} = \{J \subseteq R \mid J \text{ is an ideal of } R \text{ and } J \subseteq P_i \text{ for infinitely many } i\}$$

is nonempty, hence there exists a maximal element M of $\mathscr{J}$ by assumption that R is Noetherian. We claim that M is prime, hence we have reached a contradiction. Explicitly, if M is prime, then we must have that $M \supseteq P_i$ for all integers $i \geq 1$ by the minimality of P_i. But also, we must have that $M \subseteq P_i$ for all integers $i \geq 1$ by definition of M — a contradiction.

On the contrary, if M were not prime, then there would exist elements $a, b \in R \setminus M$ with $ab \in M$. Consequently, we have that $M \subsetneq M + aR$ and $M \subsetneq M + bR$, hence by the maximality of M, neither $M + aR$ nor $M + bR$ is contained in infinitely many of the P_i. Observe that $(M + aR)(M + bR) \subseteq M$ so that $(M + aR)(M + bR)$ is contained in infinitely many of the P_i. Either $M + aR$ or $M + bR$ is contained in infinitely many of the P_i — a contradiction. We conclude that M is prime. □

Before we state our next proposition, we recall that an element $r \in R$ is **nilpotent** if there exists an integer $n \geq 1$ such that $r^n = 0_R$. One can readily verify that the **nilradical** $\sqrt{0_R}$ is the ideal of R consisting of the nilpotent elements of R (cf. Proposition 2.1.40); it lies in every prime ideal of R.

Proposition 2.1.52. *The nilradical $\sqrt{0_R}$ of a commutative unital ring R is the intersection of all minimal prime ideals of R.*

Proof. One direction is straightforward: any nilpotent element of R is contained in all prime ideals of R, hence the nilradical of R is contained in all minimal prime ideals of R.

Conversely, we will show that if x does not belong to the nilradical of R, then it does not belong to some minimal prime ideal of R. Observe that if $x \in R \setminus \sqrt{0_R}$, then x is nonzero and $X = \{x^n \mid n \in \mathbb{Z}_{\geq 0}\}$ is a multiplicatively closed subset of R. Localizing at X yields a nonzero ring $X^{-1}R = R_x$. Considering that R_x is nonzero, there exists a prime ideal PR_x of R_x. By Proposition 2.1.9, there exists a prime ideal P of R that does not contain x. Consequently, there exists a minimal prime ideal of R that does not contain x by Proposition 2.1.50. We conclude that if x is contained in all minimal primes P of R, then x is contained in the nilradical of R. □

We say that R is **reduced** if its nilradical is the zero ideal. Our next proposition shows that if P is a minimal prime ideal of R, then the maximal ideal PR_P of R_P is equal to the nilradical of R_P.

Proposition 2.1.53. *Let R be a commutative unital ring. Let P be a minimal prime ideal of R. We have that PR_P is the nilradical of R_P. Particularly, if R is reduced, then R_P is a field.*

Proof. By the exposition preceding the statement of Proposition 2.1.52, it suffices to show that every element of PR_P is nilpotent. On the contrary, suppose that some element α of PR_P is not nilpotent. By definition, α does not belong to the nilradical of R_P, hence there exists a (minimal) prime ideal QR_P of R_P such that $\alpha \notin QR_P$ by Proposition 2.1.52. Consequently, we obtain a prime ideal Q of R such that $Q \subseteq P$ by Proposition 2.1.9. By assumption that P is a minimal prime ideal of R, we conclude that $P = Q$. But this is impossible because we have that $QR_P \subsetneq PR_P$. We conclude therefore that every element of PR_P is nilpotent so that PR_P is the nilradical of R_P. Ultimately, if R is reduced, then the maximal ideal PR_P of R is zero, hence R_P is a field. □

Observe that any element of the nilradical is a zero divisor, hence in particular, any element of a commutative unital ring that belongs to all minimal prime ideals must be a zero divisor. We demonstrate next that if R is Noetherian, then any element belonging to *any* minimal prime ideal of R must also be a zero divisor; if R is reduced, then the converse holds, as well.

Proposition 2.1.54. *Let R be a commutative unital ring. Let x be an element of R. If x belongs to any minimal prime ideal of R, then x is a zero divisor. Put another way, the non-zero divisors of a commutative unital ring do not belong to any minimal prime ideals. Conversely, if R is reduced, then every zero divisor of R belongs to some minimal prime ideal of R.*

Proof. Let x belong to some minimal prime ideal P. By Proposition 2.1.53, the image of x in PR_P is nilpotent of degree n, hence there exists an integer $n \geq 1$ and an element $t \in R \setminus P$ such that $tx^n = 0_R$ and tx^{n-1} is nonzero. We conclude that $x(tx^{n-1}) = 0_R$ so that x is a zero divisor of R.

We will assume that R is reduced and that x is a zero divisor of R. By definition, there exists a nonzero element $y \in R$ such that $xy = 0_R$. By assumption that R is reduced, the nilradical of R is the zero ideal, hence y does not belong to the nilradical. By Proposition 2.1.52, moreover, y does not belong to some minimal prime ideal P of R. But xy does, so x must belong to P. □

Even more, reduced rings can be embedded in a direct product of fields.

Proposition 2.1.55. *If R is a reduced commutative unital ring, then we may identify R with a subring of a direct product of fields.*

Proof. By Proposition 2.1.53, for every minimal prime P of R, we have that R_P is a field. Consequently, the direct product L of all localizations of R at its minimal primes is a direct product of fields. Consider the ring homomorphism $\lambda : R \to L$ that sends an element $x \in R$ to the tuple consisting of the images of x in R_P for each minimal prime P of R. By definition, if λ maps x to 0, then the image of x in R_P is 0 for each minimal prime P. Consequently, for each minimal prime P of R, there exists an element $t_P \in R \setminus P$ such that $t_P x = 0_R$. But this implies that $t_P x$ belongs to all minimal primes Q of R, hence x must belong to all minimal primes Q of R. By Proposition 2.1.52, we conclude that x belongs to the nilradical of R; this is the zero ideal by assumption. □

Corollary 2.1.56. *If R is a reduced commutative unital ring with only finitely many minimal prime ideals, then we may identify R with a subring of a finite direct product of fields.*

Proof. This follows immediately from Propositions 2.1.55 and 2.1.51. □

Our following proposition will be useful in our discussion of Gorenstein local rings.

Proposition 2.1.57. *If R is a reduced commutative unital ring with only finitely many minimal prime ideals, then the total ring of fractions $Q(R)$ of R is isomorphic to a finite direct product of fields. Explicitly, if $P_1, \ldots, P_n$ are the minimal prime ideals of R, then we have that $Q(R) \cong \prod_{i=1}^{n} R_{P_i}$.*

Proof. By Proposition 2.1.54, the set S of non-zero divisors of R is simply $R \setminus (P_1 \cup \cdots \cup P_n)$. Observe that $Q(R) = S^{-1}R$, hence by Proposition 2.1.9, the prime ideals of $Q(R)$ are precisely $S^{-1}P_1, \ldots, S^{-1}P_n$. By Proposition 2.1.12, we have that $Q(R)/S^{-1}P_i \cong \mathrm{Frac}(R/P_i)$, hence the ideals $S^{-1}P_i$ are all maximal; in particular, they are pairwise comaximal. By the Chinese Remainder Theorem, there exists a surjective ring homomorphism $\varphi : Q(R) \to \prod_{i=1}^{n} (Q(R)/S^{-1}P_i)$ with kernel

$$S^{-1}P_1 \cap \cdots \cap S^{-1}P_n = S^{-1}(P_1 \cap \cdots \cap P_n) = S^{-1}\sqrt{0_R} = S^{-1}0 = 0,$$

where the second equality holds by Proposition 2.1.52. By the First Isomorphism Theorem, it follows that $Q(R) \cong \prod_{i=1}^{n}(Q(R)/S^{-1}P_i)$. Using Proposition 2.1.12 once again, we conclude that $\text{Frac}(R/P_i) \cong R_{P_i}/PR_{P_i} \cong R_{P_i}$, where the second isomorphism holds by Proposition 2.1.53. $\square$

We refer the reader to the sections on Localization as a Functor and The Total Ring of Fractions in the appendix for more information about localization and the total ring of fractions.

2.1.3 Extensions of Rings

Let R be a commutative unital ring. We say that a commutative unital ring S is an **extension** of R if there exists a ring homomorphism $\varphi : R \to S$; alternatively, we might emphasize the map by saying that $\varphi : R \to S$ is an extension of commutative unital rings. One of the most common examples of an extension of rings is that induced by the inclusion $R \subseteq S$ of R as a subring of S.

By definition, a ring extension $\varphi : R \to S$ induces an R-module structure on S via the action $r \cdot s = \varphi(r)s$, where the latter denotes multiplication in S. Even more, for any elements $r, r' \in R$ and $s, s' \in S$, we have that $(r \cdot s)(r' \cdot s') = \varphi(rr')ss'$, hence S is an R-**algebra**. We note that the reader might already be familiar with this terminology in place of "ring extension."

If $\varphi : R \to S$ is an extension of commutative unital rings such that S is a finitely generated R-module with respect to φ, we say that S is a **module-finite extension** of R. On the other hand, if S is finitely generated as an R-algebra with respect to φ, then S is a **finite extension** of R. Even though the names are similar, we cannot overstate the importance of distinguishing these two types of extensions. For instance, for any commutative unital ring R, the univariate polynomial ring $R[x]$ is a finite extension of R because $R[x]$ is generated as an R-algebra by 1_R and x; however, it is not a module-finite extension because there exist polynomials of arbitrarily large degree.

For simplicity, we will assume that R and S are commutative unital rings such that $R \subseteq S$; however, we note that the following results hold for general ring extensions. We say that an element $s \in S$ is **integral** over R if there exists a monic polynomial $x^n + r_1x^{n-1} + \cdots + r_{n-1}x + r_n$ such that $r_1, \ldots, r_n \in R$ and $s^n + r_1s^{n-1} + \cdots + r_{n-1}s + r_n = 0_R$. Our next proposition is well-known.

Proposition 2.1.58 (Determinantal Trick)**.** *Let $R \subseteq S$ be a ring extension. Let I be an ideal of R. Let s be an element of S. If there exists a finitely generated R-module M that is faithful as an $R[s]$-module such that $sM \subseteq IM$, then s is the root of a monic polynomial $x^n + i_1 x^{n-1} + \cdots + i_{n-1}x + i_n$ for some elements $i_1, \ldots, i_n \in R$ such that $i_j \in I^j$ for each integer $1 \leq j \leq n$.*

Proof. Consider the R-module homomorphism $\varphi : M \to M$ defined by $\varphi(m) = sm$. By hypothesis that $\varphi(M) \subseteq IM$, there exist elements $i_1, \ldots, i_n \in R$ such that $i_j \in I^j$ for each integer $1 \leq j \leq n$ and $\varphi^n + i_1\varphi^{n-1} + \cdots + i_{n-1}\varphi + i_n \mathrm{id}_M$ is the zero endomorphism on M by the Cayley-Hamilton Theorem. Consequently, $(s^n + i_1 s^{n-1} + \cdots + i_{n-1}s + i_n)m = 0$ holds for each element $m \in M$, and we conclude that $s^n + i_1 s^{n-1} + \cdots + i_{n-1} + i_n = 0$ by hypothesis that M is a faithful $R[s]$-module. □

Often, the Determinantal Trick is employed for the ideal $I = R$, in which case it states that s is integral over R. Even more, in this setting, the converse holds, hence we obtain the following.

Proposition 2.1.59. *Let $R \subseteq S$ be a ring extension. Let $s \in S$. The following are equivalent.*

(i.) *The element $s \in S$ is integral over R.*

(ii.) *$R[s]$ is a finitely generated R-module.*

(iii.) *$R[s]$ is contained in a subring of S that is finitely generated as an R-module.*

(iv.) *There exists a faithful $R[s]$-module that is finitely generated as an R-module.*

Proof. By definition, if s is integral over R, then we have that $s^n + r_1 s^{n-1} + \cdots + r_{n-1}s + r_n = 0_R$ for some elements $r_1, \ldots, r_n \in R$. Consequently, for any integer $i \geq n$, the element s^i can be written as an R-linear combination of $1_R, s, \ldots, s^{n-1}$. We conclude that $R[s]$ is a finitely generated R-module. Because $R[s]$ is itself a subring of S, property (ii.) implies property (iii.). Likewise, property (iii.) implies property (iv.) because a subring S' of S that contains $R[s]$ is a faithful $R[s]$-module via the multiplication of S. Last, property (iv.) implies property (i.) by the Determinantal Trick. □

We say that S is an **integral extension** of R if every element of S is integral over R. By the previous propositions, a module-finite extension of commutative unital rings is an integral extension.

Corollary 2.1.60. *Let $R \subseteq S$ be a module-finite ring extension. Every element of S is integral over R. Put another way, a module-finite ring extension of R is an integral extension R.*

Proof. By hypothesis, S is a finitely generated R-module that is faithful as an $R[s]$-module because $R[s]$ is a subring of S. By the Determinantal Trick with $I = R$, our proof is complete. □

Conversely, an integral extension of finite type is a module-finite extension.

Corollary 2.1.61. *Let $R \subseteq S$ be a ring extension. The following properties are equivalent.*

(i.) *S is a module-finite extension of R.*

(ii.) *S is an integral extension of R that is finitely generated as an R-algebra.*

(iii.) *There exist elements $s_1, \ldots, s_n \in S$ each of which is integral over R such that $S = R[s_1, \ldots, s_n]$.*

Proof. By Corollary 2.1.60, a module-finite extension of R is an integral extension of R. Considering that a finitely generated R-module is a finitely generated R-algebra, we conclude that statement (i.) implies statement (ii.). By definition of integral extension, statement (ii.) implies statement (iii.). By induction and Proposition 2.1.59, it follows that statement (iii.) implies statement (i.). □

Corollary 2.1.62 (Determinantal Trick, Revisited)**.** *Let $R \subseteq S$ be an integral extension. Let I be an ideal of R. Every element of IS satisfies a monic polynomial $x^n + i_1 x^{n-1} + \cdots + i_{n-1}x + i_n$ for some elements $i_1, \ldots, i_n \in R$ such that $i_j \in I^j$ for each integer $1 \leq j \leq n$.*

Proof. By definition, if $\alpha \in IS$, then $\alpha = r_1 s_1 + \cdots + r_n s_n$ for some elements $r_1, \ldots, r_n \in I$ and $s_1, \ldots, s_n \in S$. By hypothesis that S is an integral extension, it follows that $S' = R[\alpha, s_1, \ldots, s_n]$ is a module-finite extension of R by Corollary 2.1.61. Even more, S' is a faithful $R[\alpha]$-module such that $\alpha S' \subseteq IS'$ because $R[\alpha]$ is a subring of S'. We conclude the result by the Determinantal Trick. □

Our immediate aim is to illustrate that integral extensions exhibit a wealth of nice behavior.

Proposition 2.1.63 (Transitivity of Integral Extensions)**.** *Let $R \subseteq S \subseteq T$ be ring extensions. We have that $R \subseteq T$ is an integral extension if and only if $S \subseteq T$ and $R \subseteq S$ are integral extensions.*

Proof. If $S \subseteq T$ is an integral extension, then for each element $t \in T$, there exist an integer $n \geq 1$ and elements $s_1, \ldots, s_n \in S$ such that $t^n + s_1 t^{n-1} + \cdots + s_{n-1} t + s_n = 0_R$. Crucially, we may view this as an equation of integral dependence of t over $R[s_1, \ldots, s_n]$, hence by Proposition 2.1.59, we find that $R[s_1, \ldots, s_n, t]$ is a finitely generated $R[s_1, \ldots, s_n]$-module. If $R \subseteq S$ is an integral extension, then the elements $s_1, \ldots, s_n$ are integral over R, from which it follows that $R[s_1, \ldots, s_n]$ is a finitely generated R-module by the same proposition as before. Ultimately, we conclude that $R[s_1, \ldots, s_n, t]$ is a finitely generated R-module, hence t is integral over R once again by the same proposition.

Conversely, if $R \subseteq T$ is an integral extension, then $R \subseteq S$ is an integral extension because every element of S lies in T and $S \subseteq T$ is an integral extension because every element of R lies in S. □

Proposition 2.1.64. *Let $R \subseteq S$ be an integral extension of integral domains. If I is a nonzero ideal of S, then $I \cap R$ is a nonzero ideal of R.*

Proof. By hypothesis that $R \subseteq S$ is an integral extension, for any nonzero element $i \in I$, there exist elements $r_1, \ldots, r_n \in R$ such that $i^n + r_1 i^{n-1} + \cdots + r_{n-1} i + r_n = 0_R$. Let k be the smallest index for which r_k is nonzero. We have that $i^k(i^{n-k} + r_1 i^{n-k-1} + \cdots + r_{k+1} i + r_k) = 0_R$, from which it follows that $i^{n-k} + r_1 i^{n-k-1} + \cdots + r_{k+1} i + r_k = 0_R$ because S is a domain. Consequently, we find that $r_k = -i(i^{n-k-1} + r_1 i^{n-k-2} + \cdots + r_{k+1})$ is a nonzero element of $I \cap R$. □

Proposition 2.1.65. *Let $R \subseteq S$ be an integral extension. For any multiplicatively closed subset W of R, we have that $W^{-1}R \subseteq W^{-1}S$ is an integral extension.*

Proof. Consider an element s/w of $W^{-1}S$. By hypothesis that $R \subseteq S$ is an integral extension, there exist elements $r_1, \ldots, r_n \in R$ such that $s^n + r_1 s^{n-1} + \cdots + r_{n-1} s + r_n = 0_R$. We conclude that

$$\left(\frac{s}{w}\right)^n + \frac{r_1}{w}\left(\frac{s}{w}\right)^{n-1} + \cdots + \frac{r_{n-1}}{w^{n-1}}\left(\frac{s}{w}\right) + \frac{r_n}{w^n} = \frac{0_R}{1_R}.$$ □

Theorem 2.1.66 (Lying Over Theorem)**.** *Let $R \subseteq S$ be an integral extension. Given any prime ideal P of R, there exists a prime ideal Q of S* **lying over** *P, i.e., such that $Q \cap R = P$.*

Proof. By Corollary 2.1.62, every element $\alpha \in IS$ satisfies $\alpha^n + i_1 \alpha^{n-1} + \cdots + i_{n-1} \alpha + i_n = 0_R$ for some elements $i_1, \ldots, i_n \in I$. Put another way, for each element $\alpha \in IS$, there exists an integer

$n \gg 0$ such that $\alpha^n \in I$ so that $IS \cap R \subseteq \sqrt{I}$. Considering that $I \subseteq IS \cap R$, we conclude that $IS \cap R = I$ for every radical ideal I. Particularly, if P is a prime ideal of R, then $PS \cap R = P$. By Proposition 2.1.9(6.) applied to the multiplicatively closed subset $W = R \setminus P$ and the ideal PS of S, there exists a prime ideal Q of S such that $Q \supseteq PS$ and $Q \cap (R \setminus P) = \emptyset$, from which it follows that $Q \cap R = P$. □

Theorem 2.1.67 (Incomparability Theorem)**.** *Let $R \subseteq S$ be an integral extension. Given any prime ideal P of R and any prime ideals $Q \subseteq Q'$ of S lying over P, we have that $Q' = Q$. Put another way, every pair of distinct prime ideals of S lying over a prime ideal of R are incomparable.*

Proof. Let $Q \subseteq Q'$ be prime ideals of S such that $Q \cap R = P = Q' \cap R$. Observe that $R/P \subseteq S/Q$ is an integral extension of integral domains: indeed, if $s \in S$ satisfies some monic polynomial, then $s + Q$ satisfies the same monic polynomial modulo Q. By the Lying Over Theorem, we have that $(Q'/Q) \cap (R/P) = 0$. By Proposition 2.1.64, we conclude that $Q'/Q = 0$ so that $Q' = Q$. □

Theorem 2.1.68 (Going Up Theorem)**.** *Let $R \subseteq S$ be an integral extension. Given any chain of prime ideals $P_n \supsetneq \cdots \supsetneq P_1 \supsetneq P_0$ of R and any prime ideal Q_0 of S lying over P_0, there exists a chain of prime ideals $Q_n \supsetneq \cdots \supsetneq Q_1 \supsetneq Q_0$ of S such that Q_i lies over P_i for each integer $1 \leq i \leq n$.*

Proof. We proceed by induction on the length n of a chain of prime ideals of R. We establish the base case; the inductive step holds by a similar argument. By the proof of the Incomparability Theorem, if Q_0 is a prime ideal of S lying over a prime ideal P_0 of R, then $R/P_0 \subseteq S/Q_0$ is an integral extension. Consequently, there exists a nonzero prime ideal Q_1/Q_0 of S/Q_0 lying over the prime ideal P_1/P_0 of R/P_0. But this implies that $P_1 \supsetneq P_0$ is a chain of prime ideals of R and $Q_1 \supsetneq Q_0$ is a chain of prime ideal of S such that $(Q_1/Q_0) \cap (R/P_0) = P_1/P_0$ or $Q_1 \cap R = P_1$. □

Corollary 2.1.69. *If $R \subseteq S$ is an integral extension, then* $\dim(R) = \dim(S)$.

Proof. By the Going Up Theorem, we have that $\dim(R) \leq \dim(S)$. Conversely, for any chain of prime ideals $Q_n \supsetneq \cdots \supsetneq Q_1 \supsetneq Q_0$ of S, there is a chain of prime ideals $(Q_n \cap R) \supsetneq \cdots \supsetneq (Q_1 \cap R) \supsetneq (Q_0 \cap R)$ of R. We conclude that $\dim(R) \geq \dim(S)$ so that equality holds, as desired. □

Our next proposition shows that maximal ideals contract and extend over integral extensions.

Proposition 2.1.70. *Let $R \subseteq S$ is an integral extension.*

(1.) *If M is a maximal ideal of S, then $M \cap R$ is a maximal ideal of R.*

(2.) *If N is a prime ideal of S lying over a maximal ideal of R, then N is a maximal ideal of S.*

Proof. (1.) Given any maximal ideal M of S, the ideal $M' = M \cap R$ is prime. On the contrary, if M' were not maximal, then there would exist a maximal ideal N' of R such that $N' \supsetneq M'$. By the Going Up Theorem, we could find a prime ideal N of S such that $N \supsetneq M$ — a contradiction.

(2.) By the proof of the Incomparability Theorem, the inclusion $R/(N \cap R) \subseteq S/N$ is an integral extension of integral domains. By hypothesis, the ideal $N \cap R$ is maximal, hence $R/(N \cap R)$ is a field. By Proposition 2.1.64, every nonzero ideal of S/N lies over a nonzero ideal of $R/(N \cap R)$. But there are no proper nonzero ideals of $R/(N \cap R)$, hence N must be a maximal ideal of S. □

Even more, any integral extension of a commutative unital Noetherian local ring by a Noetherian commutative unital ring has only finitely many maximal ideals.

Proposition 2.1.71. *Let $(R, \mathfrak{m})$ be a commutative unital Noetherian local ring. If $R \subseteq S$ is an integral extension such that S is Noetherian, then S admits finitely many maximal ideals.*

Proof. By the proof of the Lying Over Theorem, we have that $\mathfrak{m}S \cap R = \mathfrak{m}$. By the proof of the Incomparability Theorem, the inclusion $R/\mathfrak{m} \subseteq S/\mathfrak{m}S$ is an integral extension. Considering that $R/\mathfrak{m}$ is a field, it follows that $\dim(S/\mathfrak{m}S) = 0$ by Proposition 2.1.69. We conclude that $S/\mathfrak{m}S$ is Artinian by Proposition 6.1.2. Consequently, Corollary 6.1.3 yields the result. □

We define the **integral closure** of R as the collection $\overline{R} = \{\alpha \in Q(R) \mid \alpha \text{ is integral over } R\}$. By Corollary 2.1.61, for any elements $\alpha, \beta \in \overline{R}$, we have that $R[\alpha, \beta]$ is an integral extension of R. Consequently, $\alpha - \beta$ and $\alpha\beta$ belong to $\overline{R}$ so that $\overline{R}$ is a commutative unital ring by the Subring Test; in fact, it is the largest (with respect to inclusion) integral extension of R that lies in $Q(R)$.

We provide a concrete description of the integral closure of a reduced Noetherian ring.

Proposition 2.1.72. *If R is a reduced Noetherian commutative unital ring, then the integral closure of R is isomorphic to $\overline{R/P_1} \times \cdots \times \overline{R/P_n}$, where $P_1, \ldots, P_n$ are the minimal prime ideals of R.*

Proof. By hypothesis that R is reduced, we may identify R with a subring of $\prod_{i=1}^{n}(R/P_i)$ via the ring homomorphism $\varphi : R \to \prod_{i=1}^{n}(R/P_i)$ defined by $\varphi(r) = (r+P_1, \ldots, r+P_n)$: we have that $\ker\varphi = P_1 \cap \cdots \cap P_n = \sqrt{0_R} = 0$ by Proposition 2.1.52 and the definition of reduced. Observe that if $(rx_1+P_1, \ldots, rx_n+P_n) = (0_R+P_1, \ldots, 0_R+P_n)$, then $rx_i \in P_i$ for each integer $1 \leq i \leq n$. Particularly, if we have that $x_i \notin P_i$ for each integer $1 \leq i \leq n$, then we must have that $r \in P_1 \cap \cdots \cap P_n$ so that $r = 0_R$. Put another way, the finitely generated R-module $\prod_{i=1}^{n}(R/P_i)$ is faithful (cf. the exposition following Definition 2.1.13). By applying the Determinantal Trick with the ideal $I = R$ and the ring extension $S = \prod_{i=1}^{n}(R/P_i)$, we conclude that $\prod_{i=1}^{n}(R/P_i)$ is an integral extension of R.

Observe that $\overline{R/P_i}$ is integral over R/P_i for each integer $1 \leq i \leq n$, hence we have that $\prod_{i=1}^{n}\overline{R/P_i}$ is integral over $\prod_{i=1}^{n}(R/P_i)$: indeed, if $\alpha_i \in \overline{R/P_i}$ satisfies an equation of integral dependence f_i over R/P_i, then $(f_1(\alpha_1), \ldots, f_n(\alpha_n))$ is an equation of integral dependence of $(\alpha_1, \ldots, \alpha_n)$ over $\prod_{i=1}^{n}(R/P_i)$. By the Transitivity of Integral Extensions, we find that $\prod_{i=1}^{n}\overline{R/P_i}$ is an integral extension of R. We claim that $\prod_{i=1}^{n}\overline{R/P_i} = \overline{\prod_{i=1}^{n}(R/P_i)}$, hence it must be isomorphic to the integral closure of R by Proposition 2.1.57. Observe that the total ring of fractions of $\prod_{i=1}^{n}(R/P_i)$ is $\prod_{i=1}^{n}\mathrm{Frac}(R/P_i)$. If an element $(\alpha_1, \ldots, \alpha_n) \in \prod_{i=1}^{n}\mathrm{Frac}(R/P_i)$ is integral over $\prod_{i=1}^{n}(R/P_i)$, then there exists an equation of integral dependence of α_i over R/P_i for each integer $1 \leq i \leq n$, i.e., we have that $\alpha_i \in \overline{R/P_i}$ for each integer $1 \leq i \leq n$. We conclude that $\overline{\prod_{i=1}^{n}(R/P_i)} \subseteq \prod_{i=1}^{n}\overline{R/P_i}$. □

We say that a commutative unital ring R is **integrally closed** if it holds that $\overline{R} = R$.

Proposition 2.1.73. *Every unique factorization domain is integrally closed.*

Proof. Consider a nonzero element $\frac{r}{s}$ of $\mathrm{Frac}(R)$ that is integral over R. If r and s have some non-unit common factors in R, they will cancel in $\frac{r}{s}$ in $\mathrm{Frac}(R)$, hence we may assume that r and s have no non-unit common factors in R. By assumption that $\frac{r}{s}$ is integral over R, it follows that $\frac{r}{s}$ satisfies some monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ in $R[x]$. We have therefore that

$$\left(\frac{r}{s}\right)^n + \sum_{i=0}^{n-1} a_i\left(\frac{r}{s}\right)^i = 0 \text{ if and only if } \frac{r^n + \sum_{i=0}^{n-1} a_i r^i s^{n-i}}{s^n} = 0 \text{ if and only if } r^n + \sum_{i=0}^{n-1} a_i r^i s^{n-i} = 0_R$$

so that s divides r^n. Consequently, r and s share a common factor of s, from which it follows that

s must be a unit. We conclude that $\frac{r}{s}$ can be identified with an element of R, as desired. □

Corollary 2.1.74. *Every regular local ring is integrally closed. Consequently, every regular ring is* **normal***, i.e., the localizations at its prime ideals are integrally closed integral domains.*

Proof. By Proposition 2.1.144, a regular local ring is a unique factorization domain. □

We conclude with two landmark results on the integral closure of Noetherian rings.

Theorem 2.1.75 (Krull-Akizuki)**.** *[HS06, Theorem 4.9.2] If R is a reduced Noetherian commutative unital ring of dimension one, then any ring extension $R \subseteq S \subsetneq Q(R)$ is Noetherian.*

Theorem 2.1.76 (Nagata)**.** *[HS06, Theorem 4.10.6] If R is a Noetherian integral domain of dimension two, then $\overline{R}$ is Noetherian.*

We establish the useful property of a reduced commutative unital Noetherian local ring of dimension one that every ideal of its integral closure is principal.

Proposition 2.1.77. *If $(R, \mathfrak{m})$ is a reduced commutative unital Noetherian local ring of dimension one, then every ideal of the integral closure of R is principal.*

Proof. (Souvik Dey) By Proposition 2.1.72, we have that $\overline{R} \cong \prod_{i=1}^{n} \overline{R/P_i}$, where $P_1, \ldots, P_n$ are the minimal prime ideals of R. Observe that for each integer $1 \leq i \leq n$, the quotient ring R/P_i is a Noetherian integral domain of dimension one, hence by the Krull-Akizuki Theorem, the integral closures $\overline{R/P_i}$ are Noetherian; each of them is a subring of the field of fractions of the appropriate quotient ring, so they are integral domains. By Proposition 2.1.71, for each integer $1 \leq i \leq n$, there are only finitely many maximal ideals of $\overline{R/P_i}$. Even more, by Proposition 6.2.10, the localization of any $\overline{R/P_i}$ with respect to a prime ideal is once again an integrally closed integral domain that is either a field or has dimension one. Observe that a field is a principal ideal domain. On the other hand, an integrally closed Noetherian local domain of dimension one is a principal ideal domain by [DF04, Theorem 16.2.7]. Consequently, for each integer $1 \leq i \leq n$, we have that $\overline{R/P_i}$ is locally a principal ideal domain, hence every nonzero ideal of $\overline{R/P_i}$ is locally free of rank one by Proposition 6.3.11. By [Jon22, Lemma 10.78.7], every ideal of $\overline{R/P_i}$ is free, hence $\overline{R/P_i}$ is a principal ideal domain. By our opening remarks, we conclude that every ideal of $\overline{R}$ is principal. □

2.1.4 Homological Algebra

Broadly, homological algebra is the study of homomorphisms between algebraic structures such as groups, rings, and modules. One of the most basic motivations to study homological algebra is the observation that the Isomorphism Theorems hold in each of the aforementioned settings, hence it is natural to seek to generalize these theorems to all algebraic structures that behave like groups, rings, and modules. In this section, we will develop many of the tools needed throughout this thesis; we refer the interested reader to [Rot09] for many more interesting details.

Unless otherwise stated, we assume that a commutative ring R possesses a multiplicative identity 1_R. Given any R-modules M and N, we may consider the set of R-module homomorphisms

$$\mathrm{Hom}_R(M,N) = \{\varphi : M \to N \mid \varphi \text{ is an } R\text{-module homomorphism}\}.$$

One can readily verify that $\mathrm{Hom}_R(M,N)$ is itself an R-module via the action $(r \cdot \varphi)(x) = r\varphi(x)$. Our next two propositions illuminate key properties of $\mathrm{Hom}_R(M,N)$ we will soon exploit.

Proposition 2.1.78. *Let M be an R-module. We have that $\mathrm{Hom}_R(R,M) \cong M$ as R-modules.*

Proof. Observe that an R-module homomorphism $\varphi : R \to M$ is uniquely determined by $\varphi(1_R)$. Explicitly, for any element $r \in R$, we have that $\varphi(r) = r\varphi(1_R)$, hence φ can be identified with the R-module homomorphism that sends $r \mapsto r\varphi(1_R)$. Consequently, we obtain an R-module homomorphism $\psi : \mathrm{Hom}_R(R,M) \to M$ defined by $\psi(\varphi) = \varphi(1_R)$. Clearly, it is surjective: for each element $m \in M$, choose the R-module homomorphism $\varphi : R \to M$ defined by $\varphi(r) = rm$. Likewise, we have that $\varphi \in \ker \psi$ if and only if $\varphi(1_R) = 0_R$ if and only if $\varphi(r) = 0$ for all elements $r \in R$ if and only if φ is the zero homomorphism. We conclude that ψ is an R-module isomorphism. □

Observe that for any R-module homomorphisms $\alpha : A \to B$ and $\beta : B \to C$, there exists an R-module homomorphism $\beta \circ \alpha : A \to C$. Consequently, for any R-module homomorphism $\beta : B \to C$, there is a map $\mathrm{Hom}_R(A,\beta) : \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_R(A,C)$ defined by $\mathrm{Hom}_R(A,\beta)(\alpha) = \beta \circ \alpha$.

Proposition 2.1.79. *Let R be a commutative ring. Let A be an R-module. Let $\mathscr{R}$ be the category of R-modules. The map $\mathrm{Hom}_R(A,-):\mathscr{R}\to\mathscr{R}$ that sends B to $\mathrm{Hom}_R(A,B)$ and sends an R-module homomorphism $\beta:B\to C$ to the R-module homomorphism $\mathrm{Hom}_R(A,\beta)$ is a* **covariant functor**.

Proof. We have already established that $\mathrm{Hom}_R(A,B)$ is an R-module for any R-module B. By definition of covariant functor, it suffices to show that (1.) $\mathrm{Hom}_R(A,\mathrm{id}_B)=\mathrm{id}_{\mathrm{Hom}_R(A,B)}$ for any R-module B and (2.) $\mathrm{Hom}_R(A,\gamma\circ\beta)=\mathrm{Hom}_R(A,\gamma)\circ\mathrm{Hom}_R(A,\beta)$ for any R-module homomorphisms $\beta:B\to C$ and $\gamma:C\to D$. Observe that $\mathrm{Hom}_R(A,\mathrm{id}_B)(\alpha)(a)=(\mathrm{id}_B\circ\alpha)(a)=\alpha(a)$ for every R-module homomorphism $\alpha:A\to B$ and every element $a\in A$, hence (1.) holds. Likewise, we have that $\mathrm{Hom}_R(A,\gamma\circ\beta)(\alpha)=\gamma\circ\beta\circ\alpha=\gamma\circ\mathrm{Hom}_R(A,\beta)(\alpha)=\mathrm{Hom}_R(A,\gamma)\circ\mathrm{Hom}_R(A,\beta)(\alpha)$ for any R-module homomorphisms $\alpha:A\to B$, $\beta:B\to C$, and $\gamma:C\to D$ so that (2.) holds. □

Likewise, for any R-module homomorphisms $\alpha:A\to B$ and $\beta:B\to C$, there is an induced map $\mathrm{Hom}_R(\alpha,C):\mathrm{Hom}_R(B,C)\to\mathrm{Hom}_R(A,C)$ defined by $\mathrm{Hom}_R(\alpha,C)(\beta)=\beta\circ\alpha$. One can demonstrate in a manner analogous to Proposition 2.1.79 that the map $\mathrm{Hom}_R(-,C):\mathscr{R}\to\mathscr{R}$ that sends B to $\mathrm{Hom}_R(B,C)$ and sends an R-module homomorphism $\alpha:A\to B$ to the R-module homomorphism $\mathrm{Hom}_R(\alpha,C)$ is a **contravariant functor**, i.e., $\mathrm{Hom}_R(\beta\circ\alpha,C)=\mathrm{Hom}_R(\alpha,C)\circ\mathrm{Hom}_R(\beta,C)$.

We say that a sequence of R-modules and R-module homomorphisms $A\xrightarrow{\alpha}B\xrightarrow{\beta}C$ is **exact at** B whenever $\ker\beta=\mathrm{img}\,\alpha$. Consequently, a sequence of R-modules and R-module homomorphisms $\cdots\xrightarrow{\varphi_{n+1}}M_n\xrightarrow{\varphi_n}M_{n-1}\xrightarrow{\varphi_{n-1}}\cdots$ is **exact** whenever it is exact at M_i for each integer i. Particularly, a sequence $0\to A\xrightarrow{\alpha}B\xrightarrow{\beta}C\to 0$ is a **short exact sequence** if and only if $C=\ker(C\to 0)=\mathrm{img}\,\beta$ (i.e., β is surjective), $\ker\beta=\mathrm{img}\,\alpha$, and $\ker\alpha=\mathrm{img}(0\to A)=0$ (i.e., α is injective).

Proposition 2.1.80. *Let M and N be R-modules. If $0\to A\xrightarrow{\alpha}B\xrightarrow{\beta}C\to 0$ is a short exact sequence of R-modules, the sequences $0\to\mathrm{Hom}_R(M,A)\xrightarrow{\mathrm{Hom}_R(M,\alpha)}\mathrm{Hom}_R(M,B)\xrightarrow{\mathrm{Hom}_R(M,\beta)}\mathrm{Hom}_R(M,C)$ and $0\to\mathrm{Hom}_R(C,N)\xrightarrow{\mathrm{Hom}_R(\beta,N)}\mathrm{Hom}_R(B,N)\xrightarrow{\mathrm{Hom}_R(\alpha,N)}\mathrm{Hom}_R(A,N)$ are also exact. Consequently, the functors $\mathrm{Hom}_R(M,-)$ and $\mathrm{Hom}_R(-,N)$ are* **left-exact** *on the category of R-modules.*

Proof. We will prove the first claim; the second follows analogously. By Proposition 2.1.79, the first sequence is well-defined, so it suffices to prove that it is exact. Consider an R-module homo-

morphism $\varphi : M \to A$ such that $\alpha \circ \varphi = \mathrm{Hom}_R(M, \alpha)(\varphi)$ is the zero homomorphism. By hypothesis, we have that $\ker \alpha = 0$ and $\alpha \circ \varphi(x) = 0$ for all elements $x \in M$, hence we conclude that φ is the zero homomorphism. Consequently, the first sequence is exact at $\mathrm{Hom}_R(M,A)$.

By assumption that $\ker \beta = \mathrm{img}\, \alpha$, it follows that $\beta \circ \alpha \circ \varphi$ is the zero homomorphism for any R-module homomorphism $\varphi : M \to A$. Conversely, take an R-module homomorphism $\psi : M \to B$ such that $\beta \circ \psi$ is the zero homomorphism. By definition, we have that $\psi(x)$ belongs to $\ker \beta$ for all elements $x \in M$. Considering that $\ker \beta = \mathrm{img}\, \alpha$ by assumption, for each element $x \in M$, there exists an element $a_x \in A$ such that $\psi(x) = \alpha(a_x)$. By hypothesis that φ and α are R-module homomorphisms, for every element $x \in M$ and $r \in R$, there exist elements $a_x, a_y, a_{rx+y} \in A$ such that $\alpha(ra_x + a_y) = r\alpha(a_x) + \alpha(a_y) = r\psi(x) + \psi(y) = \psi(rx+y) = \alpha(a_{rx+y})$ and $ra_x + a_y = a_{rx+y}$ by assumption that α is injective. We conclude that the map $\sigma : M \to A$ defined by $\sigma(x) = a_x$ is an R-module homomorphism that satisfies $\psi = \alpha \circ \sigma$, from which it follows that ψ is in the image of $\mathrm{Hom}_R(M, \alpha)$, i.e., the first sequence is exact at $\mathrm{Hom}_R(M,B)$. □

Our previous proposition ensures that if we apply the covariant functor $\mathrm{Hom}_R(M, -)$ to any short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$, we obtain an exact sequence of R-modules $0 \to \mathrm{Hom}_R(M,A) \xrightarrow{\mathrm{Hom}_R(M,\alpha)} \mathrm{Hom}_R(M,B) \xrightarrow{\mathrm{Hom}_R(M,\beta)} \mathrm{Hom}_R(M,C)$; however, the induced cochain complex $0 \to \mathrm{Hom}_R(M,A) \xrightarrow{\mathrm{Hom}_R(M,\alpha)} \mathrm{Hom}_R(M,B) \xrightarrow{\mathrm{Hom}_R(M,\beta)} \mathrm{Hom}_R(M,C) \to 0$ is exact at $\mathrm{Hom}_R(M,C)$ if and only if $\mathrm{Hom}_R(M,\beta)$ is surjective if and only if for every R-module homomorphism $\varphi : M \to C$, there exists an R-module homomorphism $\psi : M \to B$ such that $\varphi = \beta \circ \psi$.

Proposition 2.1.81. *Let R be a commutative ring. We say that an R-module P is* **projective** *if it satisfies any of the following equivalent conditions.*

(i.) *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, then the sequence*

$$0 \to \mathrm{Hom}_R(P,A) \xrightarrow{\mathrm{Hom}_R(P,\alpha)} \mathrm{Hom}_R(P,B) \xrightarrow{\mathrm{Hom}_R(P,\beta)} \mathrm{Hom}_R(P,C) \to 0$$

is exact, i.e., the functor $\mathrm{Hom}_R(P, -)$ is **right-exact** *on the category of R-modules.*

(ii.) *If $\beta : B \to C$ is a surjective R-module homomorphism and $\varphi : P \to C$ is any R-module homomorphism, then there exists an R-module homomorphism $\psi : P \to B$ such that $\varphi = \beta \circ \psi$.*

(iii.) *There exist R-modules B and C, a surjective R-module homomorphism β, and R-modules homomorphisms φ and ψ such that the following diagram commutes.*

$$\begin{array}{ccccc} & & & & P \\ & & \overset{\exists\psi}{\swarrow} & & \downarrow{\scriptstyle \varphi} \\ B & \xrightarrow{\beta} & C & \longrightarrow & 0 \end{array}$$

(iv.) *Every short exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} P \to 0$ of R-modules splits. Explicitly, there exists an R-module isomorphism $\psi : B \to A \oplus C$ such that $\psi \circ \alpha$ is the first component inclusion map $A \to A \oplus C$ and $\beta \circ \psi^{-1}$ is the second component projection map $A \oplus C \to C$.*

(v.) *There exists an R-module Q such that $P \oplus Q$ is a free R-module.*

Proof. By Proposition 2.1.80, one can readily deduce that the first three conditions are equivalent, so it suffices to prove that (ii.) $\implies$ (iv.) $\implies$ (v.) $\implies$ (i.). Consider a short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} P \to 0$. By hypothesis, there exists an R-module homomorphism $\psi : P \to B$ such that $\mathrm{id}_P = \beta \circ \psi$. Particularly, the following diagram of R-modules commutes.

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \overset{\psi}{\swarrow} & \downarrow{\scriptstyle \mathrm{id}_P} & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & P & \longrightarrow & 0 \end{array}$$

By assumption that β is surjective, for any element $p \in P$, there exists an element $b \in B$ such that $p = \beta(b)$ and $\psi(p) = \psi \circ \beta(b)$. Conversely, for every element $b \in B$, we have that $\beta(b) \in P$, and we may consider the element $\psi \circ \beta(b)$ of B. Ultimately, for any element $b \in B$, observe that

$$\beta(b - \psi \circ \beta(b)) = \beta(b) - \beta \circ \psi \circ \beta(b) = \beta(b) - \mathrm{id}_P \circ \beta(b) = \beta(b) - \beta(b) = 0$$

so that $b - \psi \circ \beta(b)$ belongs to $\ker \beta$. By hypothesis that $\ker \beta = \operatorname{img} \alpha$, there exists an element $a \in A$ such that $b - \psi \circ \beta(b) = \alpha(a)$ and $b = \alpha(a) + \psi \circ \beta(b)$. We conclude that $B = \operatorname{img} \alpha + \operatorname{img} \psi$. We claim moreover that $\operatorname{img} \alpha \cap \operatorname{img} \psi = \{0\}$. For if $x \in \operatorname{img} \alpha \cap \operatorname{img} \psi$, then $\alpha(a) = x = \psi(y)$ for

some elements $a \in A$ and $y \in P$. Consequently, we have that $y = \beta \circ \psi(y) = \beta(x) = \beta \circ \alpha(a) = 0$ and $x = \psi(y) = \psi(0) = 0$. We conclude that $B = \operatorname{img} \alpha \oplus \operatorname{img} \psi \cong A \oplus P$, where the isomorphism follows from the fact that α is injective by hypothesis and ψ is injective because β is a left-inverse. Ultimately, the R-module isomorphism $\varphi : B \to A \oplus P$ defined by $\varphi(\alpha(a) + \psi(p)) = (a, p)$ satisfies that $\varphi \circ \alpha$ is the inclusion map $A \to A \oplus P$ and $\beta \circ \varphi^{-1}$ is the projection map $A \oplus P \to P$.

Every R-module is the homomorphic image of a free R-module. Particularly, there exists a free R-module F and an R-module K such that $0 \to K \to F \to P \to 0$ is a short exact sequence of R-modules. If condition (iv.) holds, then we have that $F = P \oplus K$ is a free R-module.

Last, we will assume that property (v.) holds. Consider a short exact sequence of R-modules $0 \to A \to B \to C \to 0$ with the surjective map $\beta : B \to C$ specified. We claim that $\operatorname{Hom}_R(P, -)$ is right-exact, i.e., we must show that for every R-module homomorphism $\varphi : P \to C$, there exists an R-module homomorphism $\psi : P \to B$ such that $\varphi = \beta \circ \psi$. By hypothesis, there exists an R-module Q such that $F = P \oplus Q$ is free. Consequently, there exists an R-module basis $\mathscr{B} = \{f_i \mid i \in I\}$ of F. Let $\rho : P \to F$ denote the first component inclusion map, and let $\sigma : F \to P$ denote the second component projection map. By assumption that β is surjective, every element of C can be written as $\beta(b)$ for some element $b \in B$. We may therefore find elements b_i of B such that $\beta(b_i) = \varphi \circ \sigma(f_i)$ for each index i. By the freeness of F, there exists a unique homomorphism $\gamma : F \to B$ such that $\gamma(f_i) = b_i$. Observe that $\beta \circ \gamma(f_i) = \beta(b_i) = \varphi \circ \sigma(f_i)$ so that $\beta \circ \gamma = \varphi \circ \sigma$, as $\mathscr{B}$ is a basis. We conclude that $\varphi = \varphi \circ \sigma \circ \rho = \beta \circ \gamma \circ \rho = \beta \circ \psi$ for the map $\psi = \gamma \circ \rho \in \operatorname{Hom}_R(P, B)$. □

Corollary 2.1.82. *Every free R-module is projective.*

Corollary 2.1.83. *Let R be a Noetherian commutative ring. If P is a projective R-module that admits finitely generated free R-modules $F_0, F_1, \ldots, F_n$ such that $0 \to F_n \to \cdots \to F_1 \to F_0 \to P \to 0$ is an exact sequence, then there exist positive integers i and j such that $P \oplus R^i \cong R^j$.*

Proof. We proceed by induction on n. Clearly, if $n = 0$, then P is a free R-module. Even more, if $n = 1$, then there exists a short exact sequence $0 \to F_1 \to F_0 \to P \to 0$ of R-modules. By Proposition 2.1.81(iv.), we conclude that $R^j = F_0 \cong P \oplus F_1 = P \oplus R^i$ for some positive integers i and j. By

hypothesis, there exist exact sequences of R-modules $0 \to F_n \to \cdots \to F_2 \to F_1 \to K \to 0$ and $0 \to K \to F_0 \to P \to 0$ such that $K = \ker(F_0 \to P)$. By the same proposition as before, the R-module K is projective; it admits finitely generated free R-modules $F_1, F_2, \ldots, F_n$ that induce an exact sequence, hence by induction, we conclude that $K \oplus R^k \cong R^j$ for some positive integers j and k. Ultimately, there exists positive integers i and j such that $R^i = F_0 \oplus R^k \cong (P \oplus K) \oplus R^k \cong P \oplus R^j$. □

By Proposition 2.1.80, if we apply the contravariant functor $\mathrm{Hom}_R(-,N)$ to any short exact sequences of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$, we obtain an exact sequence of R-modules $0 \to \mathrm{Hom}_R(C,N) \xrightarrow{\mathrm{Hom}_R(\beta,N)} \mathrm{Hom}_R(B,N) \xrightarrow{\mathrm{Hom}_R(\alpha,N)} \mathrm{Hom}_R(A,N)$. Like before, the induced map $\mathrm{Hom}_R(\alpha,N)$ is surjective if and only if for every R-module homomorphism $\varphi : A \to N$, there exists an R-module homomorphism $\psi : B \to N$ such that $\varphi = \psi \circ \alpha$.

Proposition 2.1.84. *Let R be a commutative ring. We say that an R-module Q is* **injective** *if it satisfies any of the following equivalent conditions.*

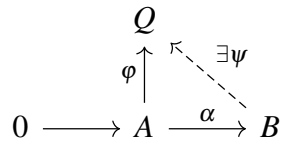
(i.) *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, then the sequence*

$$0 \to \mathrm{Hom}_R(C,Q) \xrightarrow{\mathrm{Hom}_R(\beta,Q)} \mathrm{Hom}_R(B,Q) \xrightarrow{\mathrm{Hom}_R(\alpha,Q)} \mathrm{Hom}_R(A,Q) \to 0$$

is exact, i.e., the functor $\mathrm{Hom}_R(-,Q)$ is right-exact on the category of R-modules.

(ii.) *If $\alpha : A \to B$ is an injective R-module homomorphism and $\varphi : A \to Q$ is any R-module homomorphism, then there exists an R-module homomorphism $\psi : B \to Q$ such that $\varphi = \psi \circ \alpha$.*

(iii.) *There exist R-modules A and B, an injective R-module homomorphism α, and R-modules homomorphisms φ and ψ such that the following diagram commutes.*



(iv.) *Every short exact sequence $0 \to Q \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ of R-modules splits. Explicitly, there exists*

an R-module isomorphism $\psi : B \to Q \oplus C$ such that $\psi \circ \alpha$ is the first component inclusion map $Q \to Q \oplus C$ and $\beta \circ \psi^{-1}$ is the second component projection map $Q \oplus C \to C$.

(v.) *If Q is an R-submodule of M, then there exists an R-module P such that $M = P \oplus Q$.*

Proof. Conditions (i.), (ii.), and (iii.) are equivalent by Proposition 2.1.80, so it suffices to establish that (iii.) $\implies$ (iv.) $\implies$ (v.) $\implies$ (ii.). Observe that any short exact sequence of R-modules whose first nonzero term is Q can be completed to a commutative diagram of R-modules as follows.

$$\begin{array}{ccccccccc} & & & & Q & & & & \\ & & & & \uparrow{\scriptstyle \mathrm{id}_Q} & \nwarrow{\scriptstyle \exists \psi} & & & \\ 0 & \longrightarrow & Q & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \end{array}$$

Consequently, the R-module homomorphism $\psi : B \to Q$ satisfies $\mathrm{id}_Q = \psi \circ \alpha$. Given any element $b \in B$, we have that $b = \alpha \circ \psi(b) + (b - \alpha \circ \psi(b))$. Observe that

$$\psi(b - \alpha \circ \psi(b)) = \psi(b) - \psi \circ \alpha \circ \psi(b) = \psi(b) - \psi(b) = 0,$$

hence we have that $b - \alpha \circ \psi(b) \in \ker \psi$. We conclude that $B = \operatorname{img} \alpha + \ker \psi$. Even more, the sum is direct: if $b \in \operatorname{img} \alpha \cap \ker \psi$, then $b = \alpha(q)$ so that $0 = \psi(b) = \psi \circ \alpha(q) = q$ and $b = \alpha(0) = 0$. By hypothesis that α is injective, we find that $\operatorname{img} \alpha \cong Q$. On the other hand, for every element $c \in C$, there exists an element $b \in B$ such that $c = \beta(b)$. Considering that $B = \operatorname{img} \alpha \oplus \ker \psi$, there exist unique elements $q \in Q$ and $x \in \ker \psi$ such that $c = \beta(b) = \beta(\alpha(q) + x) = \beta(x)$, where the third equality follows from the fact that $\ker \beta = \operatorname{img} \alpha$. We conclude that $\ker \psi \cong C$. Ultimately, we find that $B = \operatorname{img} \alpha \oplus \ker \psi \cong Q \oplus C$ via the R-module homomorphism $\psi(\alpha(q) + x) = (q, \beta(x))$.

Observe that if Q is an R-submodule of M, then the inclusion $Q \subseteq M$ induces a short exact sequence of R-modules $0 \to Q \to M \to M/Q \to 0$. If every short exact sequence of R-modules splits, then we have that $M \cong Q \oplus (M/Q)$, hence Q is a direct summand of M.

We prove (v.) $\implies$ (ii.) as a corollary of Proposition 2.1.109. Explicitly, Q is an R-submodule of an injective R-module E, so it is a direct summand of E. But this implies that Q is injective. $\square$

Our next example illustrates that some modules are neither projective nor injective.

Example 2.1.85. Let $n \geq 2$ be an integer. Let $M = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n. Observe that M is a $\mathbb{Z}$-module because it is an abelian group; however, it is not projective because for any abelian group G, the $\mathbb{Z}$-module $(\mathbb{Z}/n\mathbb{Z}) \oplus G$ has torsion. On the other hand, multiplication by n is an injective $\mathbb{Z}$-module homomorphism $n\cdot : \mathbb{Z} \to \mathbb{Z}$; however, for the canonical surjection $\pi : \mathbb{Z} \to M$, there does not exist a $\mathbb{Z}$-module homomorphism $\psi : \mathbb{Z} \to M$ such that $\pi = \psi \circ \cdot n$, as the latter is always zero. Consequently, the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ is neither projective nor injective.

Consequently, we may seek to measure the injective (or projective) "defect" of a module over a commutative unital ring. We define this notion rigorously as follows.

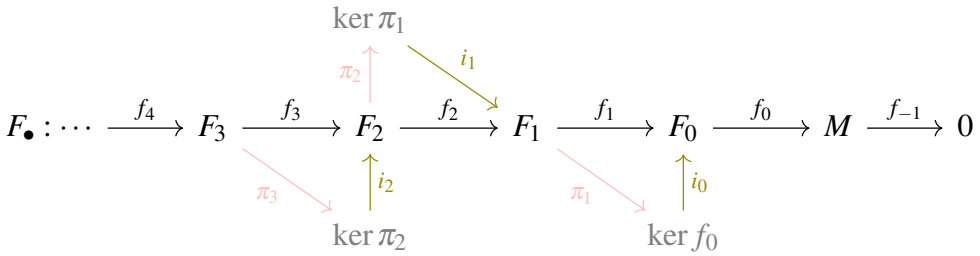
Let M be an R-module. We say that a sequence of R-modules and R-module homomorphisms

$$Z_\bullet : \cdots \xrightarrow{z_{n+1}} Z_n \xrightarrow{z_n} \cdots \xrightarrow{z_2} Z_1 \xrightarrow{z_1} Z_0 \xrightarrow{z_0} M \xrightarrow{z_{-1}} 0$$

is a (left) **resolution** of M if $Z_\bullet$ is exact at M and Z_i for each integer $i \geq 0$. If the R-modules Z_i are free for each integer $i \geq 0$, then $Z_\bullet$ is simply called a **free resolution** of M.

Proposition 2.1.86. *Every R-module admits a free resolution.*

Proof. Let M be an R-module. Observe that there exists a free R-module F_0 indexed by M and a surjective R-module homomorphism $f_0 : F_0 \to M$; its kernel injects into F_0 via the inclusion map $i_0 : \ker f_0 \to F_0$. Considering that $\ker f_0$ is an R-module, there exists a free R-module F_1 indexed by $\ker f_0$ and a surjective R-module homomorphism $\pi_1 : F_1 \to \ker f_0$. Consequently, the composition $f_1 = i_0 \circ \pi_1$ yields a map $f_1 : F_1 \to F_0$ such that $\operatorname{img} f_1 = \operatorname{img} \pi_1 = \ker f_0$. Likewise, the R-module $\ker \pi_1$ injects into F_1 via the inclusion map $i_1 : \ker \pi_1 \to F_1$, and there exists a free R-module F_2 indexed by $\ker \pi_1$ and a surjective R-module homomorphism $\pi_2 : F_2 \to \ker \pi_1$. Consequently, the composition $f_2 = i_1 \circ \pi_2$ yields a map $f_2 : F_2 \to F_1$ such that $\operatorname{img} f_2 = \operatorname{img} \pi_2 = \ker \pi_1 = \ker f_1$. Continuing in this manner produces the following commutative diagram of R-modules.



Consequently, the sequence $F_\bullet$ is a resolution of M in which each of the R-modules F_i is free. □

Combined, Proposition 2.1.86 and Corollary 2.1.82 imply that any R-module M admits a **projective resolution**, i.e., a (left) resolution $P_\bullet : \cdots \xrightarrow{p_{n+1}} P_n \xrightarrow{p_n} \cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} M \xrightarrow{p_{-1}} 0$ in which P_i is projective for each integer $i \geq 0$. Given an R-module N, consider the cochain complex

$$\mathrm{Hom}_R(P_\bullet, N) : 0 \to \mathrm{Hom}_R(P_0, N) \xrightarrow{p_0^*} \mathrm{Hom}_R(P_1, N) \xrightarrow{p_1^*} \cdots \xrightarrow{p_{n-1}^*} \mathrm{Hom}_R(P_n, N) \xrightarrow{p_n^*} \cdots$$

with cochain maps defined by $p_i^* = \mathrm{Hom}_R(p_{i+1}, N)$ for each integer $i \geq 0$. We define the ith cohomology module $\mathrm{Ext}_R^i(M,N) = \ker p_i^* / \operatorname{img} p_{i-1}^*$ for each integer $i \geq 0$. Crucially, Cartan and Eilenberg demonstrated that $\mathrm{Ext}_R^i(M,N)$ is independent of the choice of a projective resolution of M, hence the R-modules $\mathrm{Ext}_R^i(M,N)$ are well-defined (cf. [Rot09, Proposition 6.56]).

Proposition 2.1.87. *Let N be an R-module. The following properties hold.*

(1.) *We have that $\mathrm{Ext}_R^0(M,N) \cong \mathrm{Hom}_R(M,N)$ for all R-modules M.*

(2.) *Every short exact sequence of R-modules $0 \to M' \to M \to M'' \to 0$ induces an exact sequence*
$\cdots \to \mathrm{Ext}_R^{i-1}(M'',N) \to \mathrm{Ext}_R^i(M',N) \to \mathrm{Ext}_R^i(M,N) \to \mathrm{Ext}_R^i(M'',N) \to \mathrm{Ext}_R^{i+1}(M',N) \to \cdots$.

(3.) *We have that $\mathrm{Ext}_R^i(M,N) = 0$ for all $i \geq 1$ and all R-modules M if and only if N is injective.*

Proof. (1.) Consider a projective resolution $P_\bullet$ of M that ends with the terms $P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} M \to 0$. By Proposition 2.1.80, we may apply $\mathrm{Hom}_R(-,N)$ to obtain the sequence of R-modules

$$0 \to \mathrm{Hom}_R(M,N) \xrightarrow{\mathrm{Hom}_R(p_0,N)} \mathrm{Hom}_R(P_0,N) \xrightarrow{\mathrm{Hom}_R(p_1,N)} \mathrm{Hom}_R(P_1,N)$$

exact in the first two places. Consequently, we find that $\ker p_0^* = \operatorname{img} \operatorname{Hom}_R(p_0, N) \cong \operatorname{Hom}_R(M,N)$ by the First Isomorphism Theorem. We conclude that $\operatorname{Ext}_R^0(M,N) = \ker p_0^* \cong \operatorname{Hom}_R(M,N)$.

(3.) We assume first that N is injective. By Proposition 2.1.84, the functor $\operatorname{Hom}_R(-,N)$ is exact, hence for any R-module M and any projective resolution $P_\bullet$ of M, the induced cochain complex $\operatorname{Hom}_R(P_\bullet, N)$ is exact. We conclude that $\operatorname{Ext}_R^i(M,N) = 0$ for all integers $i \geq 1$. Conversely, suppose that $\operatorname{Ext}_R^i(M,N) = 0$ for all $i \geq 1$ and all R-modules M. Consequently, for any short exact sequence of R-modules $0 \to M' \to M \to M'' \to 0$, there exists a long exact sequence of R-modules that begins $0 \to \operatorname{Hom}_R(M'',N) \to \operatorname{Hom}_R(M,N) \to \operatorname{Hom}_R(M',N) \to 0$. By Proposition 2.1.81, N is injective.

We omit the proof of property (2.), but we refer the reader to [Rot09, Corollary 6.46]. □

One can show that $\operatorname{Ext}_R^i(-,N)$ is a contravariant functor from the category of R-modules to itself that preserves multiplication (cf. [Rot09, Theorem 6.37 and Proposition 6.38]), hence Proposition 2.1.87 implies that the functors $\operatorname{Ext}_R^i(-,N)$ measure the injective "defect" of N.

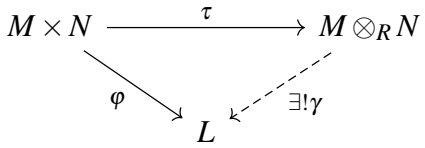
One might naturally expect that in order to rigorously define the projective "defect" of an R-module M, we must look at the cohomology modules of the induced cochain complex obtained by applying $\operatorname{Hom}_R(M,-)$ to an injective resolution of some R-module; however, it is unclear that an arbitrary R-module admits an injective resolution. Consequently, we must first establish that every R-module admits an injective resolution; then, we will proceed in a manner analogous to the exposition preceding Proposition 2.1.87. We begin by constructing a functor from the category of R-modules to itself that forms an "adjoint pair" with the covariant functor $\operatorname{Hom}_R(M,-)$.

Let M and N be R-modules. Consider the free R-module F with basis $M \times N$. Explicitly, we view F as the set of all finite formal R-linear combinations of pairs of elements of F with pointwise addition and scalar multiplication. Let $\mathscr{R}$ denote the R-submodule of F generated by all elements of the form $(m_1 + m_2, n) - (m_1, n) - (m_2, n)$, $(m, n_1 + n_2) - (m, n_1) - (m, n_2)$, $(rm, n) - r(m, n)$, and $(m, rn) - r(m, n)$ for any element $r \in R$. We define the **tensor product** of M and N with respect to R as the quotient R-module $M \otimes_R N = F/\mathscr{R}$. Observe that every element of $M \otimes_R N$ is of the form $\sum_{i=1}^k r_i(m_i, n_i) + \mathscr{R}$ for some integer $k \geq 0$, some elements $r_1, \ldots, r_k \in R$, and some distinct elements $m_1, \ldots, m_k \in M$, and $n_1, \ldots, n_k \in N$. Conventionally, we write such an element as

$\sum_{i=1}^{k} r_i(m_i \otimes_R n_i)$; elements of the form $m \otimes_R n$ are called the **pure tensors** of $M \otimes_R N$, hence by definition, the pure tensors generated $M \otimes_R N$ as an R-module. Even more, by construction, there is a canonical R-module homomorphism $\tau : M \times N \to M \otimes_R N$ defined by $(m,n) \mapsto m \otimes_R n$; it is R-**bilinear**, i.e., it satisfies $\tau(m_1 + m_2, n) = \tau(m_1, n) + \tau(m_2, n)$, $\tau(m, n_1 + n_2) = \tau(m, n_1) + \tau(m, n_2)$, and $\tau(rm, n) = r\tau(m, n) = \tau(m, rn)$ for all elements $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, and $r \in R$.

One can alternatively describe the tensor product of M and N with respect to R as the unique solution to the following universal mapping problem. Given any R-modules M and N, we seek an R-module T and a bilinear R-module homomorphism $\tau : M \times N \to T$ such that for any R-module L and any bilinear R-module homomorphism $\varphi : M \times N \to L$, there exists a unique bilinear R-module homomorphism $\gamma : T \to L$ such that $\varphi = \gamma \circ \tau$ (cf. [Gat13, Propositions 5.4 and 5.5]).

Proposition 2.1.88 (Universal Property of the Tensor Product)**.** *Let R be a commutative ring. Let M and N be R-modules. If L is an R-module such that there exists a bilinear R-module homomorphism $\varphi : M \times N \to L$, then there exists a unique bilinear R-module homomorphism $\gamma : M \otimes_R N \to L$ such that $\varphi = \gamma \circ \tau$, i.e., such that the following diagram of R-modules commutes.*



Unsurprisingly, the Universal Property of the Tensor Product yields an abundance of results.

Proposition 2.1.89. *Let R be a commutative ring. Let M and N be R-modules.*

(1.) *We have that $M \otimes_R N \cong N \otimes_R M$.*

(2.) *We have that $R \otimes_R M \cong M$.*

(3.) *We have that $(R/I) \otimes_R M \cong M/IM$ for any ideal I of R.*

(4.) *For any (possibly infinite) index set I and any family of R-modules $(M_i)_{i \in I}$, we have that $(\bigoplus_{i \in I} M_i) \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N)$, i.e., the tensor product commutes with direct sums.*

Proof. (1.) By the Universal Property of the Tensor Product, the bilinear R-module homomorphisms $\sigma_1 : M \times N \to N \otimes_R M$ and $\sigma_2 : N \times M \to M \otimes_R N$ defined by $\sigma_1(m,n) = n \otimes_R m$ and $\sigma_2(n,m) = m \otimes_R n$ induce the following commutative diagrams of R-modules.

$$\begin{array}{ccc} M \times N & \xrightarrow{\tau_1} & M \otimes_R N \\ \downarrow{\scriptstyle \sigma_1} & \swarrow{\scriptstyle \exists \gamma_1} & \\ N \otimes_R M & & \end{array} \qquad \begin{array}{ccc} N \times M & \xrightarrow{\tau_2} & N \otimes_R M \\ \downarrow{\scriptstyle \sigma_2} & \swarrow{\scriptstyle \exists \gamma_2} & \\ M \otimes_R N & & \end{array}$$

We claim that γ_1 and γ_2 are inverses, hence they are isomorphisms. Observe that for every element $(m,n) \in M \times N$, we have that $\tau_2(n,m) = n \otimes_R m = \sigma_1(m,n) = \gamma_1 \circ \tau_1(m,n) = \gamma_1(m \otimes_R n)$. Consequently, we find that $\gamma_2 \circ \gamma_1(m \otimes_R n) = \gamma_2 \circ \tau_2(n,m) = \sigma_2(n,m) = m \otimes_R n$ so that $\gamma_2 \circ \gamma_1$ is the identity homomorphism on the pure tensors of $M \otimes_R N$. Considering that the pure tensors generated $M \otimes_R N$ as an R-module, we conclude that $\gamma_2 \circ \gamma_1$ is the identity homomorphism on $M \otimes_R N$. Conversely, $\gamma_1 \circ \gamma_2$ is the identity homomorphism on $N \otimes_R M$, as desired.

(2.) By definition, the R-module action of R on M induces a bilinear R-module homomorphism $\mu : R \times M \to M$ defined by $\mu(r,m) = rm$. Once again, the Universal Property of the Tensor Product guarantees the existence of a bilinear R-module homomorphism $\gamma : R \otimes_R M \to M$ that satisfies $rm = \mu(r,m) = \gamma \circ \tau(r,m) = \gamma(r \otimes_R m)$ for all elements $(r,m) \in R \times M$. We will construct an inverse homomorphism for γ. Consider the map $\varphi : M \to R \otimes_R M$ defined by $\varphi(m) = 1_R \otimes_R m$. By the properties of the tensor product, φ is an R-module homomorphism. Observe that for every element $m \in M$, we have that $m = 1_R m = \gamma(1_R \otimes_R m) = \gamma \circ \varphi(m)$. Conversely, for any pure tensor $r \otimes_R m$, we have that $r \otimes_R m = r(1_R \otimes_R m) = r\varphi(m) = \varphi(rm) = \varphi \circ \gamma(r \otimes_R m)$.

(3.) We may view M/IM as an R/I-module via the action $(r+I) \cdot (m+IM) = rm + IM$. Consequently, we obtain a bilinear R-module homomorphism $\mu : (R/I) \times M \to M/IM$ defined by $\mu(r+I,m) = rm+IM$; the Universal Property of the Tensor Product ensures that there is a bilinear R-module homomorphism $\gamma : (R/I) \otimes_R M \to M/IM$ that sends $(r+I) \otimes_R m \mapsto rm+IM$. We claim that the R-linear map $\varphi : M/IM \to (R/I) \otimes_R M$ defined by $\varphi(m+IM) = (1_R+I) \otimes_R m$ is well-defined. If $m+IM = n+IM$, then there exist elements $r_1, \ldots, r_k \in I$ and $x_1, \ldots, x_k \in M$ such that

$m-n = r_1x_1 + \cdots + r_kx_k$. Considering that $r_i + I = 0_R + I$ for each integer $1 \leq i \leq k$, we find that

$$(1_R + I) \otimes_R (m-n) = (1_R + I) \otimes_R \left(\sum_{i=1}^{k} r_i x_i \right) = \sum_{i=1}^{k} [(r_i + I) \otimes_R x_i] = 0$$

so that $\varphi(m + IM) = (1_R + I) \otimes_R m = (1_R + I) \otimes_R n = \varphi(n + IM)$. One can check in a manner analogous to the previous paragraph the φ and γ are inverse homomorphisms.

(4.) Given any (possibly infinite) index set I and any family of R-modules $(M_i)_{i \in I}$, the tensor product yields a bilinear R-module homomorphism $\sigma : (\bigoplus_{i \in I} M_i) \times N \to \bigoplus_{i \in I} (M_i \otimes_R N)$ that sends $((m_i)_{i \in I}, n) \mapsto (m_i \otimes_R n)_{i \in I}$. By the Universal Property of the Tensor Product, there exists a bilinear R-module homomorphism $\gamma : (\bigoplus_{i \in I} M_i) \otimes_R N \to \bigoplus_{i \in I} (M_i \otimes_R N)$ such that $\sigma = \gamma \circ \tau$. Likewise, for each index $i \in I$, there exists an R-module homomorphism $\varphi_i : M_i \otimes_R N \to (\bigoplus_{i \in I} M_i) \otimes_R N$ that sends $m_i \otimes_R n \mapsto (\delta_{ij} m_j)_{j \in I} \otimes_R n$ for the Kronecker delta δ_{ij}. By definition, the elements of $\bigoplus_{i \in I} (M_i \otimes_R N)$ are I-tuples with finitely many nonzero components, hence we obtain an R-module homomorphism $\varphi : \bigoplus_{i \in I} (M_i \otimes_R N) \to (\bigoplus_{i \in I} M_i) \otimes_R N$ that sends $(m_i \otimes_R n)_{i \in I} \mapsto \sum_{i \in I} \varphi_i(m_i \otimes_R n)$. One can readily verify that γ and φ are inverses on the pure tensors, hence they are inverses. $\square$

Our next proposition extends the notion of a tensor product to R-module homomorphisms.

Proposition 2.1.90. *Let R be a commutative ring. Let $\varphi : M \to M'$ and $\psi : N \to N'$ be R-module homomorphisms. There exists a bilinear R-module homomorphism $\gamma_{\varphi,\psi} : M \otimes_R N \to M' \otimes_R N'$ defined by $\gamma_{\varphi,\psi}(m \otimes_R n) = \varphi(m) \otimes_R \psi(n)$. Consequently, the assignment $\eta(\varphi \otimes_R \psi) = \gamma_{\varphi,\psi}$ induces an R-module homomorphism $\eta : \mathrm{Hom}_R(M, M') \otimes_R \mathrm{Hom}_R(N, N') \to \mathrm{Hom}_R(M \otimes_R N, M' \otimes_R N')$.*

Proof. Consider the map $\sigma : M \times N \to M' \otimes_R N'$ defined by $\sigma(m,n) = \varphi(m) \otimes_R \varphi(n)$. By hypothesis that φ and ψ are R-module homomorphisms, it follows that σ is a bilinear R-module homomorphism by construction of the tensor product. Consequently, by the Universal Property of the Tensor Product, there exists a unique bilinear R-module homomorphism $\gamma_{\varphi,\psi} : M \otimes_R N \to M' \otimes_R N'$ defined by $\gamma_{\varphi,\psi}(m \otimes_R n) = \varphi(m) \otimes_R \psi(n)$. Put another way, the assignment $\eta(\varphi \otimes_R \psi) = \gamma_{\varphi,\psi}$ induces a well-defined map $\eta : \mathrm{Hom}_R(M, M') \otimes_R \mathrm{Hom}_R(N, N') \to \mathrm{Hom}_R(M \otimes_R N, M' \otimes_R N')$; it is not difficult to verify that η is R-linear, but we leave the details to the reader. $\square$

Remark 2.1.91. Often, the induced R-module homomorphism $\gamma_{\varphi,\psi} : M \otimes_R N \to M' \otimes_R N'$ is denoted simply by $\varphi \otimes_R \psi$; this is an abuse of notation, but the meaning is clear.

Corollary 2.1.92. *Let R be a commutative ring. Let M be an R-module. Let $\mathscr{R}$ be the category of R-modules. The map $M \otimes_R - : \mathscr{R} \to \mathscr{R}$ that sends A to $M \otimes_R A$ and sends an R-module homomorphism $\varphi : A \to A'$ to the R-module homomorphism $\mathrm{id}_M \otimes_R \varphi$ is a covariant functor.*

Proof. By construction, $M \otimes_R N$ is an R-module for any R-module N; we need only establish that (1.) $\mathrm{id}_M \otimes_R \mathrm{id}_N = \mathrm{id}_{M \otimes_R N}$ for any R-module N and (2.) $\mathrm{id}_M \otimes_R (\psi \circ \varphi) = (\mathrm{id}_M \otimes_R \psi) \circ (\mathrm{id}_M \otimes_R \varphi)$ for any R-module homomorphisms $\varphi : N \to N'$ and $\psi : N' \to N''$. By Remark 2.1.91, we have that $(\mathrm{id}_M \otimes_R \mathrm{id}_N)(m \otimes_R n) = m \otimes_R n = \mathrm{id}_{M \otimes_R N}(m \otimes_R n)$; because these maps agree on the pure tensors of $M \otimes_R N$, they are equal as homomorphisms. On the other hand, for any R-module homomorphisms $\varphi : N \to N'$ and $\psi : N' \to N''$, we have that $(\mathrm{id}_M \otimes_R (\psi \circ \varphi))(m \otimes_R n) = m \otimes_R (\psi \circ \varphi(n))$ and similarly $(\mathrm{id}_M \otimes_R \psi) \circ (\mathrm{id}_M \otimes_R \varphi)(m \otimes_R n) = (\mathrm{id}_M \otimes_R \psi)(m \otimes_R \varphi(n)) = m \otimes_R (\psi \circ \varphi(n))$. □

Given a functor from the category of R-modules to itself, one naturally wonders about its behavior on short exact sequences of R-modules. By Corollary 2.1.92, for any short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ and any R-module M, we obtain an induced sequence of R-modules $M \otimes_R A \xrightarrow{\mathrm{id}_M \otimes_R \alpha} M \otimes_R B \xrightarrow{\mathrm{id}_M \otimes_R \beta} M \otimes_R C$. By hypothesis that β is surjective, for each element $c \in C$, there exists an element $b \in B$ such that $c = \beta(b)$. Consequently, for each pure tensor $m \otimes_R c$ of $M \otimes_R C$, there exists a pure tensor $m \otimes_R b$ of $M \otimes_R B$ such that $m \otimes_R c = m \otimes_R \beta(b)$. Considering that the pure tensors of $M \otimes_R C$ generate it as an R-module, we conclude that the induced map $\mathrm{id}_M \otimes_R \beta : M \otimes_R B \to M \otimes_R C$ is surjective; this proves the following.

Proposition 2.1.93. *Let M be an R-module. If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is a short exact sequence of R-modules, then the induced sequence $M \otimes_R A \xrightarrow{\mathrm{id}_M \otimes_R \alpha} M \otimes_R B \xrightarrow{\mathrm{id}_M \otimes_R \beta} M \otimes_R C \to 0$ is also exact. Consequently, the functor $M \otimes_R -$ is right-exact on the category of R-modules.*

Proposition 2.1.94. *Let R be a commutative ring. We say that an R-module L if* **flat** *if it satisfies any of the following equivalent conditions.*

(i.) *If* $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ *is a short exact sequence of R-modules, then the sequence*

$$0 \to L \otimes_R A \xrightarrow{\mathrm{id}_L \otimes_R \alpha} L \otimes_R B \xrightarrow{\mathrm{id}_L \otimes_R \beta} L \otimes_R C \to 0$$

is exact, i.e., the functor $L \otimes_R -$ *is left-exact on the category of R-modules.*

(ii.) *If* $\alpha : A \to B$ *is an injective R-module homomorphism, then the induced R-module homomorphism* $\mathrm{id}_L \otimes_R \alpha : L \otimes_R A \to L \otimes_R B$ *is injective.*

(iii.) *For any ideal I of R, the map* $\mathrm{id}_L \otimes_R i : L \otimes_R I \to L$ *that sends* $\ell \otimes_R r \mapsto r\ell$ *is injective.*

Proof. Conditions (i.) and (ii.) are equivalent by Proposition 2.1.93. Considering that the inclusion $I \subseteq R$ of an ideal I of R induces an injective R-module homomorphism, it follows that (ii.) implies (iii.). We refer the reader to [Rot09, Proposition 3.58] for the proof that (iii.) implies (i.). □

Corollary 2.1.95. *Every commutative ring R is flat as a module over itself.*

Proof. Consider an injective R-module homomorphism $\alpha : A \to B$. By Proposition 2.1.89(2.), there exist R-module isomorphisms $\varphi : A \to R \otimes_R A$ and $\psi : B \to R \otimes_R B$ defined by $\varphi(a) = 1_R \otimes_R a$ and $\psi(b) = 1_R \otimes_R b$. Observe that $\psi \circ \alpha(a) = 1_R \otimes_R \alpha(a) = (\mathrm{id}_R \otimes_R \alpha) \circ \varphi(a)$ for all elements $a \in A$, hence $\psi \circ \alpha$ and $(\mathrm{id}_R \otimes_R \alpha) \circ \varphi$ are equal as R-module homomorphisms. Considering that φ, ψ, and α are injective, $\mathrm{id}_R \otimes_R \alpha$ must be injective, from which it follows that R is a flat R-module. □

Corollary 2.1.96. *Let R be a commutative ring. A direct sum of R-modules is flat if and only if each direct summand is flat. Particularly, any free R-module is flat.*

Proof. Let $(L_i)_{i \in I}$ be a family of R-modules indexed by some (possibly infinite) set I. Consider an injective R-module homomorphism $\alpha : A \to B$. For each index $i \in I$, there exists an R-module homomorphism $\mathrm{id}_{L_i} \otimes_R \alpha : L_i \otimes_R A \to L_i \otimes_R B$; together, these induce an R-module homomorphism $\gamma : \bigoplus_{i \in I}(L_i \otimes_R A) \to \bigoplus_{i \in I}(L_i \otimes_R B)$ that acts as $\mathrm{id}_{L_i} \otimes_R \alpha$ on the ith component of the direct sum. By Proposition 2.1.89(3.), there exists R-module isomorphisms $\varphi : \bigoplus_{i \in I}(L_i \otimes_R A) \to (\bigoplus_{i \in I} L_i) \otimes_R A$ and $\psi : \bigoplus_{i \in I}(L_i \otimes_R B) \to (\bigoplus_{i \in I} L_i) \otimes_R B$. Let $S = \bigoplus_{i \in I} L_i$. Observe that $\psi \circ \gamma$ and $(\mathrm{id}_S \otimes_R \alpha) \circ \varphi$ are

equal on the pure tensors of $\bigoplus_{i\in I}(L_i \otimes_R A)$, hence they are equal as R-module homomorphisms. Consequently, $S = \bigoplus_{i\in I} L_i$ is flat if and only if $\mathrm{id}_S \otimes_R \alpha$ is injective if and only if γ is injective if and only if $\mathrm{id}_{L_i} \otimes_R \alpha$ is injective for all indices if and only if each direct summand L_i is flat.

Last, a free R-module is flat by Corollary 2.1.95, as it is a direct sum of copies of R. □

Corollary 2.1.97. *Let R be a commutative ring. Every projective R-module is flat.*

Proof. By Proposition 2.1.81(v.), a projective R-module is a direct summand of a free R-module. Every free R-module is flat; a direct summand of a flat R-module is flat by Corollary 2.1.96. □

Proposition 2.1.98. *Over a local ring, a finitely generated flat module is free.*

Proof. Let $(R,\mathfrak{m})$ be a local ring. Let L be a finitely generated flat R-module. Consider a system of generators $x_1,\ldots,x_n$ of L whose images in $L/\mathfrak{m}L$ form an $R/\mathfrak{m}$-vector space basis. By Nakayama's Lemma, we have that $L = R\langle x_1,\ldots,x_n\rangle$. Consequently, the canonical R-module homomorphism $\pi : R^n \to L$ defined by $\pi(r_1,\ldots,r_n) = r_1x_1 + \cdots + r_nx_n$ induces a short exact sequence of R-modules $0 \to K \xrightarrow{i} R^n \xrightarrow{\pi} L \to 0$, where $K = \ker\pi$ and $i : K \to R^n$ is the inclusion. By Proposition 2.1.93, there exists an exact sequence of R-modules $(R/\mathfrak{m}) \otimes_R K \to (R/\mathfrak{m}) \otimes_R R^n \to (R/\mathfrak{m}) \otimes_R L \to 0$. Combining (2.) and (4.) of Proposition 2.1.89, we obtain an exact sequence of $R/\mathfrak{m}$-vector spaces $K/(\mathfrak{m}K) \to (R/\mathfrak{m})^n \to L/(\mathfrak{m}L) \to 0$ (cf. the discussion following Definition 2.1.13). By hypothesis, the $R/\mathfrak{m}$-vector space dimension of $L/(\mathfrak{m}L)$ is n, so the Rank-Nullity Theorem implies that $K/(\mathfrak{m}K) = 0$ and $\mathfrak{m}K = K$. Corollary 2.1.17 yields $\ker\pi = K = 0$ so that L is a free R-module. □

Corollary 2.1.99. *Let $(R,\mathfrak{m})$ be a commutative unital local ring. Let M be a finitely generated R-module. The following statements are equivalent.*

(i.) *M is flat.*

(ii.) *M is projective*

(iii.) *M is free.*

Even if R is not local, a flat module over a Noetherian ring R is projective, and a finitely generated module whose localization with respect to any maximal ideal is projective must be projective.

Proposition 2.1.100. *[Rot09, Corollary 3.57] Over a Noetherian ring, a finitely generated flat module is projective. Particularly, flatness and projectivity are equivalent.*

Corollary 2.1.101. *If R is a Noetherian ring, then any finitely generated R-module M such that $M_{\mathfrak{m}}$ is projective for all maximal ideals $\mathfrak{m}$ of R is projective.*

Proof. Observe that if $M_{\mathfrak{m}}$ is projective for all maximal ideals $\mathfrak{m}$ of R, then $M_{\mathfrak{m}}$ is flat for all maximal ideals $\mathfrak{m}$ by Corollary 2.1.97. Consequently, by [Rot09, Corollary 7.18], we conclude that M is a finitely generated flat R-module so that M is projective by Proposition 2.1.100. □

Corollary 2.1.102. *Let R be a Noetherian commutative unital ring. Let M be a finitely generated R-module. The following statements are equivalent.*

(i.) *$M_{\mathfrak{m}}$ is flat for all maximal ideals $\mathfrak{m}$ of R.*

(ii.) *$M_{\mathfrak{m}}$ is projective for all maximal ideals $\mathfrak{m}$ of R.*

(iii.) *$M_{\mathfrak{m}}$ is free for all maximal ideals $\mathfrak{m}$ of R.*

If any of the above conditions hold, then M is projective.

Generally, the tensor product fails to preserve left-exactness of short exact sequences.

Example 2.1.103. Let $n \geq 2$ be an integer. Let $M = \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n. Observe that the multiplication map $\cdot n : \mathbb{Z} \to \mathbb{Z}$ is injective because $\mathbb{Z}$ is a domain; however, the induced map $(\mathbb{Z}/n\mathbb{Z}) \otimes_R \mathbb{Z} \xrightarrow{\cdot n} (\mathbb{Z}/n\mathbb{Z}) \otimes_R \mathbb{Z}$ is identically zero. Consequently, $\mathbb{Z}/n\mathbb{Z}$ is not flat as a $\mathbb{Z}$-module.

Like before, we may rigorously define the flat "defect" of an R-module M as follows. Begin with a projective resolution $L_\bullet : \cdots \xrightarrow{\ell_{n+1}} L_n \xrightarrow{\ell_n} \cdots \xrightarrow{\ell_2} L_1 \xrightarrow{\ell_1} L_0 \xrightarrow{\ell_0} N \to 0$ of some R-module N. (By Corollary 2.1.97, this is a **flat resolution** of N.) Consider the induced chain complex

$$M \otimes_R L_\bullet : \cdots \xrightarrow{\ell^*_{n+1}} M \otimes_R L_n \xrightarrow{\ell^*_n} \cdots \xrightarrow{\ell^*_2} M \otimes_R L_1 \xrightarrow{\ell^*_1} M \otimes_R L_0 \to 0$$

with chain maps defined by $\ell_i^* = \mathrm{id}_M \otimes_R \ell_i$ for each integer $i \geq 0$. We define the ith homology module $\mathrm{Tor}_i^R(M,N) = \ker \ell_i^* / \operatorname{img} \ell_{i+1}^*$ for each integer $i \geq 0$; these are independent of the choice of a projective resolution of N, hence they are well-defined (cf. [Rot09, Corollary 6.21]).

Proposition 2.1.104. *Let M be an R-module. The following properties hold.*

(1.) *We have that $\mathrm{Tor}_0^R(M,N) \cong M \otimes_R N$ for all R-modules N.*

(2.) *Every short exact sequence of R-modules $0 \to N' \to N \to N'' \to 0$ induces an exact sequence*
$$\cdots \to \mathrm{Tor}_{i+1}^R(M,N'') \to \mathrm{Tor}_i^R(M,N') \to \mathrm{Tor}_i^R(M,N) \to \mathrm{Tor}_i^R(M,N'') \to \mathrm{Tor}_{i-1}^R(M,N') \to \cdots.$$

(3.) *We have that $\mathrm{Tor}_i^R(M,N) = 0$ for all integers $i \geq 1$ and all R-modules N if and only if M is flat.*

Proof. (1.) Given any R-module N, we may consider a flat resolution $L_\bullet$ of N that ends with the terms $L_1 \xrightarrow{\ell_1} L_0 \xrightarrow{\ell_0} N \to 0$. By applying the right-exact covariant functor $M \otimes_R -$, we obtain a chain complex ending in $M \otimes_R L_1 \xrightarrow{\ell_1^*} M \otimes_R L_0 \xrightarrow{\ell_0^*} 0$ with chain maps $\ell_i^* = \mathrm{id}_M \otimes_R \ell_i$. Consequently, we find that $\ker \ell_0^* = M \otimes_R L_0$ and $\operatorname{img} \ell_1^* = \operatorname{img}(\mathrm{id}_M \otimes_R \ell_1) = M \otimes_R (\operatorname{img} \ell_1)$, where the second equality holds because the pure tensors of $M \otimes_R (\operatorname{img} \ell_1)$ generate $\operatorname{img}(\mathrm{id}_M \otimes_R \ell_1)$. Consider the short exact sequence of R-modules $0 \to \operatorname{img} \ell_1 \xrightarrow{\subseteq} L_0 \to L_0/(\operatorname{img} \ell_1) \to 0$. By Proposition 2.1.89 and 2.1.93, we obtain a sequence of R-modules $M \otimes_R (\operatorname{img} \ell_1) \to M \otimes_R L_0 \to M \otimes_R (L_0/(\operatorname{img} \ell_1)) \to 0$ that is exact in the last two places. Considering that the map on the left is the identity on both components, we conclude that $M \otimes_R (L_0/(\operatorname{img} \ell_1)) \cong (M \otimes_R L_0)/[M \otimes_R (\operatorname{img} \ell_1)]$ by the First Isomorphism Theorem. By definition, we have that $\mathrm{Tor}_0^R(M,N) = \ker \ell_0^* / \operatorname{img} \ell_1^* = (M \otimes_R L_0)/[M \otimes_R (\operatorname{img} \ell_1)]$, hence our previous computation shows that $\mathrm{Tor}_0^R(M,N) \cong M \otimes_R (L_0/(\operatorname{img} \ell_1)) \cong M \otimes_R N$, as desired.

(3.) If M is flat, then $M \otimes_R -$ is exact by Proposition 2.1.94, hence for any flat resolution $L_\bullet$ of any R-module N, the chain complex $M \otimes_R L_\bullet$ is exact. We conclude that $\mathrm{Tor}_i^R(M,N) = 0$ for all integers $i \geq 1$. Conversely, suppose that $\mathrm{Tor}_i^R(M,N) = 0$ for all integers $i \geq 1$ and all R-modules N. For any short exact sequence of R-modules $0 \to N' \to N \to N'' \to 0$, there exists a long exact sequence that begins $0 \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$. By Proposition 2.1.94, M is flat.

We omit the proof of property (2.), but we refer the reader to [Rot09, Corollary 6.30]. □

One can show that $\mathrm{Tor}_i^R(M,-)$ is a covariant functor from the category of R-modules to itself that preserves multiplication (cf. [Rot09, Theorem 6.17 and Proposition 6.18]), hence we may deduce from Proposition 2.1.104 that the R-modules $\mathrm{Tor}_i^R(M,-)$ measure the flat "defect" of M. By Proposition 2.1.89, the R-modules $M \otimes_R N$ and $N \otimes_R M$ are isomorphic for any pair of R-modules M and N, hence one can establish a similar theory for the covariant functors $\mathrm{Tor}_i^R(-,N)$. Ultimately, there is an isomorphism of functors $\mathrm{Tor}_R^i(M,-)$ and $\mathrm{Tor}_R^i(-,N)$ for all R-modules M and N, hence there is no need to make any distinction between the two (cf. [Rot09, Theorem 6.32]).

We are now able to return to our discussion of injective modules. We begin with the following.

Theorem 2.1.105 (Baer's Criterion)**.** *Let R be a commutative unital ring. Let I be a nonzero ideal of R. An R-module Q is injective if and only if for every R-module homomorphism $\varphi : I \to Q$, there exists an R-module homomorphism $\widetilde{\varphi} : R \to Q$ such that $\widetilde{\varphi}(i) = \varphi(i)$ for each element $i \in I$.*

Corollary 2.1.106. *Let $\mathbb{Z}$ be the abelian group of integers. Let $\mathbb{Q}$ be the abelian group of rational numbers. The quotient group $\mathbb{Q}/\mathbb{Z}$ is injective as a $\mathbb{Z}$-module.*

Proof. By Baer's Criterion, it suffices to show that any $\mathbb{Z}$-module homomorphism $\varphi : n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ lifts to a $\mathbb{Z}$-module homomorphism $\widetilde{\varphi} : \mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ such that $\widetilde{\varphi}(na) = \varphi(na)$ for any $a \in \mathbb{Z}$. Consider the map $\widetilde{\varphi} : \mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ defined by $\widetilde{\varphi}(a) = \dfrac{a}{n}\varphi(n)$. By hypothesis that φ is a $\mathbb{Z}$-module homomorphism, it follows that $\widetilde{\varphi}$ is a $\mathbb{Z}$-module homomorphism such that $\widetilde{\varphi}(na) = \dfrac{na}{n}\varphi(n) = \varphi(na)$. $\square$

We prove next that every R-module can be identified with an R-submodule of an injective R-module; this analogizes the fact that any R-module is the homomorphic image of a free R-module.

Lemma 2.1.107. *Every $\mathbb{Z}$-module embeds in an injective $\mathbb{Z}$-module. Explicitly, for every $\mathbb{Z}$-module M, there exists an injective $\mathbb{Z}$-module Q and an injective $\mathbb{Z}$-module homomorphism $\varphi : M \to Q$.*

Proof. Given any $\mathbb{Z}$-module M, consider its character group $M^* = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. We may subsequently define the character group $M^{**} = \mathrm{Hom}_{\mathbb{Z}}(M^*, \mathbb{Q}/\mathbb{Z})$ of M^* that consists of all $\mathbb{Z}$-module homomorphisms that send a $\mathbb{Z}$-module homomorphism $\varphi : M \to \mathbb{Q}/\mathbb{Z}$ to an element of $\mathbb{Q}/\mathbb{Z}$.

Consequently, we may define a map $\mathrm{ev} : M \to M^{**}$ satisfying $\mathrm{ev}(m)(\varphi) = \varphi(m)$. Observe that $\mathrm{ev}(am+m')(\varphi) = \varphi(am+m') = \varphi(am)+\varphi(m') = a\varphi(m)+\varphi(m') = a\,\mathrm{ev}(m)(\varphi)+\mathrm{ev}(m')(\varphi)$ for any integer a, any elements $m, m' \in M$, and any $\mathbb{Z}$-module homomorphism $\varphi : M \to \mathbb{Q}/\mathbb{Z}$, hence ev is a $\mathbb{Z}$-module homomorphism. One can verify that $\mathrm{ev}(m)(a\varphi+\psi) = a\,\mathrm{ev}(m)(\varphi)+\mathrm{ev}(m)(\psi)$ for any integer a and $\mathbb{Z}$-module homomorphisms $\varphi : M \to \mathbb{Q}/\mathbb{Z}$ and $\psi : M \to \mathbb{Q}/\mathbb{Z}$, hence ev is well-defined. Last, we claim that ev is injective. By the contrapositive, it suffices to show that every nonzero element $m \in M$ induces a $\mathbb{Z}$-linear homomorphism $\widetilde{\varphi} : M \to \mathbb{Q}/\mathbb{Z}$ for which $\widetilde{\varphi}(m)$ is nonzero. By hypothesis that $m \in M$ is nonzero, the $\mathbb{Z}$-module $C = \mathbb{Z}\langle m\rangle$ is nonzero. If $nm = 0$ for some integer $n \geq 2$, then the assignment $m \mapsto \dfrac{1}{n}+\mathbb{Q}/\mathbb{Z}$ induces a well-defined $\mathbb{Z}$-linear homomorphism $\varphi : C \to \mathbb{Q}/\mathbb{Z}$ defined by $\varphi(am) = \dfrac{a}{n}+\mathbb{Q}/\mathbb{Z}$. Otherwise, the assignment $m \mapsto \dfrac{1}{2}+\mathbb{Q}/\mathbb{Z}$ induces a well-defined $\mathbb{Z}$-linear homomorphism $\varphi : C \to \mathbb{Q}/\mathbb{Z}$ defined by $\varphi(am) = \dfrac{a}{2}+\mathbb{Q}/\mathbb{Z}$. Either way, by the injectivity of $\mathbb{Q}/\mathbb{Z}$ as a $\mathbb{Z}$-module, the inclusion homomorphism $i : C \to M$ can be extended to a $\mathbb{Z}$-linear map $\widetilde{\varphi} : M \to \mathbb{Q}/\mathbb{Z}$ such that $\varphi = \widetilde{\varphi} \circ i$ and $\widetilde{\varphi}(m) = \varphi(m)$ is nonzero.

Considering that M^* is a $\mathbb{Z}$-module, there exists a free $\mathbb{Z}$-module F and a surjective $\mathbb{Z}$-module homomorphism $\pi : F \to M$, i.e., there exists an exact sequence of $\mathbb{Z}$-modules $F \xrightarrow{\pi} M^* \to 0$. By Proposition 2.1.84, $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ induces an exact sequence of $\mathbb{Z}$-modules $0 \to M^{**} \xrightarrow{\pi^*} F^*$. Observe that if $F = \bigoplus_{\varphi \in M^*} \mathbb{Z}$, then $F^* = \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{\varphi \in M^*} \mathbb{Z}, \mathbb{Q}/\mathbb{Z}\right) \cong \prod_{\varphi \in M^*} (\mathbb{Q}/\mathbb{Z})$. Ultimately, $\pi^* \circ \mathrm{ev} : M \to F^*$ is an injective $\mathbb{Z}$-module homomorphism, so our proof is complete in view of the fact that F^* is an injective $\mathbb{Z}$-module by Corollary 2.1.106 and [Rot09, Proposition 3.28(i)]. □

Lemma 2.1.108. *Let R be a commutative ring. If P is a projective R-module and Q is an injective $\mathbb{Z}$-module, then $P^Q = \mathrm{Hom}_{\mathbb{Z}}(P, Q)$ is an injective R-module.*

Proof. We may define an R-module action on P^Q via $(r \cdot \varphi)(x) = \varphi(rx)$ because the identity

$$[(r+s)\cdot\varphi](x) = \varphi((r+s)x) = \varphi(rx+sx) = \varphi(rx)+\varphi(sx) = (r\cdot\varphi + s\cdot\varphi)(x)$$

holds for all elements $r, s \in R$ and $x \in P$, as φ is a group homomorphism. By Proposition 2.1.84, it suffices to show that $\mathrm{Hom}_R(-, P^Q)$ is right-exact on the category of R-modules. Given any short

exact sequence of R-modules $0 \to A \to B \to C \to 0$, we obtain an exact sequence of R-modules

$$0 \to A \otimes_R P \to B \otimes_R P \to C \otimes_R P \to 0$$

by Propositions 2.1.89(1.) and 2.1.97. By applying Proposition 2.1.84, we find that

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(C \otimes_R P, Q) \to \mathrm{Hom}_{\mathbb{Z}}(B \otimes_R P, Q) \to \mathrm{Hom}_{\mathbb{Z}}(A \otimes_R P, Q) \to 0$$

is a short exact sequence of $\mathbb{Z}$-modules. Last, the Tensor-Hom Adjunction yields a short exact sequence $0 \to \mathrm{Hom}_R(C, P^Q) \to \mathrm{Hom}_R(B, P^Q) \to \mathrm{Hom}_R(A, P^Q) \to 0$ of R-modules, as desired. □

Proposition 2.1.109. *Every R-module embeds into an injective R-module.*

Proof. Let M be an R-module. By definition, $(M, +)$ is an abelian group, hence it is a $\mathbb{Z}$-module. By Lemma 2.1.107, there exists an injective $\mathbb{Z}$-module Q and an injective $\mathbb{Z}$-module homomorphism $\varphi : M \to Q$. By Proposition 2.1.80, this induces an injective $\mathbb{Z}$-module homomorphism $\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) : \mathrm{Hom}_{\mathbb{Z}}(R, M) \to \mathrm{Hom}_{\mathbb{Z}}(R, Q)$. Crucially, $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective R-module by Lemma 2.1.108, hence it suffices to find an injective R-module homomorphism $M \to \mathrm{Hom}_{\mathbb{Z}}(R, Q)$.

Consider the map $\mu : M \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$ defined by $\mu(m)(r) = rm$ for all elements $r \in R$. Observe that $\mu(m+m')(r) = r(m+m') = rm + rm' = (\mu(m) + \mu(m'))(r)$ for all elements $r \in R$ and any elements $m, m' \in M$. We conclude that μ is a $\mathbb{Z}$-module homomorphism. Even more, if $\mu(m)$ is the zero homomorphism, then $m = 1_R m = \mu(m)(1_R) = 0$, hence μ is injective. Consequently, the map $\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu : M \to \mathrm{Hom}_{\mathbb{Z}}(R, Q)$ is an injective $\mathbb{Z}$-module homomorphism.

Given any element $r \in R$, observe that $(\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(rm) = \varphi \circ \mu(rm)$ is the $\mathbb{Z}$-module homomorphism that sends an element $s \in R$ to the element $\varphi(rsm)$ of Q. Likewise, the composite map $(\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(m)$ is the $\mathbb{Z}$-module homomorphism that sends an element $s \in R$ to the element $\varphi(sm)$ of Q. By the R-module structure of $\mathrm{Hom}_{\mathbb{Z}}(R, Q)$ defined in Lemma 2.1.108, it follows that $r[(\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(m)]$ and $(\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu)(rm)$ are identical on R, hence they are equal. We conclude that $\mathrm{Hom}_{\mathbb{Z}}(R, \varphi) \circ \mu$ is an R-module homomorphism. □

Ultimately, Proposition 2.1.109 implies that every R-module N admits an **injective resolution**, i.e., a (right) resolution $Q^\bullet : 0 \to N \to Q^0 \xrightarrow{q^0} Q^1 \xrightarrow{q^1} \cdots \xrightarrow{q^n} Q^{n+1} \xrightarrow{q^{n+1}} \cdots$ in which Q^i is injective for each integer $i \geq 0$. Given an R-module M, consider the cochain complex

$$\operatorname{Hom}_R(M, Q^\bullet) : 0 \to \operatorname{Hom}_R(M, Q^0) \xrightarrow{q^0_*} \operatorname{Hom}_R(M, Q^1) \xrightarrow{q^1_*} \cdots \xrightarrow{q^n_*} \operatorname{Hom}_R(M, Q^n) \xrightarrow{q^{n+1}_*} \cdots$$

with cochain maps defined by $q^i_* = \operatorname{Hom}_R(M, q^i)$ for each integer $i \geq 0$. We define the ith cohomology module $\operatorname{Ext}^i_R(M,N) = \ker q^i_* / \operatorname{img} q^{i-1}_*$ for each integer $i \geq 0$. Like before, $\operatorname{Ext}^i_R(M,N)$ is independent of the choice of an injective resolution of N (cf. [Rot09, Proposition 6.40]).

Proposition 2.1.110. *Let M be an R-module. The following properties hold.*

(1.) *We have that* $\operatorname{Ext}^0_R(M,N) \cong \operatorname{Hom}_R(M,N)$ *for all R-modules N.*

(2.) *Every short exact sequence of R-modules* $0 \to N' \to N \to N'' \to 0$ *induces an exact sequence* $\cdots \to \operatorname{Ext}^{i-1}_R(M,N'') \to \operatorname{Ext}^i_R(M,N') \to \operatorname{Ext}^i_R(M,N) \to \operatorname{Ext}^i_R(M,N'') \to \operatorname{Ext}^{i+1}_R(M,N') \to \cdots$.

(3.) *We have that* $\operatorname{Ext}^i_R(M,N) = 0$ *for all* $i \geq 1$ *and all R-modules N if and only if M is projective.*

Proof. We omit the proof, as it is analogous to the proof of Proposition 2.1.110. □

One can show that $\operatorname{Ext}^i_R(M,-)$ is a covariant functor from the category of R-modules to itself that preserves multiplication (cf. [Rot09, Theorem 6.37 and Proposition 6.38]), hence we may deduce from Proposition 2.1.110 that the functors $\operatorname{Ext}^i_R(M,-)$ measure the projective "defect" of M. Later, in our discussion of canonical modules, we will need the following proposition.

Proposition 2.1.111. *[Rot09, Proposition 7.24] Let R be a commutative ring with R-modules A and C. If* $\operatorname{Ext}^1_R(C,A) = 0$, *then every short exact sequence* $0 \to A \to B \to C \to 0$ *splits.*

Proof. Consider a short exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$. By applying $\operatorname{Hom}_R(C,-)$, we obtain a long exact sequence of Ext in which the terms $\operatorname{Hom}_R(C,B) \xrightarrow{\gamma} \operatorname{Hom}_R(C,C) \xrightarrow{\alpha^*} \operatorname{Ext}^1_R(C,A)$ appear. By hypothesis that $\operatorname{Ext}^1_R(C,A) = 0$, we find that $\operatorname{Hom}_R(C,C) = \ker \alpha^* = \operatorname{img} \gamma$, hence γ is surjective.

Particularly, there exists an R-module homomorphism $\beta' : C \to B$ such that $\mathrm{id}_C = \beta \circ \beta'$. By the Splitting Lemma, we conclude that the short exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ splits. □

If an R-module M admits an injective resolution with finitely many nonzero injective modules, then its **injective dimension** is the minimum length of all of such resolutions, i.e.,

$$\mathrm{injdim}_R(M) = \inf\{n \mid Q^\bullet : 0 \to M \to Q^0 \to Q^1 \to \cdots \to Q^n \to 0 \text{ is an injective resolution of } M\}.$$

Otherwise, we say that M does not have finite injective dimension. Our next proposition describes the injective dimension of a module in terms of Ext. Before this, we need the following lemma.

Lemma 2.1.112. *Let R be a commutative ring. Let A be an R-module. Let M be an R-module with an injective resolution $Q^\bullet : 0 \to M \xrightarrow{q^{-1}} Q^0 \xrightarrow{q^0} Q^1 \xrightarrow{q^1} \cdots$. Let $I_i = \mathrm{img}\, q^i$ for each integer $i \geq -1$. For all integers $n \geq i+2$, there exist R-modules isomorphisms $\mathrm{Ext}^{n-i}_R(A, I_i) \cong \mathrm{Ext}^{n-i-1}_R(A, I_{i+1})$.*

Proof. We will illustrate that $\mathrm{Ext}^{n+1}_R(A,M) \cong \mathrm{Ext}^n_R(A, I_0)$; the remaining isomorphisms follow similarly. By hypothesis that $Q^\bullet$ is an injective resolution of M, we may obtain an injective resolution of $I_0 = \mathrm{img}\, q^0$ by taking $Q^\bullet_0 : 0 \to I_0 \xrightarrow{i} Q^1 \xrightarrow{q^1} Q^2 \xrightarrow{q^2} \cdots$; indeed, it suffices to note that $\ker q^1 = \mathrm{img}\, q^0 = I^0 = \mathrm{img}\, i$ by construction, and the rest of the resolution is exact by assumption. Consequently, if we relabel the injective modules Q^i as X^{i-1} and the maps q^i as χ^{i-1}, we find that

$$\mathrm{Ext}^{n+1}_R(A,M) = \frac{\ker q^n_*}{\mathrm{img}\, q^{n+1}_*} = \frac{\ker \chi^{n-1}_*}{\mathrm{img}\, \chi^n_*} = \mathrm{Ext}^n_R(A, I_0).$$

Because Ext is independent of the choice of injective resolution, the isomorphism holds. □

Proposition 2.1.113. *Let R be a commutative ring. The following are equivalent.*

(i.) *The R-module M has* $\mathrm{injdim}_R(M) \leq n$.

(ii.) *The R-module M satisfies* $\mathrm{Ext}^{n+1}_R(A,M) = 0$ *for all R-modules A.*

Proof. If M is an R-module of injective dimension no larger than n, then there exists an injective resolution $Q^\bullet : 0 \to M \to Q^0 \to Q^1 \to \cdots \to Q^n \to 0$. By Lemma 2.1.112, for every R-module A,

we have that $\operatorname{Ext}_R^{n+1}(A,M) \cong \operatorname{Ext}_R^1(A,Q^n)$. But Q^n is injective, hence the latter Ext vanishes by Proposition 2.1.87. Conversely, suppose that $\operatorname{Ext}_R^{n+1}(A,M) = 0$ for all R-modules A. Consider an injective resolution $Q^\bullet$ of M. By Lemma 2.1.112, we have that $\operatorname{Ext}_R^{n+1}(A,M) \cong \operatorname{Ext}_R^1(A,I_n)$, hence by assumption, we conclude that I_n is an injective R-module. Consequently, we obtain a finite injective resolution of M of length n by truncating the injective resolution $Q^\bullet$ at I_n. □

Corollary 2.1.114. *Let R be a commutative unital ring. Let M be an R-module. For any positive integer k, we have that* $\operatorname{injdim}_R(M^{\oplus n}) \leq n$ *if and only if* $\operatorname{injdim}_R(M) \leq n$.

Using the tools introduced in the next section, we will determine a pleasant formula the injective dimension of a module of finite injective dimension. Until then, we note the following.

Proposition 2.1.115. *[BH93, Proposition 3.1.14] Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Let M be a finitely generated R-module. We have that*

$$\operatorname{injdim}_R(M) = \sup\{i \geq 0 \mid \operatorname{Ext}_R^i(k,M) \neq 0\}.$$

One can likewise define the **projective dimension** of an R-module M as

$$\operatorname{projdim}_R(M) = \inf\{n \mid P_\bullet : \cdots \to P_n \to \cdots \to P_1 \to P_0 \to M \to 0 \text{ is a projective resolution of } M\}.$$

Like with injective dimension, the projective dimension of a module can be checked by the vanishing of Tor. We state two facts that are analogous to Lemma 2.1.112 and Proposition 2.1.113; we omit the proofs, as they are almost identical to the proofs of the aforementioned results.

Lemma 2.1.116. *Let R be a commutative ring. Let M be an R-module. Let B be an R-module with an projective resolution $P_\bullet : \cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \xrightarrow{p_0} B \xrightarrow{p_{-1}} 0$. Let $K_i = \ker p_i$ for each integer $i \geq -1$. For all integers $n \geq i+2$, there exist R-modules isomorphisms* $\operatorname{Tor}_{n-i}^R(M,K_i) \cong \operatorname{Tor}_{n-i-1}^R(M,K_{i+1})$.

Proposition 2.1.117. *Let R be a commutative ring. The following are equivalent.*

(i.) *The R-module M has* $\operatorname{projdim}_R(M) \leq n$.

(ii.) *The R-module M satisfies* $\operatorname{Tor}_{n+1}^R(M,B) = 0$ *for all R-modules B.*

Corollary 2.1.118. *If* $0 \to A \to B \to C \to 0$ *is a short exact sequence of R-modules such that two modules have finite projective dimension, then the third module has finite projective dimension.*

Proof. We will prove that if A and B have finite projective dimension, then C has finite projective dimension; the other two cases follow similarly. By Proposition 2.1.117, if $\operatorname{projdim}_R(A) = m$ and $\operatorname{projdim}_R(B) = n$, then for all R-modules M, we have that $\operatorname{Tor}_i^R(A,M) = 0$ for all integers $i \geq m+1$ and $\operatorname{Tor}_j^R(B,M) = 0$ for all integers $j \geq n+1$. Consequently, for all R-modules M and all integers $k \geq \max\{m,n\}+1$, we have that $\operatorname{Tor}_k^R(C,M) = 0$ by Proposition 2.1.104. □

One of the most important results concerning projective dimension is the following.

Theorem 2.1.119 (Auslander-Buchsbaum Formula)**.** *[AB57, Theorem 3.7] Let* $(R,\mathfrak{m})$ *be a Noetherian local ring. If M is a finitely generated R-module with finite projective dimension, then*

$$\operatorname{projdim}_R(M) + \operatorname{depth}(M) = \operatorname{depth}(R).$$

Proposition 2.1.120. *For any (possibly infinite) index set I and any family of R-modules* $(M_i)_{i\in I}$ *of finite projective dimension,* $\bigoplus_{i\in I} M_i$ *has finite projective dimension.*

Proof. For each index $i \in I$, there exists a finite projective resolution $P_\bullet^i$ of M_i. □

2.1.5 Graded Rings and Modules

We say that a ring R is **graded** if there exist abelian groups $(R_i,+)$ indexed by some monoid M such that $R = \bigoplus_i R_i$ as an abelian group and $R_iR_j \subseteq R_{i+j}$. We refer to the abelian group R_i as the ith **graded piece** of R; the elements of R_i are called **homogeneous** of **degree** i. Graded rings generalize polynomial rings: indeed, the homogeneous elements of a polynomial ring are the homogeneous polynomials, and the degree of an element of a polynomial ring is the usual degree of a polynomial, i.e., the maximum of the sum of the exponents of its nonzero monomial summands. If R and S are

graded rings with respect to the same monoid M, then a ring homomorphism $\varphi : R \to S$ is **graded** if the image of the ith graded piece of R lies in the ith graded piece of S, i.e., $\varphi(R_i) \subseteq S_i$.

Often, we will emphasize the underlying monoid with respect to which a ring is graded. Given any field k, the polynomial ring $k[x_1,\ldots,x_n]$ is graded with respect to the non-negative integers $\mathbb{Z}_{\geq 0}$. On the other hand, the ring of Laurent polynomials $k[x_1,\ldots,x_n,x_1^{-1},\ldots,x_n^{-1}]$ is graded with respect to the integers $\mathbb{Z}$, as there exist polynomials of arbitrarily large negative degree.

Observe that if R is graded with respect to a monoid M and $\varphi : M \to N$ is a monoid homomorphism, then R is graded with respect to N by the abelian groups $(R_n,+)$ such that $\varphi(m) = n$. We define the dth **Veronese** subring of $k[x_1,\ldots,x_n]$ for any integer $d \geq 1$ as the $d\mathbb{Z}_{\geq 0}$-graded ring

$$k[x_1,\ldots,x_n]^{(d)} = \bigoplus_{i\geq 0} k[x_1,\ldots,x_n]_{di} = \bigoplus_{i\geq 0} k\langle x_1^{a_1}\cdots x_n^{a_n} \mid a_1+\cdots+a_n = di\rangle.$$

We discuss this further in the chapter On a Generalization of Two-Dimensional Veronese Subrings.

Unless otherwise stated, we assume throughout this section that R is a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring; however, we emphasize that many of the forthcoming details hold for (commutative) rings graded over any (commutative) cancellative torsion-free monoid. By definition of a direct sum, every element of r can be written uniquely as a finite sum $r = r_0 + \cdots + r_n$ of homogeneous elements; we refer to the summands $r_i \in R_i$ as the **homogeneous components** of r. Even more, the collection $R_+ = \bigoplus_{i\geq 1} R_i$ of positively graded elements of R forms the **irrelevant ideal** of R. We say that an ideal I is **homogeneous** if the homogeneous components of any element of I lie in I.

Our next two propositions on $\mathbb{Z}_{\geq 0}$-graded rings distinguish the 0th graded piece of R.

Proposition 2.1.121. *If R is a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring, then R_0 is a subring of R. Particularly, the additive identity 0_R and multiplicative identity 1_R of R lie in R_0.*

Proof. By definition of a graded ring, $(R_0,+)$ is an abelian group, hence R_0 possesses an additive identity element e. Observe that $e = e+e$ in R_0; cancellation in R yields $e = 0_R$. Even more, R_0 is closed under subtraction and $R_0R_0 \subseteq R_0$. We conclude that R_0 is a subring by the Subring Test.

We will establish now that $1_R \in R_0$. We may write $1_R = r_0 + \cdots + r_n$ for some homogeneous

elements $r_i \in R_i$. By definition of 1_R, we have that $r_i = 1_R \cdot r_i = r_0 r_i + \cdots + r_n r_i$ for each integer $1 \leq i \leq n$. We note that $r_j r_i \in R_{i+j}$ for each integer $0 \leq j \leq n$. Comparing degrees of the expressions on the left- and right-hand sides of the equation $r_i = r_0 r_i + \cdots + r_n r_i$ and using the uniqueness of the homogeneous components of an element of R, we find that that $r_i = r_i r_0$ for each integer $1 \leq i \leq n$. Ultimately, we conclude that $1_R = r_0 + \cdots + r_n = (r_0 + \cdots + r_n) r_0 = 1_R \cdot r_0 = r_0$. □

Proposition 2.1.122. *If R is a $\mathbb{Z}_{\geq 0}$-graded integral domain, then every unit of R lies in R_0.*

Proof. By definition, if u is a unit of R, then $uv = 1_R$ for some nonzero element $v \in R$. We may write $u = u_0 + \cdots + u_m$ and $v = v_0 + \cdots + v_n$ so that $1_R = \sum_{i,j} u_i v_j$. By Proposition 2.1.121, the multiplicative identity 1_R is homogeneous of degree zero, hence every element $u_i v_j$ of degree $i + j \geq 1$ must be 0_R. By assumption that R is an integral domain, we must have that $u_i = 0_R$ or $v_j = 0_R$ for each pair of integers such that $i + j \geq 1$. We will denote by k and ℓ the largest integers such that $u_k \neq 0_R$ and $v_\ell \neq 0_R$. Once again, by hypothesis that R is an integral domain, it follows that $u_k v_\ell \neq 0_R$ so that $u_k v_\ell = 1_R$. Comparing degrees, we find that $k = \ell = 0$ and $u = u_0 \in R_0$. □

Unless R is an integral domain, the previous proposition does not determine the units of R. We will soon provide a necessary and sufficient condition on the units of a $\mathbb{Z}_{\geq 0}$-graded ring. Before this, we discuss the properties of the quotient of a graded ring by a homogeneous ideal.

Proposition 2.1.123. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. If I is a homogeneous ideal of R, then the quotient ring R/I is $\mathbb{Z}_{\geq 0}$-graded with respect to the abelian groups $(R_i + I)/I$.*

Proof. Every element of R can be written uniquely as $r = r_0 + \cdots + r_n$ for some homogeneous elements $r_i \in R_i$, hence every element of R/I can be written as $r + I = (r_0 + I) + \cdots + (r_n + I)$. Observe that if $r + I = (r_0' + I) + \cdots + (r_n' + I)$ for some homogeneous elements $r_i' \in R_i$, then there exists some element $x \in I$ such that $r_0 + \cdots + r_n = r_0' + \cdots + r_n' + x$ and $x = (r_0 - r_0') + \cdots + (r_n - r_n')$. By assumption that I is a homogeneous ideal, each of the homogeneous elements $r_i - r_i'$ belongs to I so that $r_i + I = r_i' + I$ for each integer $0 \leq i \leq n$. Consequently, every element of R/I can be written uniquely as a sum of elements of $(R_i + I)/I$. Even more, it is straightforward to verify that the product of the abelian groups $(R_i + I)/I$ and $(R_j + I)/I$ lies in $(R_{i+j} + I)/I$. □

Consequently, homogeneous ideals are precisely the kernels of graded ring homomorphisms.

Proposition 2.1.124. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. Every homogeneous ideal of R is equal to the kernel of some graded ring homomorphism from R to a $\mathbb{Z}_{\geq 0}$-graded ring S.*

Proof. We will first establish that the kernel of a graded ring homomorphism $\varphi : R \to S$ to a $\mathbb{Z}_{\geq 0}$-graded ring S is homogeneous. We may write every element of $\ker \varphi$ as $r = r_0 + \cdots + r_n$ for some homogeneous elements $r_i \in R_i$. By assumption that φ is a graded ring homomorphism, it follows that $0_S = \varphi(r) = \varphi(r_0) + \cdots + \varphi(r_n)$ with $\varphi(r_i) \in S_i$ for each integer $0 \leq i \leq n$. Consequently, we find that $\varphi(r_i) = 0_S$ for each integer $0 \leq i \leq n$, hence $\ker \varphi$ is homogeneous.

Conversely, if I is a homogeneous ideal of R, then R/I is a $\mathbb{Z}_{\geq 0}$-graded ring with respect to the abelian groups $(R_i + I)/I$; thus, the natural surjection $R \to R/I$ is graded with kernel I. □

Prime ideals of a graded ring need not be homogeneous; however, the homogeneous ideal generated by the homogeneous elements of a prime ideal is also a prime ideal.

Proposition 2.1.125. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. Let P be a prime ideal of R. The ideal P_H generated by the homogeneous elements of P is prime. Particularly, the quotient ring R/P_H is a $\mathbb{Z}_{\geq 0}$-graded integral domain with respect to the abelian groups $(R_i + P_H)/P_H$.*

Proof. Consider any elements $r, s \in R$ such that $rs \in P_H$. Observe that P_H is a homogeneous ideal by construction, hence the homogeneous components of r and s belong to P_H. Explicitly, if we write $r = r_0 + \cdots + r_m$ and $s = s_0 + \cdots + s_n$ for some homogeneous elements $r_i \in R_i$ and $s_j \in R_j$, then for every pair of integers $0 \leq i \leq m$ and $0 \leq j \leq n$, we have that $r_i s_j \in P_H$. Considering that P_H is contained in the prime ideal P, we have that $r_i s_j \in P$ so that either $r_i \in P$ or $s_j \in P$ for every pair of integers $0 \leq i \leq m$ and $0 \leq j \leq n$. By definition, the ideal P_H contains the homogeneous elements of P, hence either $r_i \in P_H$ or $s_j \in P_H$ for every pair of integers $0 \leq i \leq m$ and $0 \leq j \leq n$. On the contrary, if neither $r \in P_H$ nor $s \in P_H$, then the integers $k = \max\{i \mid r_i \notin P_H\}$ and $\ell = \max\{j \mid s_j \notin P_H\}$ are well-defined. Observe that the homogeneous component of rs of degree $k + \ell$ is given by $\sum_{i,j} r_i s_j$ such that $k + \ell = i + j$; it lies in P_H. Each of the products $r_i s_j$ with $i > k$ or $j > \ell$ belongs to P_H by

definition of k and ℓ, hence $r_k s_\ell$ belongs to P_H, as well. But this implies that $r_k s_\ell$ belongs to P so that either $r_k \in P$ or $s_\ell \in P$ and either $r_k \in P_H$ or $s_\ell \in P_H$ — a contradiction. □

We return to provide a necessary and sufficient condition on the units of R, as promised.

Proposition 2.1.126. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring.*

(1.) *Let $r = r_0 + \cdots + r_n$ be the unique expression of an element $r \in R$ in terms of its homogeneous components $r_i \in R_i$. We have that r is a unit if and only if r_0 is a unit and $r_1, \ldots, r_n$ are nilpotent.*

(2.) *If R is reduced and* $\mathrm{Spec}(R)$ *is connected, then every unit of R is homogeneous.*

Proof. (1.) By the Multinomial Theorem, the sum of a unit and some nilpotent elements is a unit. Conversely, suppose that $r = r_0 + \cdots + r_n$ is a unit of R. By definition, there exists a nonzero element $s = s_0 + \cdots + s_m$ of R such that $rs = 1_R$. Comparing degrees of the homogeneous summands on the left- and right-hand sides of this equation, we conclude that $1_R = rs = r_0 s_0$ so that r_0 is a unit. We claim that r_i is nilpotent for each integer $1 \leq i \leq n$. By Proposition 2.1.52, the collection of nilpotent elements of R is equal to the intersection of the minimal prime ideals of R, so it suffices to prove that r_i is contained in every minimal prime ideal of R for each integer $1 \leq i \leq n$. Considering that r_i is homogeneous for each integer $1 \leq i \leq n$, it follows that r_i belongs to a minimal prime ideal P of R if and only if r_i belongs to the ideal P_H generated by the homogeneous elements of P. By Proposition 2.1.125, for every minimal prime ideal P of R, the homogeneous ideal P_H is prime, hence R/P_H is a $\mathbb{Z}_{\geq 0}$-graded integral domain by the same proposition. By assumption that r is a unit, it follows that $r + P_H$ is a unit. By Proposition 2.1.122, we conclude that $r + P_H$ lies in $(R_0 + P_H)/P_H$, from which it follows that $r_i + P_H = 0_R + P_H$ and $r_i \in P_H$ for each integer $1 \leq i \leq n$.

(b.) On the contrary, suppose that R admits a unit u with (at least two) nonzero homogeneous components $u_0, \ldots, u_n$. Consider the open set $D(u_i)$ of prime ideals of R that do not contain u_i. By Proposition 2.1.52, it follows that $D(u_i)$ is empty if and only if u_i is nilpotent, hence by assumption that R is reduced and u_i is nonzero, we conclude that $D(u_i)$ is nonempty. By hypothesis that u is a unit of R, it is not contained in any prime ideal of R, hence every prime ideal of R must

not contain u_i for some integer $0 \leq i \leq n$. Consequently, we have that $\mathrm{Spec}(R) = \bigcup_{i=0}^{n} D(u_i)$. By assumption that $\mathrm{Spec}(R)$ is connected, for every pair of integers $0 \leq i < j \leq n$, we must have that $D(u_i) \cap D(u_j)$ is nonempty, hence there exists a prime ideal P of R that contains neither u_i nor u_j. By Proposition 2.1.125, the homogeneous ideal P_H generated by the homogeneous elements of P is prime; it contains neither u_i nor u_j, so it cannot contain u. Consequently, the nonzero element $u + P_H$ is a unit of the $\mathbb{Z}_{\geq 0}$-graded integral domain R/P_H and must therefore lie in $(R_0 + P_H)/P_H$ by Proposition 2.1.122. But this implies that $u_1, \ldots, u_n$ belong to P_H — a contradiction. □

We continue to explore the similarities between graded rings and polynomial rings.

Proposition 2.1.127. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. Some homogeneous elements of positive degree generate R as an R_0-algebra if and only if they generate the ideal R_+.*

Proof. Let $r_1, \ldots, r_n$ be homogeneous elements such that $r_j \in R_{i_j}$ and $i_j \geq 1$. If $r_1, \ldots, r_n$ generate R as an R_0-algebra, then every element of R_+ can be written as a polynomial in the elements $r_1, \ldots, r_n$ with coefficients in R_0, hence we have that $R_+ \subseteq (r_1, \ldots, r_n)$; the other containment is clear.

We will assume now that $R_+ = (r_1, \ldots, r_n)$. We claim that every element of R can be written as a polynomial in the elements $r_1, \ldots, r_n$ with coefficients in R_0. Considering that every element of R can be expressed uniquely as a sum of homogeneous elements, it suffices to prove this claim for the homogeneous elements of R. We proceed by induction on the degree d of a homogeneous element s_d. If $d = 0$, then s_d is a constant polynomial in $r_1, \ldots, r_n$ with coefficients in R_0, so we may assume that $d \geq 1$. By hypothesis that $R_+ = (r_1, \ldots, r_n)$, there exist elements $a_1, \ldots, a_d \in R$ such that $s_d = a_1 r_1 + \cdots + a_n r_n$. Comparing degrees on both sides of this equation, we may write $s_d = b_1 r_1 + \cdots b_n r_n$ for some homogeneous elements $b_1, \ldots, b_n$ with $b_j \in R_{d-i_j}$. By induction, the elements $b_1, \ldots, b_n$ are polynomials in the elements $r_1, \ldots, r_n$ with coefficients in R_0. We conclude that s_d is a polynomial in the elements $r_1, \ldots, r_n$ with coefficients in R_0. □

Proposition 2.1.128. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. The following conditions are equivalent.*

(i.) *R is Noetherian.*

(ii.) *R_0 is Noetherian and R is finitely generated as an R_0-algebra.*

Proof. We will assume first that R_0 is Noetherian and that R is finitely generated as an R_0-algebra. Every element of a finite generating set for R as an R_0-algebra can be expressed uniquely as the sum of homogeneous elements of R, hence we may replace each generator by its homogeneous components to obtain a system of homogeneous generators $r_1, \ldots, r_n$ for R as an R_0-algebra. Consequently, the graded ring homomorphism $R_0[x_1, \ldots, x_n] \to R$ induced by the assignment $x_i \mapsto r_i$ is surjective. By hypothesis that R_0 is Noetherian, it follows that $R_0[x_1, \ldots, x_n]$ is Noetherian by Hilbert's Basis Theorem, hence we conclude that R is Noetherian.

Conversely, if R is Noetherian, then the ideal $R_+ = \bigoplus_{i \geq 1} R_i$ is finitely generated. By the previous paragraph, we may assume that the generators of R_+ are homogeneous, hence they generate R as an R_0-algebra by Proposition 2.1.127. Last, we note that $R_0 \cong R/R_+$ is Noetherian. □

We say that a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring R is **standard graded** if R is generated as an R_0-algebra by the homogeneous elements of degree one, i.e., $R = R_0[R_1]$. For instance, any polynomial ring $S[x_1, \ldots, x_n]$ is standard graded: the S-algebra generators are the monomials $x_1, \ldots, x_n$. Even more, if R is standard graded, R_0 is a field, and R is finitely generated as an R_0-algebra, then R is Noetherian and the ideal R_+ is maximal by Proposition 2.1.128 and its proof. We show that there is in fact no other homogeneous maximal ideal of R whenever R_0 is a field.

Proposition 2.1.129. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. If R_0 is a field, then the unique homogeneous maximal ideal of R is $R_+ = \bigoplus_{i \geq 0} R_i$.*

Proof. Let I be a proper homogeneous ideal of R. We will show that $I \subseteq R_+$. By definition, the homogeneous components of any element of I lie in I, so it suffices to show that I does not contain any nonzero elements of R_0. But this is clear because R_0 is a field and I is a proper ideal of R. □

Generally, the following proposition characterizes the homogeneous maximal ideal of R.

Proposition 2.1.130. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. If I_0 is a proper ideal of the commutative unital ring R_0, then $I = I_0 \oplus R_+$ is a proper ideal of R. Even more, a proper*

homogeneous ideal M of R is maximal if and only if there exists a maximal ideal M_0 of R_0 such that $M = M_0 \oplus R_+$. Consequently, if R_0 is a local ring with unique maximal ideal $\mathfrak{m}$, then $\mathfrak{m} \oplus R_+$ is the unique homogeneous maximal ideal of R. We refer to R in this case as a **graded local** *ring.*

Proof. Observe that $(I,+)$ is an abelian group, hence it suffices to show that I is closed under scalar multiplication by elements of R. Every element of R can be written as $r = r_0 + r_1 + \cdots + r_m$ with $r_i \in R_i$, and every element of I can be written as $x = x_0 + s_1 + \cdots + s_n$ with $x_0 \in I_0$ and $s_i \in R_i$. Observe that the degree zero homogeneous component $r_0 x_0$ of rx lies in I_0 by assumption that I_0 is an ideal of R_0, and the rest of the homogeneous summands of rx lie in R_+. Consequently, the product of any element of R with any element of I lies in I, hence I is an ideal of R.

We will assume now that M_0 is a maximal ideal of R_0 and $M = M_0 \oplus R_+$. Observe that M is a homogeneous ideal, hence by Proposition 2.1.123, the quotient ring R/M is graded with respect to the abelian groups $(R_i + M)/M$. By construction, for each integer $i \geq 1$, we have that $R_i \subseteq M$ so that $(R_i + M)/M$ is zero. On the other hand, the maximal ideal M_0 of R_0 is contained in M, hence there exists a well-defined surjective ring homomorphism $R_0/M_0 \to R/M$. Considering that R_0/M_0 is a field, this map is an isomorphism, hence R/M is a field and M is maximal.

Conversely, if M is a homogeneous maximal ideal of R, then the quotient ring R/M is a $\mathbb{Z}_{\geq 0}$-graded field by Proposition 2.1.123, and every element of R/M lies in $(R_0 + M)/M$ by Proposition 2.1.122. We conclude that $(R_i + M)/M$ is zero for all integers $i \geq 1$, from which it follows that $R_i + M \subseteq M$ so that $R_i \subseteq M$ for all integers $i \geq 1$. Consequently, there exists an ideal M_0 of R_0 such that $M = M_0 \oplus R_+$. Observe that any containment $M_0 \subsetneq I_0$ of ideals of R_0 induces a containment of ideals $M = M_0 \oplus R_+ \subsetneq I_0 \oplus R_+$ of ideals of R, hence M_0 must be a maximal ideal of R_0. □

Certainly, the localization of a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring R with respect to a multiplicatively closed subset S of R yields a commutative unital ring $S^{-1}R$; however, it is not true a priori that $S^{-1}R$ admits a grading. Under mild assumptions, $S^{-1}R$ will also be $\mathbb{Z}_{\geq 0}$-graded.

Proposition 2.1.131. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. If S is a multiplicatively*

closed subset of homogeneous elements of R, then $S^{-1}R$ is $\mathbb{Z}$-graded with respect to

$$(S^{-1}R)_i = \left\{ \frac{r}{s} : r \in R_m,\, s \in R_n,\ \textit{and}\ i = m-n \right\}.$$

Proof. We must first establish that the degree of a homogeneous element of $S^{-1}R$ is well-defined. Consider two representations $\frac{r}{s} = \frac{r'}{s'}$ of a homogeneous element of $S^{-1}R$. By definition of the grading on $S^{-1}R$, the elements r, r', s, and s' are homogeneous with respective degrees m, m', n, and n'. By definition of the localization, there exists an element $t \in S$ such that $trs' = tr's$. By hypothesis that S consists of homogeneous elements of R, it follows that t is homogeneous of degree d. Consequently, we have that $d+m+n' = d+m'+n$ so that $m-n = m'-n'$.

We will demonstrate next that $(S^{-1}R)_i$ is an abelian group and $(S^{-1}R)_i(S^{-1}R)_j \subseteq (S^{-1}R)_{i+j}$. One can readily verify the latter fact by definition of the multiplication in $S^{-1}R$. Observe that if $\frac{a}{b}$ and $\frac{c}{d}$ are homogeneous elements of $(S^{-1}R)_i$, then their sum is $\frac{ad+bc}{bd}$. If $a \in R_m$, $b \in R_n$, $c \in R_{m'}$, and $d \in R_{n'}$, then ad lies in $R_{m+n'}$, bc lies in $R_{m'+n}$, and bd lies in $R_{n+n'}$. Considering that $m-n = i = m'-n'$, we conclude that $m+n' = m'+n$ so that $ad+bc$ is homogeneous of degree $m+n'$ and $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ is homogeneous of degree $(m+n')-(n+n') = m-n = i$.

Last, we will illustrate that every element of $S^{-1}R$ can be written uniquely as a sum of homogeneous elements of $S^{-1}R$. By hypothesis that S consists of homogeneous elements of R, every element of $S^{-1}R$ can be written as $\frac{r}{s}$ such that s is homogeneous. We may write $r = r_0 + \cdots + r_n$ for some homogeneous elements $r_i \in R_i$, hence we have that $\frac{r}{s} = \frac{r_0}{s} + \cdots + \frac{r_n}{s}$. We claim that this representation is unique. Observe that if there exist homogeneous elements $r'_i \in R_i$ and a homogeneous element $s \in S$ such that $\frac{r}{s} = \frac{r'_0}{s'} + \cdots + \frac{r'_n}{s'} = \frac{r'_0 + \cdots + r'_n}{s'}$, then there exists a homogeneous element $t \in S$ such that $ts'(r_0 + \cdots + r_n) = ts(r'_0 + \cdots + r'_n)$. Comparing degrees shows that $ts'r_i = tsr'_i$ for each integer $0 \leq i \leq n$ so that $\frac{r_i}{s} = \frac{r'_i}{s'}$ for each integer $0 \leq i \leq n$, as desired. □

Graded modules over graded rings are defined in a manner analogous to that of graded rings: an R-module M is $\mathbb{Z}_{\geq 0}$-**graded** if there exist abelian groups $(M_i, +)$ such that $M = \bigoplus_{i \geq 0} M_i$ as an abelian group and $R_i M_j \subseteq M_{i+j}$. We say that a graded R-module M is **finitely generated** if it is

finitely generated as an R-module; however, every finitely generated graded R-module admits a system of homogeneous generators of M. Crucially, for any finite system of generators of M, we may write each generator as a unique sum of its homogeneous components; the homogeneous system of generators for M consists precisely of these homogeneous summands. Crucially, a version of Nakayama's Lemma holds for $\mathbb{Z}_{\geq 0}$-graded modules over commutative unital $\mathbb{Z}_{\geq 0}$-graded rings.

Lemma 2.1.132 (Nakayama's Lemma)**.** *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. Let M be a $\mathbb{Z}_{\geq 0}$-graded R-module. If $I \subseteq R_+$ is a nonzero homogeneous ideal and $IM = M$, then $M = 0$.*

Proof. On the contrary, suppose that M is nonzero. Consequently, there exists a least integer $d \geq 0$ such that M_d is nonzero. By assumption that I is a nonzero proper homogeneous ideal of R, there exists a least integer $d' \geq 1$ such that $I_{d'}$ is nonzero. Observe that $I_{d'}M_d \subseteq M_{d+d'}$ is the smallest graded piece of IM that is nonzero. But the integer $d + d'$ is strictly larger than d, hence we must have that $IM \subsetneq M$ — a contradiction. We conclude that M must be the zero module. □

Graded R-module homomorphisms are precisely the R-module homomorphisms $\varphi : M \to N$ such that the ith graded piece of M lies in the ith graded piece of N, i.e., $\varphi(M_i) \subseteq N_i$. We say that a subset $N \subseteq M$ is a **graded R-submodule** of M if N is a graded R-module and $N_i \subseteq M_i$.

Proposition 2.1.133. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. Let M be a $\mathbb{Z}_{\geq 0}$-graded R-module. Let N be an R-submodule of M. The following conditions are equivalent.*

(i.) *N is graded.*

(ii.) *N is generated as an R-module by homogeneous elements.*

Proof. If N is graded, then every element of N can be written uniquely as a sum of homogeneous elements of N. Consequently, N is generated as an R-module by its homogeneous elements.

Conversely, suppose that N is generated as an R-module by homogeneous elements. We claim that N is graded with respect to the abelian groups $N_i = N \cap M_i$. By hypothesis that M is a $\mathbb{Z}_{\geq 0}$-graded R-module, it follows that $R_iN_j = R_i(N \cap M_j) \subseteq R_iN \cap R_iM_j \subseteq N \cap M_{i+j} = N_{i+j}$. Even more, for every element $n \in N$, there exist elements $r_0, \ldots, r_k \in R$ and homogeneous elements $n_0, \ldots, n_k$

with $n_i \in N_i$ such that $n = r_0 n_0 + \cdots + r_k n_k$. By writing $r_0, \ldots, r_k$ as sums of homogeneous components of R, the right-hand side of the above identity yields an expression of n as a sum of homogeneous elements of N_i. We conclude that $N \subseteq \sum_{i \geq 0} N_i$; the reverse containment is clear, hence it suffices to show that $N_i \cap N_j = 0$ if $i \neq j$. But this follows by assumption that $M = \bigoplus_{i \geq 0} M_i$. □

We note that the annihilator of a graded R-module is always homogeneous.

Proposition 2.1.134. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. Let M be a $\mathbb{Z}_{\geq 0}$-graded R-module. The annihilator* $\operatorname{ann}_R(M)$ *of M is a homogeneous ideal of R.*

Proof. Every nonzero element of M may be written as $m = m_0 + \cdots + m_k$ for some homogeneous elements $m_i \in M_i$. Likewise, every nonzero element of $\operatorname{ann}_R(M)$ may be written as $r = r_0 + \cdots + r_\ell$ for some homogeneous elements $r_j \in R_j$. Crucially, observe that $0 = rm_i = r_0 m_i + \cdots + r_\ell m_i$ for all integers $0 \leq i \leq k$ and the elements $r_j m_i$ lie in M_{i+j} for each integer $0 \leq j \leq \ell$. Consequently, we must have that $r_j m_i = 0$ for all integers $0 \leq i \leq k$ and $0 \leq j \leq \ell$, hence the homogeneous components of any element of $\operatorname{ann}_R(M)$ lie in $\operatorname{ann}_R(M)$, i.e., $\operatorname{ann}_R(M)$ is homogeneous. □

Corollary 2.1.135. *Let R be a commutative unital $\mathbb{Z}_{\geq 0}$-graded ring. If M is a $\mathbb{Z}_{\geq 0}$-graded R-module, then the annihilator of any nonzero element of M is a homogeneous ideal of R.*

Proof. Let m be a nonzero element of M. Consider the ideal $\operatorname{ann}_R(m) = \{r \in R \mid rm = 0\}$. Observe that Rm is a $\mathbb{Z}_{\geq 0}$-graded R-module with respect to the abelian groups $(Rm)_i = R_i m$. One can readily verify that $\operatorname{ann}_R(m) = \operatorname{ann}_R(Rm)$, hence $\operatorname{ann}_R(m)$ is homogeneous by Proposition 2.1.134 □

We turn our attention now to the construction of a "canonical" $\mathbb{Z}_{\geq 0}$-graded ring that can be obtained from any commutative unital ring R and any proper ideal I of R. We begin by defining the **associated graded ring** of R with respect to I as the R-module

$$\operatorname{gr}_I(R) = \bigoplus_{i \geq 0} \frac{I^i}{I^{i+1}} = \frac{R}{I} \oplus \frac{I}{I^2} \oplus \cdots$$

with $I^0 = R$. Our next proposition establishes that $\operatorname{gr}_I(R)$ is a commutative unital ring, hence in particular, $\operatorname{gr}_I(R)$ is $\mathbb{Z}_{\geq 0}$-graded with respect to the abelian groups $\operatorname{gr}_I(R)_i = I^i / I^{i+1}$.

Proposition 2.1.136. *If R is a commutative unital ring and I is a proper ideal of R, then $\operatorname{gr}_I(R)$ is a commutative unital ring with respect to the multiplication $(r+I^{i+1})(s+I^{j+1}) = rs+I^{i+j+1}$. Particularly, $\operatorname{gr}_I(R)$ is a $\mathbb{Z}_{\geq 0}$-graded ring with respect to the abelian groups $\operatorname{gr}_I(R)_i = I^i/I^{i+1}$.*

Proof. We must first demonstrate that the prescribed multiplication is well-defined. Observe that if $r+I^{i+1} = r'+I^{i+1}$ and $s+I^{j+1} = s'+I^{j+1}$, then $r-r' \in I^{i+1}$ and $s-s' \in I^{j+1}$. Considering that $r' \in I^i$ and $s \in I^j$, it follows that $rs-r's \in I^{i+j+1}$ and $r's-r's' \in I^{i+j+1}$ so that $rs-r's' \in I^{i+j+1}$ and $rs+I^{i+j+1} = r's'+I^{i+j+1}$. Consequently, $\operatorname{gr}_I(R)$ is a commutative ring with unity 1_R+I. Even more, we have established that $(\operatorname{gr}_I(R)_i)(\operatorname{gr}_I(R)_j) = (I^i/I^{i+1})(I^j/I^{j+1}) \subseteq I^{i+j}/I^{i+j+1} = \operatorname{gr}_I(R)_{i+j}$. □

Unsurprisingly, the structure of the associated graded ring $\operatorname{gr}_I(R)$ of R with respect to a proper ideal I is largely determined by the ring R and the ideal I, as we illustrate in the following.

Proposition 2.1.137. *Let R be a standard graded ring. If R_0 is a field, then $\operatorname{gr}_{R_+}(R) \cong R$.*

Proof. By hypothesis that R is standard graded and R_0 is a field, every nonzero non-unit element of R can be written uniquely as $\sum_{i=1}^{k} \alpha_i r_{i,1} \cdots r_{i,n_i}$ for some integers $k, n_1, \ldots, n_k \geq 1$, some elements $r_{1,1}, \ldots, r_{k,n_k} \in R_1$, and some elements $\alpha_1, \ldots, \alpha_k \in R_0$. Considering that $R_i R_j \subseteq R_{i+j}$, every nonzero summand $\alpha_i r_{i,n_1} \cdots r_{i,n_i}$ of this expression has a well-defined degree n_i. Consequently, we may define a graded ring homomorphism $\varphi : R \to \operatorname{gr}_{R_+}(R)$ by declaring that $\varphi(\alpha_i) = \alpha_i + R_+$ and $\varphi(\alpha_i r_{i,n_1} \cdots r_{i,n_i}) = \alpha_i r_{i,n_1} \cdots r_{i,n_i} + R_+^{n_i+1}$. By definition of $\operatorname{gr}_{R_+}(R)$, for every element $t \in \operatorname{gr}_{R_+}(R)$, there exists an integer $n \gg 0$ and elements $t_0, \ldots, t_n$ such that $t_i \in R_+^i \setminus R_+^{i+1}$; the ith component of t is $t_i + R_+^{i+1}$; and the kth component of t is zero for all integers $k \geq n+1$. Observe that $s = \sum_{j \geq i} t_i$ satisfies $s + R_+^{i+1} = t_i + R_+^{i+1}$, hence we conclude that $\varphi(s) = t$ so that φ is surjective. Even more, we have that $\ker \varphi = \bigcap_{i \geq 0} R_+^i$. By Krull's Intersection Theorem and the Graded Nakayama's Lemma, we conclude that $\bigcap_{i \geq 0} R_+^i = 0$, hence φ must be injective, as well. □

Proposition 2.1.138. *Let $(R, \mathfrak{m}, k)$ be a commutative unital local ring. Let I be a proper ideal of R. If $r_1, \ldots, r_n$ form a basis for the k-vector space $I/\mathfrak{m}I$, then $\operatorname{gr}_I(R) \cong (R/I)[r_1, \ldots, r_n]$.*

Proof. Consider the nonzero graded ring homomorphism $\varphi : R[r_1, \ldots, r_n] \to \operatorname{gr}_I(R)$ induced by the assignment $r_i \mapsto r_i + I^2$. By hypothesis that $I = (r_1, \ldots, r_n)$, it follows that φ is surjective. Observe

that the kernel of φ consists of those polynomials in the elements $r_1, \ldots, r_n$ with coefficients in I, i.e., $\ker \varphi = I[r_1, \ldots, r_n]$. By the First Isomorphism Theorem, we conclude the desired result. $\square$

Corollary 2.1.139. *If $(R, \mathfrak{m}, k)$ is a commutative unital Noetherian local ring and I is a proper ideal of R, then $\operatorname{gr}_I(R)$ is finitely generated as an R-module.*

Proof. By hypothesis that R is Noetherian, the ideal I is finitely generated. By Proposition 2.1.138, it follows that $\operatorname{gr}_I(R)$ is finitely generated as an algebra over the Noetherian ring R/I. By Proposition 2.1.128, we conclude that $\operatorname{gr}_I(R)$ is Noetherian, so it is finitely generated as an R-module. $\square$

Proposition 2.1.140. *Let $(R, \mathfrak{m}, k)$ be a regular local ring of dimension d with $\mathfrak{m} = (r_1, \ldots, r_d)$. Let $x_1, \ldots, x_d$ be indeterminates. We have that $\operatorname{gr}_{\mathfrak{m}}(R) \cong k[x_1, \ldots, x_d]$.*

Proof. By Proposition 2.1.138, we have that $\operatorname{gr}_{\mathfrak{m}}(R) \cong k[r_1, \ldots, r_d]$. We claim that the surjective ring homomorphism $\psi : k[x_1, \ldots, x_d] \to k[r_1, \ldots, r_d]$ induced by the assignment $x_i \mapsto r_i$ is injective. Each of the elements $r_1, \ldots, r_d$ lies in $\mathfrak{m} \setminus \mathfrak{m}^2$, hence they are homogeneous elements of degree one in $\operatorname{gr}_{\mathfrak{m}}(R)$. Consequently, the ring homomorphism ψ is graded, hence $\ker \psi$ is a homogeneous ideal of $k[x_1, \ldots, x_d]$ by Proposition 2.1.124. We claim that $\ker \psi = 0$. On the contrary, suppose that there exists a nonzero homogeneous polynomial $f \in \ker \psi$ of degree $i \geq 1$. Observe that the k-vector space $(\ker \varphi)_n$ is generated by the homogeneous polynomials of $\ker \varphi$ of degree n for every integer $n \geq 1$. Consequently, for any monomial $x_1^{a_1} \cdots x_d^{a_d}$ of degree $n - i > 0$, we have that $f x_1^{a_1} \cdots x_d^{a_d} \in (\ker \varphi)_n$. Even more, the collection of $\binom{d+n-i-1}{d-1}$ distinct polynomials $f x_1^{a_1} \cdots x_d^{a_d}$ with $a_1 + \cdots + a_d = n - i$ is k-linearly independent, hence we find that $\dim_k (\ker \varphi)_n \geq \binom{d+n-i-1}{d-1}$. By a similar analysis, the k-vector space $k[x_1, \ldots, x_d]_n$ is generated by the monomials of $k[x_1, \ldots, x_d]$ of degree n, hence we have that $\dim_k k[x_1, \ldots, x_d]_n = \binom{d+n-1}{d-1}$ for every integer $n \geq 1$. By the additivity of length along short exact sequences (cf. [Gat13, Proposition 3.22]), the graded short exact sequence

$$0 \to (\ker \varphi)_n \to k[x_1, \ldots, x_d]_n \to \frac{k[x_1, \ldots, x_d]_n + \ker \varphi}{\ker \varphi}$$

and our above computations yield that $\dim_k (k[x_1, \ldots, x_d]_n + \ker \varphi)/\ker \varphi \leq \binom{d+n-1}{d-1} - \binom{d+n-i-1}{d-1}$ for all integers $n > i \geq 1$. Observe that as a polynomial in d, the expression on the right-hand side

above has no more than $d-2$ (or zero if $d=1$). On the other hand, we have that $\mathfrak{m}^n$ is minimally generated in R by the elements $r_1^{a_1}\cdots r_d^{a_d}$ such that $a_1+\cdots+a_d=n$, from which it follows that $\dim_k \mathfrak{m}^n/\mathfrak{m}^{n+1} = \binom{d+n-1}{d-1}$ is a polynomial in d of degree $d-1$. But this is impossible: the First Isomorphism Theorem implies that $k[r_1,\ldots,r_d] \cong k[x_1,\ldots,x_d]/\ker\varphi$ as $\mathbb{Z}_{\geq 0}$-graded rings, hence the k-vector space dimension of the nth graded components of each of these should have the same degree as a polynomial in d. We conclude that $\ker\psi = 0$, and the desired isomorphism holds. $\square$

Conversely, the associated graded ring can provide some information about the underlying ring.

Proposition 2.1.141. *Let $(R,\mathfrak{m})$ be a commutative unital Noetherian local ring. If $\mathrm{gr}_{\mathfrak{m}}(R)$ is an integral domain, then R is an integral domain.*

Proof. Consider any elements $r,s \in R$ such that $rs = 0_R$. On the contrary, suppose that neither r nor s is zero. By Krull's Intersection Theorem, we have that $\bigcap_{n\geq 0}\mathfrak{m}^n = 0$, hence there exist integers $i \gg 0$ and $j \gg 0$ such that $r \in \mathfrak{m}^i$, $s \in \mathfrak{m}^j$, $r \notin \mathfrak{m}^{i+1}$, and $s \notin \mathfrak{m}^{j+1}$. Consequently, the nonzero elements $r+\mathfrak{m}^{i+1}$ and $s+\mathfrak{m}^{j+1}$ of $\mathrm{gr}_{\mathfrak{m}}(R)$ satisfy $(r+\mathfrak{m}^{i+1})(s+\mathfrak{m}^{j+1}) = rs+\mathfrak{m}^{i+j+1} = 0_R+\mathfrak{m}^{i+j+1}$. But if $\mathrm{gr}_{\mathfrak{m}}(R)$ is a domain, then either $r \in \mathfrak{m}^{i+1}$ or $s \in \mathfrak{m}^{j+1}$ — a contradiction. $\square$

One of the most important features of the associated graded ring of a Noetherian local ring is that it preserves Krull dimension. We omit the proof; it can be found in [BH93, Theorem 4.5.6].

Proposition 2.1.142. *If $(R,\mathfrak{m})$ is a Noetherian local ring, then* $\dim(R) = \dim(\mathrm{gr}_I(R))$.

Even more, the associated graded ring of a commutative unital ring R with respect to a maximal ideal $\mathfrak{m}$ can be identified with the associated graded ring of the local ring $(R_{\mathfrak{m}}, \mathfrak{m}R_{\mathfrak{m}})$.

Proposition 2.1.143. *We have that $\mathrm{gr}_{\mathfrak{m}}(R) \cong \mathrm{gr}_{\mathfrak{m}R_{\mathfrak{m}}}(R_{\mathfrak{m}})$ for any maximal ideal $\mathfrak{m}$ of R.*

Proof. By definition, the ith graded piece of $\mathrm{gr}_{\mathfrak{m}}(R)$ is $\mathrm{gr}_{\mathfrak{m}}(R)_i = \mathfrak{m}^i/\mathfrak{m}^{i+1}$. Considering that $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is annihilated by the maximal ideal $\mathfrak{m}$ of R, it follows that $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is an $R/\mathfrak{m}$-vector space for each integer $i \geq 0$. Consequently, the elements of $R\setminus\mathfrak{m}$ must act invertibly on the $R/\mathfrak{m}$-vector spaces $\mathfrak{m}^i/\mathfrak{m}^{i+1}$, as they are precisely the units of R modulo $\mathfrak{m}$. By Propositions 6.2.7 and 6.2.10, we conclude that $(\mathfrak{m}^iR_{\mathfrak{m}})/(\mathfrak{m}^{i+1}R_{\mathfrak{m}}) \cong (\mathfrak{m}^i/\mathfrak{m}^{i+1})_{\mathfrak{m}} \cong R_{\mathfrak{m}} \otimes_R (\mathfrak{m}^i/\mathfrak{m}^{i+1}) \cong \mathfrak{m}^i/\mathfrak{m}^{i+1}$. $\square$

We conclude this section with a crucial result on regular local rings.

Proposition 2.1.144. *Every regular local ring $(R,\mathfrak{m})$ is a unique factorization domain.*

Proof. By Proposition 2.1.140, we have that $\mathrm{gr}_{\mathfrak{m}}(R)$ is an integral domain, hence we conclude that R is an integral domain by Proposition 2.1.141.

We will now demonstrate that R is a unique factorization domain. We proceed by induction on $\dim(R) = d$. By Example 2.1.47, a regular local ring of dimension zero is a field, hence the claim holds for $d = 0$. Even more, if $d = 1$, then for any nonzero proper ideal I of R, there exists an element $x \in I \setminus \mathfrak{m}I$ by the contrapositive of Corollary 2.1.17. By Krull's Intersection Theorem applied to the nonzero proper ideal xR, for every element $r \in I$, there exists an integer $n \gg 0$ and an element $s \in R$ such that $x^n r = x^{n+1}s$. Cancellation holds in R because it is a domain, hence we conclude that $r = xs$ so that $I = xR$. Consequently, R is a principal ideal domain.

We will assume inductively that the claim holds for all integers not exceeding $d-1$. By Proposition 2.1.48, it suffices to show that every height-one prime ideal P of R is principal. Once again, we may consider an element $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Observe that x is R-regular, hence we find that R/xR is a regular local ring by Proposition 2.2.28. Consequently, the quotient ring R/xR is an integral domain so that xR is a prime ideal of height one. Observe that if $x \in P$, then $P = xR$ is principal, and our proof is complete. We may assume therefore that $x \in R \setminus P$. Observe that $S = \{x^i \mid i \geq 0\}$ is a multiplicatively closed subset of R, hence we may obtain the localization $S^{-1}R = R_x$. By Proposition 2.1.9, the prime ideals of R_x are in bijection with the prime ideals of R that do not contain x. Consequently, by Proposition 6.2.5, every localization of R_x at a prime ideal of R_x is isomorphic to R_Q for some prime ideal Q of R such that Q does not contain x. Crucially, such a prime ideal Q cannot be the maximal ideal $\mathfrak{m}$, hence R_Q must be a regular local ring of dimension strictly lesser than $\dim(R)$ by [BH93, Corollary 2.2.9]. Observe that if $P \subseteq R \setminus Q$, then $PR_Q = R_Q$, hence PR_Q is a free R_Q-module of rank one. Conversely, if $P \subseteq Q$, then PR_Q is a height-one prime ideal of the regular local ring R_Q of dimension strictly lesser than $\dim(R)$ because PR_x is a height-one prime ideal of R_x. By induction, we find that PR_Q is a principal ideal of the integral domain R_Q, hence we have that $PR_Q \cong R_Q$ is a free R_Q-module of rank one. Consequently, we conclude by

Propositions 2.1.101 that PR_x is a projective R_x-module. By [BH93, Theorem 2.2.7], there exists a free resolution $F_\bullet : 0 \to F_n \to \cdots \to F_1 \to F_0 \to P \to 0$ of P as an ideal of R; its localization $S^{-1}F_\bullet : 0 \to S^{-1}F_n \to \cdots \to S^{-1}F_1 \to S^{-1}F_0 \to PR_x \to 0$ yields a free resolution of PR_x by Propositions 6.2.4 and 6.2.10 and Corollary 6.2.9. Considering that PR_x is a projective R_x-module, we conclude that there exist positive integers i and j such that $R_x^i \cong PR_x \oplus R_x^j$ by Corollary 2.1.83. Localizing at any prime ideal Q of R_x yields that $R_Q^i \cong PR_Q \oplus R_Q^j$, hence the isomorphism $PR_Q \cong R_Q$ implies that $i = j+1$. By [BH93, Theorem 1.4.17], we conclude that PR_x is a principal ideal of R_x. Consequently, there exists a nonzero element $p \in P$ such that $PR_x = \frac{p}{1_R}R_x$. Observe that if p divides rs in R, then $\frac{rs}{1_R}$ lies in the prime ideal PR_x, from which it follows that $\frac{p}{1_R}$ divides either $\frac{r}{1_R}$ or $\frac{s}{1_R}$ in R_x. By definition of divisibility in R_x, there exists an integer $i \geq 0$ and an element $t \in R$ such that $pt = rx^i$ or $pt = sx^i$. Either way, we conclude that p must divide either r or s because p does not divide any power of x by assumption that x does not lie in P. Ultimately, this shows that pR is a prime ideal of R that lies in the height-one prime ideal P of R so that $P = pR$. □

2.1.6 Completions of Rings and Modules

Given any proper ideal I of a commutative unital ring R, we can impose a topology — called the I-**adic topology** — on R by declaring that $U \subseteq R$ is open if and only if for every element $x \in U$, there exists an integer $n \gg 0$ such that $x + I^n \subseteq U$. Consequently, we may view R as a topological ring. Under this identification, one can define a **Cauchy sequence** of elements of R (with respect to I) as any infinite tuple $(r_n)_{n\geq 0}$ of elements of R such that for all integers $k \geq 0$, there exists an integer $N_k \gg 0$ such that $r_m - r_n \in I^k$ for all integers $m, n \geq N_k$. We say that a sequence $(r_n)_{n\geq 0}$ of elements of R **converges to zero** in the I-adic topology if for all integers $k \geq 0$, there exists an integer $N_k \gg 0$ such that $r_n \in I^k$ for all integers $n \geq N_k$; a sequence $(r_n)_{n\geq 0}$ of elements of R **converges** to an element $r \in R$ in the I-adic topology if the sequence $(r_n - r)_{n\geq 0}$ converges to zero in the I-adic topology. By definition, the topological ring R is complete if and only if all Cauchy sequences of elements of R converge to an element of R. Certainly, this is not always the case.

Example 2.1.145. Observe that the ring $\mathbb{R}[x]$ of univariate real polynomials equipped with the

(x)-adic topology admits a Cauchy sequence $(1+x+\cdots+x^n)_{n\geq 0}$ whose limit is the formal power series $(1-x)^{-1}=\sum_{n=0}^{\infty}x^n$, hence $\mathbb{R}[x]$ is not complete with respect to the (x)-adic topology.

Consequently, one may naturally seek to construct the **completion** $\widehat{R}_I$ of R with respect to the I-adic topology. Clearly, in order to complete R with respect to the I-adic topology, we must expand R to include the limit of all Cauchy sequences of elements of R; however, as we began with a commutative unital ring R, we require that the completion $\widehat{R}_I$ is also a commutative unital ring. Observe that the set $C_I(R)$ of Cauchy sequences of elements of R with respect to the I-adic topology is a commutative unital ring with respect to componentwise addition and multiplication: indeed, we have that $C_I(R)\subseteq\prod_{n\geq 0}R$, and $C_I(R)$ is closed under addition and multiplication. Further, it is a ring extension of R via the map $\gamma\colon R\to C_I(R)$ defined by $\gamma(r)=(r)_{n\geq 0}$; however, $C_I(R)$ is "larger" than $\widehat{R}_I$, so this naïve topological approach fails. Our next construction is purely algebraic, instead.

Consider the descending filtration $R\supsetneq I\supsetneq I^2\supsetneq\cdots$ of R-submodules. Canonically, there exist ring homomorphisms $\pi_n : R\to R/I^n$ and $\pi_{m,n} : R/I^m\to R/I^n$ for any integers $m\geq n\geq 0$ defined by $\pi_n(r)=r+I^n$ and $\pi_{m,n}(r+I^m)=r+I^n$ that satisfy $\pi_n=\pi_{m,n}\circ\pi_m$, hence the **inverse limit**

$$\varprojlim(R/I^n)=\left\{(r_n+I^n)_{n\geq 0}\in\prod_{n\geq 0}R/I^n : r_m-r_n\in I^n \text{ for all integers } m\geq n\geq 0\right\}$$

of R with respect to the inverse system $((R/I^n)_{n\geq 0},\{\pi_{m,n}\}_{m\geq n})$ is a commutative unital ring. Even more, it is complete with respect to the I-adic topology by construction. Given any element $(r_n)_{n\geq 0}$ of $C_I(R)$ and any integer $k\geq 0$, there exists an integer $N_k\gg 0$ such that $r_m+I^k=r_n+I^k$ for all integers $m,n\geq N_k$. Consequently, the map $\varphi_k : C_I(R)\to R/I^k$ defined by $\varphi_k((r_n)_{n\geq 0})=r_{N_k}+I^k$ is a well-defined ring homomorphism. Constant sequences of elements of R are Cauchy, hence φ_k is surjective. Further, we have that $\varphi_n=\pi_{m,n}\circ\varphi_m$, hence there exists a unique ring homomorphism $\varphi : C_I(R)\to\varprojlim(R/I^n)$ such that $\pi_n\circ\varphi=\varphi_n$ by the universal property of the inverse limit. Considering that φ_n is surjective, the induced map φ must be surjective; it maps the Cauchy sequence $(r_n)_{n\geq 0}$ onto the Cauchy sequence $(r_{N_n})_{n\geq 0}$, so its kernel consists of all Cauchy sequences $(r_n)_{n\geq 0}$ of elements of R such that for any integer $k\geq 0$, there exists an integer $N_k\gg 0$ such that $r_n\in I^k$ for

all integers $n \geq N_k$, i.e., $\ker \varphi$ is equal to the ideal $Z_I(R)$ of Cauchy sequences that converge to zero in the I-adic topology. We conclude that $C_I(R)/Z_I(R) \cong \varprojlim(R/I^n)$; the latter is the completion $\widehat{R}_I$ of R with respect to the I-adic topology by the universal property of the inverse limit. We invite the reader to reference [Rot09, Section 5.2] for more information on inverse limits in general.

Before we proceed, we record a proposition that allows us to work with elements of $\widehat{R}_I$.

Proposition 2.1.146. *Let R be a commutative unital ring. Let I be a proper ideal of R. Let $C_I(R)$ denote the ring of Cauchy sequences of elements of R in the I-adic topology. Let $Z_I(R)$ denote the ideal of Cauchy sequences that converge to zero in the I-adic topology. Let $\widehat{R}_I$ be the completion of R with respect to the I-adic topology. For any sequence $(r_n)_{n\geq 0} \in C_I(R)$ and any subsequence $(r_{n_k})_{k\geq 0}$, we have that $(r_k - r_{n_k})_{k\geq 0} \in Z_I(R)$. Particularly, every element of $\widehat{R}_I$ can be identified with a sequence $(r_n)_{n\geq 0}$ of elements of R such that $r_{n+1} - r_n \in I^n$ for all integers $n \geq 0$.*

Proof. Let $(r_n)_{n\geq 0}$ be a Cauchy sequence of elements of R with respect to the I-adic topology, and let $(r_{n_k})_{k\geq 0}$ be any subsequence. Given an integer $\ell \geq 0$, there exists an integer $N_\ell \gg 0$ such that $r_m - r_n \in I^\ell$ for all integers $m, n \geq N_\ell$. Considering that $(r_{n_k})_{k\geq 0}$ is a subsequence of $(r_n)_{n\geq 0}$, it follows that $n_k \geq k$ for each integer $k \geq 0$ so that $n_m \geq m \geq N_\ell$ and $r_m - r_{n_m} \in I^\ell$. We conclude that $(r_k - r_{n_k})_{k\geq 0}$ is a Cauchy sequence that converges to zero with respect to the I-adic topology.

Consequently, for any element $r \in \widehat{R}_I$, there exists a Cauchy sequence $(r_n)_{n\geq 0}$ of elements of R such that $r_{n+1} - r_n \in I^n$ for all integers $n \geq 0$ whose image in $\widehat{R}_I$ is equal to r. □

Example 2.1.147. Let $R = \mathbb{R}[x]$, and let $I = (x)$. By Proposition 2.1.146, every element of $\widehat{R}_I$ can be identified with a sequence of elements of R such that $r_{n+1} - r_n \in I^n$ for all integers $n \geq 0$. One can construct such an sequence recursively as follows. Begin with some elements $r_0, r_1 \in \mathbb{R}[x]$. Using the fact that $r_2 - r_1 \in I$, it follows that $r_2 = p_1(x)x + r_1$ for some polynomial $p_1(x) \in \mathbb{R}[x]$. Likewise, we have that $r_3 - r_2 \in I^2$ so that $r_3 = p_2(x)x^2 + r_2 = p_2(x)x^2 + p_1(x)x + r_1$. Continuing in this manner, there exist elements $a_0, a_1, \ldots, a_n \in \mathbb{R}$ such that $r_{n+1} = r_1 + \sum_{k=0}^{n} p_k(x)x^k$. Considering that $\widehat{R}_I$ is complete, it must contain the limit of all such sequences, hence we conclude that $\widehat{R}_I$ is the ring of formal power series with real coefficients, i.e., we have that $\widehat{R}_I = \mathbb{R}[\![x]\!]$.

Our next proposition illustrates that many of the properties of $\widehat{R}_I$ are determined by I.

Proposition 2.1.148. *Let R be a commutative unital ring. Let I be a proper ideal of R. Let $\widehat{R}_I$ be the completion of R with respect to the I-adic topology. Consider the canonical ring homomorphisms $\gamma_I : R \to \widehat{R}_I$ and $\pi_I : \widehat{R}_I \to R/I$ defined by $\gamma_I(r) = (r+I^n)_{n\geq 0}$ and $\pi_I((r_n+I^n)_{n\geq 0}) = r_1 + I$.*

(1.) *If R is Noetherian, then $\widehat{R}_I$ is Noetherian.*

(2.) *We have that $\ker \gamma_I = \bigcap_{n\geq 0} I^n$. Particularly, if R is a Noetherian local ring or a Noetherian integral domain, then γ_I is injective, and we may identify R with a subring of $\widehat{R}_I$.*

(3.) *We have that $\ker \pi_I = \{(r_n+I^n)_{n\geq 0} \mid r_n \in I \text{ for all integers } n \geq 1\}$.*

(4.) *If u is a unit of $\widehat{R}_I$ and r lies in $\ker \pi_I$, then $u+r$ is a unit of $\widehat{R}_I$.*

(5.) *Every maximal ideal of $\widehat{R}_I$ contains $\ker \pi_I$, hence the maximal ideals of $\widehat{R}_I$ and R/I are in one-to-one correspondence. Particularly, if R/I is a local ring, then $\widehat{R}_I$ is a local ring.*

Proof. (1.) If R is Noetherian, then I is generated by some elements $r_1, \ldots, r_n \in R$. Consider the surjective ring homomorphism $\varphi : R[x_1, \ldots, x_n] \to R$ induced by the assignments $x_i \mapsto r_i$. We have that $I^k = \varphi[(x_1, \ldots, x_n)^k]$ for each integer $k \geq 0$, hence there exists a well-defined surjective ring homomorphism $R[x_1, \ldots, x_n]/(x_1, \ldots, x_n)^k \to R/I^k$ for each integer $k \geq 0$. Consequently, the completion of $R[x_1, \ldots, x_n]$ with respect to the $(x_1, \ldots, x_n)$-adic topology surjects onto $\widehat{R}_I$. By Example 2.1.147, the former is the ring $R[\![x_1, \ldots, x_n]\!]$; it is Noetherian, so $\widehat{R}_I$ is Noetherian.

(2.) Observe that $r \in \ker \gamma_I$ if and only if $r + I^n = 0_R + I^n$ for each integer $n \geq 0$ if and only if $r \in \bigcap_{n\geq 0} I^n$, hence we find that $\ker \gamma_I = \bigcap_{n\geq 0} I^n$. If R is a Noetherian local ring, then $\bigcap_{n\geq 0} I^n = 0$ by 2.1.20. If R is a Noetherian domain, then there exists an element $x \in I$ such that $(1_R - x)\bigcap_{n\geq 0} I^n = 0_R$ by 2.1.20. Consequently, for any element $i \in \bigcap_{n\geq 0} I^n$, we have that $(1_R - x)i = 0_R$. But I is a proper ideal of R and $x \in I$, so we must have that $i = 0_R$.

(3.) Observe that $(r_n + I^n)_{n\geq 0} \in \ker \pi_I$ if and only if $r_1 + I = 0_R + I$ if and only if $r_1 \in I$ if and only if $r_n \in I$ for each integer $n \geq 1$. Crucially, the last equivalence holds because an element $(r_n + I^n)_{n\geq 0}$ of $\widehat{R}_I$ must satisfy the condition that $r_n - r_1 \in I$ for each integer $n \geq 1$.

(4.) (Hochster) By hypothesis that u is a unit of $\widehat{R}_I$, we have that $u+r = u(1+u^{-1}r)$, and it suffices to show that $1+u^{-1}r$ is a unit of $\widehat{R}_I$. Given an element $(r_n)_{n\geq 0}$ of $\widehat{R}_I$ that represents $u^{-1}r$, we may consider the sequence $s_n = 1+\sum_{k=0}^{n}(-1)^{k+1}r_n^{k+1}$ for each integer $n \geq 0$. Observe that

$$s_{n+1} - s_n = \sum_{k=0}^{n+1}(-1)^{k+1}r_{n+1}^{k+1} - \sum_{k=0}^{n}(-1)^{k+1}r_n^{k+1} = (-1)^{n+2}r_{n+1}^{n+2} + \sum_{k=0}^{n}(-1)^{k+1}(r_{n+1}^{k+1} - r_n^{k+1}).$$

Considering that $r_{n+1}-r_n$ divides $r_{n+1}^{k+1} - r_n^{k+1}$, the latter summand belongs to I^n; the former summand belongs to I^{n+2} by the condition that $r_{n+1} - r_1 \in I$ for each integer $n \geq 0$. Ultimately, this implies that $s_{n+1} - s_n$ belongs to I^n for each integer $n \geq 0$ so that $s_m - s_n \in I^n$ for all integers $m \geq n \geq 0$, i.e., $(s_n)_{n\geq 0}$ is a Cauchy sequence with respect to the I-adic topology. Even more, we have that $(1+r_n)s_n = 1 - r_n^{n+2}$ so that $r_n^{n+2} = 1-(1+r_n)s_n$. Considering that the sequence $(r_n^{n+2})_{n\geq 0}$ converges to zero with respect to the I-adic topology, we conclude that the sequence $((1+r_n)s_n)_{n\geq 0}$ converges to 1 in the I-adic topology, i.e., $1+u^{-1}r$ is a unit of $\widehat{R}_I$.

(5.) On the contrary, assume that M is a maximal ideal of $\widehat{R}_I$ that does not contain $\ker \pi_I$. By hypothesis, the quotient ring $\widehat{R}_I/M$ is a field, and there exists an element $r \in \ker \pi_I$ such that $r+M$ is a unit of $\widehat{R}_I/M$. Consequently, there exists an element $s+M$ such that $rs+M = 1+M$ and $rs = 1+x$ for some element $x \in M$. By the previous part of the proposition, the element $x = 1-rs$ of M is a unit of $\widehat{R}_I$ — a contradiction. We conclude that every maximal ideal of $\widehat{R}_I$ contains $\ker \pi_I$, hence the maximal ideals of $\widehat{R}_I$ are in one-to-one correspondence with the maximal ideals of $\widehat{R}_I/\ker \pi_I$; these are in bijection with the maximal ideals of R/I via the isomorphism $\widehat{R}_I/\ker \pi_I \cong R/I$. □

Corollary 2.1.149. *If $(R,\mathfrak{m})$ is a local ring, its $\mathfrak{m}$-adic completion $\widehat{R}_{\mathfrak{m}}$ is a complete local ring.*

We conclude this section with a discussion of completion as a functor. Given a commutative unital ring R and a proper ideal I of R, for any R-module M, one can define the completion of M with respect to the I-adic topology as the inverse limit $\widehat{M}_I = \varprojlim(M/I^nM)$. Observe that $\widehat{M}_I$ is an $\widehat{R}_I$-module with respect to componentwise multiplication, hence the map $\widehat{R}_I \otimes_R M \to \widehat{M}_I$ that sends $(r_n+I^n)_{n\geq 0}\otimes_R m \mapsto (r_nm + I^nM)_{n\geq 0}$ is a well-defined $\widehat{R}_I$-module homomorphism. On the other hand, by Proposition 2.1.89, it follows that $\widehat{R}_I \otimes_R R^n \cong (\widehat{R}_I \otimes_R R)^n \cong \widehat{R}_I^n$ for any integer

$n \geq 1$. Our immediate aim is to establish a similar fact for the right-exact functors $\widehat{R}_I \otimes_R -$. Before this, we note that if $\varphi : M \to N$ is an R-module homomorphism, then there exists an induced R-module homomorphism $\widehat{\varphi}_I : \widehat{M}_I \to \widehat{N}_I$ by the universal property of the inverse limit, as the R-module homomorphisms $\varphi_n : M/I^nM \to N/I^nN$ that send $m + I^nM \mapsto \varphi(m) + I^nN$ are well-defined.

Lemma 2.1.150. *Let R be a commutative unital ring. Let I be a proper ideal of R. Let M and N be R-modules. Let $\widehat{M}_I$ and $\widehat{N}_I$ be the respective completions of M and N with respect to the I-adic topology. If $\varphi : M \to N$ is a surjective R-module homomorphism, then $\widehat{\varphi}_I : \widehat{M}_I \to \widehat{N}_I$ is surjective.*

Proof. Observe that if $\varphi : M \to N$ is a surjective R-module homomorphism, then for each integer $n \geq 1$, the map $\varphi_n : M/I^nM \to N/I^nN$ that sends $x + I^nM \mapsto \varphi(x) + I^nN$ is a well-defined surjective R-module homomorphism. Consequently, the R-modules $K_n = \{x \in M \mid \varphi(x) \in I^nN\}$ induce short exact sequences of R-modules $0 \to K_n/I^nM \to M/I^nM \to N/I^nN \to 0$ for each integer $n \geq 1$. We claim that there exist surjective R-module homomorphisms $K_m/I^mM \to K_n/I^nM$ for all integers $m \geq n \geq 1$. By definition, for any element $x \in K_n$, there exists an integer $\ell \geq 0$ and elements $r_1, \ldots, r_\ell \in I^n$ and $y_1, \ldots, y_\ell \in N$ such that $\varphi(x) = r_1y_1 + \cdots + r_\ell y_\ell$. By hypothesis that $\varphi : M \to N$ is a surjective R-module homomorphism, there exist elements $x_1, \ldots, x_\ell \in M$ such that $\varphi(x_i) = y_i$ and $\varphi(x) = r_1\varphi(x_1) + \cdots + r_\ell\varphi(x_\ell) = \varphi(r_1x_1 + \cdots + r_\ell x_\ell)$ so that $\varphi[x - (r_1x_1 + \cdots + r_\ell x_\ell)] = 0$. Consequently, $x - (r_1x_1 + \cdots r_\ell x_\ell)$ lies in K_m, and its image modulo I^nM lies in K_n. We conclude that for all integers $m \geq n \geq 1$, the map $\pi_{m,n} : K_m/I^mM \to K_n/I^nM$ that sends $x + I^mM \mapsto x + I^nM$ is a well-defined surjective R-module homomorphism. Observe that these maps induce a surjective inverse system $((K_n/I^nM)_{n\geq 0}, \{\pi_{m,n}\}_{m\geq n})$. By [AM69, Proposition 10.2], we conclude that the sequence $0 \to \varprojlim(K_n/I^nM) \to \varprojlim(M/I^nM) \to \varprojlim(N/I^nM) \to 0$ is exact. By identifying the R-modules $\widehat{M}_I = \varprojlim(M/I^nM)$ and $\widehat{N}_I = \varprojlim(N/I^nM)$, it follows that $\widehat{\varphi}_I : \widehat{M}_I \to \widehat{N}_I$ is surjective. $\square$

Proposition 2.1.151. *Let R be a Noetherian commutative unital ring. Let I be a proper ideal of R. Let L, M, and N be finitely generated R-modules. Let $\widehat{L}_I$, $\widehat{M}_I$, and $\widehat{N}_I$ be the respective completions of L, M, and N with respect to the I-adic topology. If there exists an exact sequence of R-modules $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$, then the induced sequence $0 \to \widehat{L}_I \xrightarrow{\widehat{\varphi}_I} \widehat{M}_I \xrightarrow{\widehat{\psi}_I} \widehat{N}_I \to 0$ is exact.*

Proof. Let $0 \to L \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$ be a short exact sequence of R-modules. By the proof of Lemma 2.1.150, for each integer $n \geq 1$, there exists a well-defined surjective R-module homomorphism $\psi_n : M/I^nM \to N/I^nN$ that sends $x + I^nM \mapsto \psi(x) + I^nN$ and satisfies the property that

$$\ker \psi_n = \left\{ x + I^nM : \psi\left(x - \sum_{i=1}^{\ell} r_i x_i \right) = 0 \text{ for some elements } r_1, \ldots, r_\ell \in I^n \text{ and } x_1, \ldots, x_\ell \in M \right\}.$$

Put another way, $\ker \psi_n$ consists precisely of those elements $x \in M$ such that the difference of x and some element of I^nM lies in $\ker \psi$. By our initial short exact sequence, we have that $\ker \psi = \operatorname{img} \varphi$, from which it follows that $\ker \psi_n$ consists precisely of those elements $x \in M$ that are the sum of an element of $\operatorname{img} \varphi$ and an element of I^nM. Put another way, we have that $\ker \psi_n = \operatorname{img} \varphi + I^nM$. Consequently, we may define for each integer $n \geq 1$ a well-defined injective R-module homomorphism $\varphi_n : L/\varphi^{-1}(I^nM) \to M/I^nM$ that sends $y + \varphi^{-1}(I^nM) \mapsto \varphi(y) + I^nM$ and satisfies the property that $\operatorname{img} \varphi_n = \ker \psi_n$. Ultimately, for each integer $n \geq 1$, there exists a short exact sequence of R-modules $0 \to L/\varphi^{-1}(I^nM) \xrightarrow{\varphi_n} M/I^nM \xrightarrow{\psi_n} N/I^nN \to 0$. Even more, the R-modules $(L/\varphi^{-1}(I^nM))_{n \geq 0}$ together with the R-module maps $L/\varphi^{-1}(I^mM) \to L/\varphi^{-1}(I^nM)$ that send $y + \varphi^{-1}(I^mM) \mapsto y + \varphi^{-1}(I^nM)$ for each integer $m \geq n \geq 1$ form a surjective inverse system. We conclude that $0 \to \varprojlim(L/\varphi^{-1}(I^nM)) \to \varprojlim(M/I^nM) \to \varprojlim(N/I^nN) \to 0$ is an exact sequence by [AM69, Proposition 10.2]. By the Artin-Rees Lemma, there exists an integer $k \gg 0$ such that

$$I^n\varphi(L) \subseteq I^nM \cap \varphi(L) = I^{n-k}(I^kM \cap \varphi(L)) \subseteq I^{n-k}\varphi(L)$$

for all integers $n \geq k$. By hypothesis that φ is injective, we find that

$$I^nL = \varphi^{-1}(I^n\varphi(L)) \subseteq \varphi^{-1}(I^nM \cap \varphi(L)) = \varphi^{-1}(I^nM) \subseteq \varphi^{-1}(I^{n-k}\varphi(L)) = I^{n-k}L.$$

Consequently, we conclude that $\varprojlim(L/\varphi^{-1}(I^nM)) = \varprojlim(L/I^nL) = \widehat{L}_I$, as desired. □

Combining our previous work yields the following property of Noetherian rings.

Corollary 2.1.152. *Let R be a commutative unital ring. Let I be a proper ideal of R. The map*

$(-)^\wedge$ that sends an R-module M to its completion $\widehat{M}_I$ with respect to the I-adic topology and sends an R-module homomorphism $\varphi : M \to N$ to $\widehat{\varphi}_I : \widehat{M}_I \to \widehat{N}_I$ is a covariant right-exact functor. If R is Noetherian, then it is left-exact on exact sequences of finitely generated R-modules.

By Definition 2.1.3, every ideal of a Noetherian commutative unital ring is finitely generated. Consequently, any short exact sequences of R-modules consisting of ideals of R and quotients thereof induces a short exact sequence of their completions by Proposition 2.1.151.

Corollary 2.1.153. *Let R be a Noetherian commutative unital ring. Let I be a proper ideal of R. Let $\widehat{R}$ be the completion of R with respect to the I-adic topology. We have that $R/I^n \cong \widehat{R}/\widehat{I^n}$ and $I^n/I^{n+1} \cong \widehat{I^n}/\widehat{I^{n+1}}$ as R-modules.*

Proof. Observe that for each integer $n \geq 0$, the R-modules $R_n = R/I^n$ and $Q_n = I^n/I^{n+1}$ are annihilated by all sufficiently large powers of I so that $R/I^n = R_n \cong \varprojlim(R_n/I^k R_n) = \widehat{R_n} = \widehat{R/I^n}$ and $I^n/I^{n+1} = Q_n \cong \varprojlim(Q_n/I^k Q_n) = \widehat{Q_n} = \widehat{I^n/I^{n+1}}$. Consequently, the short exact sequence of R-modules $0 \to I^n \to R \to R/I^n \to 0$ induces a short exact sequence $0 \to \widehat{I^n} \to \widehat{R} \to R/I^n \to 0$ by Proposition 2.1.151, from which it follows that $R/I^n \cong \widehat{R}/\widehat{I^n}$ by the First Isomorphism Theorem. Likewise, the short exact sequence of R-modules $0 \to I^{n+1} \to I^n \to I^n/I^{n+1} \to 0$ induces a short exact sequence $0 \to \widehat{I^{n+1}} \to \widehat{I^n} \to I^n/I^{n+1} \to 0$, and the result follows as before. □

Corollary 2.1.154. *Let R be a Noetherian commutative unital ring. Let I be a proper ideal of R. Let $\widehat{R}$ be the completion of R with respect to the I-adic topology. We have that $\mathrm{gr}_I(R) \cong \mathrm{gr}_{\widehat{I}}(\widehat{R})$.*

Proof. By Proposition 2.1.153, there are isomorphisms $R/I \to \widehat{R}/\widehat{I}$ and $I^n/I^{n+1} \to \widehat{I^n}/\widehat{I^{n+1}}$ of R-modules for each integer $n \geq 0$. Consequently, there exists an R-module isomorphism

$$\mathrm{gr}_I(R) = \bigoplus_{n \geq 0} \frac{I^n}{I^{n+1}} \to \bigoplus_{n \geq 0} \frac{\widehat{I^n}}{\widehat{I^{n+1}}} = \mathrm{gr}_{\widehat{I}}(\widehat{R}).$$ □

Corollary 2.1.155. *Let $(R, \mathfrak{m})$ be a commutative unital Noetherian local ring. Let I be a proper ideal. Let $\widehat{R}$ be the completion with respect to the I-adic topology. We have that $\dim(R) = \dim(\widehat{R})$.*

Proof. By Proposition 2.1.142 and Corollary 2.1.154, we have that

$$\dim(R) = \dim(\mathrm{gr}_I(R)) = \dim(\mathrm{gr}_{\widehat{I}}(\widehat{R})) = \dim(\widehat{R}). \qquad \square$$

Corollary 2.1.156. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. The following are equivalent.*

(i.) *R is regular.*

(ii.) *$\widehat{R}_{\mathfrak{m}}$ is regular.*

Proof. We will simply write $\widehat{R}$ for the completion of R with respect to the $\mathfrak{m}$-adic topology. By Corollary 2.1.153, we have that $R/\mathfrak{m} \cong \widehat{R}/\widehat{\mathfrak{m}}$ and $\mathfrak{m}/\mathfrak{m}^2 \cong \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}^2}$, from which it follows that $\mu(\widehat{\mathfrak{m}}) = \mu(\mathfrak{m})$. On the other hand, it follows that $\dim(\widehat{R}) = \dim(R)$ by Corollary 2.1.155. Combined, these two observations imply that $\dim(R) = \mu(\mathfrak{m})$ if and only if $\dim(\widehat{R}) = \mu(\widehat{\mathfrak{m}})$. $\square$

We return to our investigation of the tensor product with the I-adic completion $\widehat{R}_I$.

Proposition 2.1.157. *Let R be a commutative unital ring. Let I be a proper ideal of R. Let $\widehat{R}_I$ be the completion of R with respect to the I-adic topology. Let M be a finitely generated R-module. Let $\widehat{M}_I$ be the completion of M with respect to the I-adic topology. The canonical R-module homomorphism $\widehat{R}_I \otimes_R M \to \widehat{M}_I$ is surjective. If R is Noetherian, this map is injective, i.e., $\widehat{R}_I \otimes_R M \cong \widehat{M}_I$.*

Proof. By hypothesis that M is a finitely generated R-module, there exists an integer $n \geq 1$ and a surjective R-module homomorphism $\varphi : R^n \to M$ that induces a short exact sequence of R-modules $0 \to \ker\varphi \xrightarrow{i} R^n \xrightarrow{\varphi} M \to 0$. By Proposition 2.1.93 and Lemma 2.1.150, we obtain the following.

$$\begin{array}{ccccccc}
\widehat{R}_I \otimes_R \ker\varphi & \xrightarrow{\tau_1} & \widehat{R}_I \otimes_R R^n & \xrightarrow{\tau_2} & \widehat{R}_I \otimes_R M & \longrightarrow & 0 \\
\downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_3} & & \\
\widehat{\ker\varphi}_I & \xrightarrow{\widehat{i}_I} & \widehat{R}_I^n & \xrightarrow{\widehat{\varphi}_I} & \widehat{M}_I & \longrightarrow & 0
\end{array}$$

Observe that π_2 is an isomorphism by the paragraph preceding Lemma 2.1.150. Each of the maps $\widehat{\varphi}_I$, π_2, and τ_2 are surjective. Commutativity of the diagram implies that $\pi_3 \circ \tau_2 = \widehat{\varphi}_I \circ \pi_2$, hence π_3 is surjective. We conclude that $\widehat{R}_I \otimes_R M \to \widehat{M}_I$ is surjective on finitely generated R-modules.

If R is Noetherian, then $\widehat{i_I}$ is injective by Proposition 2.1.151, hence the bottom row of the above diagram is exact. By the Snake Lemma, we obtain exact sequence of R-modules

$$\ker \pi_1 \to \ker \pi_2 \to \ker \pi_3 \to \operatorname{coker} \pi_1 \to \operatorname{coker} \pi_2 \to \operatorname{coker} \pi_3.$$

Considering that $\ker \pi_2$ and $\operatorname{coker} \pi_1$ are zero because π_2 is injective and π_1 is surjective, respectively, we conclude that $\ker \pi_3$ is zero so that π_3 is injective, as desired. □

Corollary 2.1.151 established that the completion of a finitely generated module over a Noetherian ring is a covariant exact functor. Our next proposition establishes the remarkable fact that the tensor product with the completion of a Noetherian ring is a covariant exact functor on any module. Consequently, the "most correct" way to obtain the completion of an arbitrary R-module is by taking the tensor product with the completion of R with respect to the appropriate topology. Before we state the result, we recall that an R-module M is **faithfully flat** if the sequence of R-modules $0 \to M \otimes_R A \to M \otimes_R B \to M \otimes_R C \to 0$ is exact if and only if $0 \to A \to B \to C \to 0$ is exact.

Proposition 2.1.158. *Let R be a Noetherian commutative unital ring. Let I be a proper ideal of R. The completion $\widehat{R}_I$ of R with respect to the I-adic topology is flat as an R-module. Even more, if $(R, \mathfrak{m})$ is a local ring, then $\widehat{R}_I$ is faithfully flat as an R-module.*

Proof. By Proposition 2.1.94, it suffices to prove that the map $\mathrm{id}_{\widehat{R}_I} \otimes_R j : \widehat{R}_I \otimes_R J \to \widehat{R}_I \otimes_R R$ induced by the inclusion $j : J \to R$ is injective for every ideal J of R. By assumption that R is Noetherian, it follows by Proposition 2.1.151 that the induced map $\widehat{j_I} : \widehat{J_I} \to \widehat{R}_I$ is injective. By Proposition 2.1.157, we have that $\pi_I : \widehat{R}_I \otimes_R J \to \widehat{J_I}$ is an isomorphism. We note also that $\tau : \widehat{R}_I \otimes_R R \to \widehat{R}_I$ is an isomorphism by Proposition 2.1.89. Combined with the observation that $\tau \circ (\mathrm{id}_{\widehat{R}_I} \otimes_R j)$ and $\widehat{j_I} \circ \pi_I$ are equal as R-module homomorphisms, these facts yield that $\mathrm{id}_{\widehat{R}} \otimes_R j$ is injective, as desired.

Conversely, assume that $\mathfrak{m}$ is the unique maximal ideal of R. By assumption that I is a proper ideal of R, it follows that $I \subseteq \mathfrak{m}$. Consequently, we have that $\mathfrak{m}/I$ is a maximal ideal of R/I, from which it follows by Proposition 2.1.148(5.) that there exists a maximal ideal $\mathfrak{M}$ of $\widehat{R}_I$ such that

$\mathfrak{M}/\ker\pi_I \cong \mathfrak{m}/I$. We conclude that $\widehat{R}_I \otimes_R (R/\mathfrak{m}) \cong \widehat{R}_I \otimes_R (\widehat{R}_I/\mathfrak{M}) \cong \widehat{R}_I/\mathfrak{M}$ is nonzero by the Third Isomorphism Theorem so that $\widehat{R}_I$ is faithfully flat by [Jon22, Lemma 10.39.15]. □

Corollary 2.1.159. *Let R be a Noetherian commutative unital ring. Let I and J be proper ideals of R. Let $\widehat{R}_I$ be the completion of R with respect to the I-adic topology. We have that $\widehat{J_I} \cong J\widehat{R}_I$.*

Proof. By Propositions 2.1.157, 2.1.158, and 2.1.94, we have that $\widehat{J_I} \cong \widehat{R}_I \otimes_R J \cong J\widehat{R}_I$. □

By the Cohen Structure Theorem, the properties of a complete Noetherian commutative unital local ring are completely determined by its dimension, residue field, and characteristic. Correctly leveraging this knowledge, one can establish the following powerful result.

Theorem 2.1.160. *[HS06, Theorem 4.3.4] If $(R,\mathfrak{m})$ is a complete Noetherian local integral domain, then its integral closure $\overline{R}$ is finitely generated as an R-module.*

Later, in the chapter on the Canonical Blow-Up of One-Dimensional Singularities, we will exclusively study the case that $(R,\mathfrak{m})$ is a one-dimensional analytically unramified commutative unital Noetherian local ring. By definition, an **analytically unramified** ring is a Noetherian local ring $(R,\mathfrak{m})$ such that $\widehat{R}_\mathfrak{m}$ is reduced (cf. the exposition preceding Proposition 2.1.53). One of the earliest equivalent characterizations of analytically unramified rings is due to Rees in 1961.

Theorem 2.1.161 (Rees)**.** *[HS06, Theorem 9.2.2] Let $(R,\mathfrak{m})$ be a Noetherian local integral domain. The following conditions are equivalent.*

(i.) *R is analytically unramified.*

(ii.) *If $R \subseteq S \subseteq \mathrm{Frac}(R)$ is a module-finite extension, then $\overline{S}$ is finitely generated as an S-module.*

By Proposition 2.1.148(2.), an analytically unramified Noetherian local ring $(R,\mathfrak{m})$ must reduced, as it is isomorphic to a subring of the reduced ring $\widehat{R}_\mathfrak{m}$. Even more, the following hold.

Proposition 2.1.162. *If $(R,\mathfrak{m})$ is an analytically unramified commutative unital Noetherian local ring, then its integral closure $\overline{R}$ is finitely generated as an R-module.*

Proof. By hypothesis that R is Noetherian, it follows that its $\mathfrak{m}$-adic completion $\widehat{R}$ is Noetherian by Proposition 2.1.148. Consequently, there are finitely many minimal prime ideals $P_1, \ldots, P_n$ of $\widehat{R}$ by Proposition 2.1.51. Even more, the integral closure of $\widehat{R}$ is isomorphic to $\overline{\widehat{R}/P_1} \times \cdots \times \overline{\widehat{R}/P_n}$ by Proposition 2.1.72. Each of the quotient rings $\widehat{R}/P_i$ is a complete Noetherian local integral domain, hence $\overline{\widehat{R}/P_i}$ is finitely generated as a $\widehat{R}/P_i$-module for each integer $1 \leq i \leq n$ by Theorem 2.1.160. Considering that $\widehat{R}$ is Noetherian, it follows that $\overline{\widehat{R}/P_i}$ is finitely generated as a $\widehat{R}$-module for each integer $1 \leq i \leq n$ so that the integral closure of $\widehat{R}$ is finitely generated as a $\widehat{R}$-module.

By Proposition 2.1.158, the inclusion $\overline{R} \subseteq Q(R)$ induces an inclusion $\widehat{R} \otimes_R \overline{R} \subseteq \widehat{R} \otimes_R Q(R)$. Considering that $R \subseteq \overline{R}$ is an integral extension of R, it follows that the induced map $\widehat{R} \to \widehat{R} \otimes_R \overline{R}$ is an integral extension of $\widehat{R}$ by Proposition 6.5.2, hence $\widehat{R} \otimes_R \overline{R}$ is a $\widehat{R}$-submodule of the integral closure of $\widehat{R}$. By the previous paragraph, the integral closure of $\widehat{R}$ is finitely generated over the Noetherian ring $\widehat{R}$, hence any $\widehat{R}$-submodule of the integral closure of $\widehat{R}$ is finitely generated as a $\widehat{R}$-submodule by Definition 2.1.18. Consequently, there exist elements $\alpha_1, \ldots, \alpha_n \in \overline{R}$ whose images in $\widehat{R} \otimes_R \overline{R}$ generated $\widehat{R} \otimes_R \overline{R}$ as a $\widehat{R}$-module. Once again, by Proposition 2.1.158, we conclude that $\alpha_1, \ldots, \alpha_n$ generate $\overline{R}$ as an R-module: indeed, the short exact sequence $\widehat{R} \otimes_R \overline{R}^{\oplus n} \to \widehat{R} \otimes_R \overline{R} \to 0$ and the faithful flatness of $\widehat{R}$ together yield a short exact sequence $\overline{R}^{\oplus n} \to \overline{R} \to 0$. □

Proposition 2.1.163. *If $(R, \mathfrak{m})$ is an analytically unramified commutative unital Noetherian local ring of dimension one, then every ideal of the integral closure of R is principal.*

Proof. If R is analytically unramified, then it is reduced; Proposition 2.1.77 yields the result. □

Before we conclude this section, we lay the groundwork for two fundamental observations regarding the interplay between a Noetherian local ring and its completion.

Proposition 2.1.164. *Let $(R, \mathfrak{m})$ be a commutative unital Noetherian local ring. If M is an R-module that has finite length over R, then M is complete with respect to the $\mathfrak{m}$-adic topology.*

Proof. By Proposition 2.1.24, there exists an integer $n \gg 0$ such that $\mathfrak{m}^n M = 0$. We conclude that $\widehat{M}_{\mathfrak{m}} = \varprojlim (M/\mathfrak{m}^n M) = M$, hence M is complete with respect to the $\mathfrak{m}$-adic topology. □

Corollary 2.1.165. *Let $(R,\mathfrak{m})$ be a commutative unital Noetherian local ring. A finite-dimensional $R/\mathfrak{m}$-vector space is complete with respect to the $\mathfrak{m}$-adic topology.*

Proof. Observe that if V is a finite dimensional $R/\mathfrak{m}$-vector space, then V has finite length as an $R/\mathfrak{m}$-module. By Proposition 2.1.26, we conclude that V has finite length as an R-module. □

2.1.7 Regular Sequences and Associated Primes

Eventually, we will extend the property of Proposition 2.1.40(4.) to a more general class of Noetherian commutative unital rings, but in order to accomplish this, we must relate the topological invariant of (Krull) dimension with some homological invariant. Unless otherwise stated, we assume throughout this section that R is a commutative unital ring and M is an arbitrary R-module.

Definition 2.1.166. We say that an element $x \in R$ is M-**regular** whenever

(i.) $xm = 0$ implies that $m = 0$ and

(ii.) $xM \neq M$.

If x only satisfies condition (i.), we say that x is **weakly** M-**regular**. We note that some authors refer to such an element as a **non-zero divisor** of M. Under this naming convention, an element $x \in R$ that does not satisfy condition (i.) of Definition 2.1.166 is called a **zero divisor** of M.

Remark 2.1.167. We note that condition (ii.) of Definition 2.1.166 is a provision to prevent the "degenerate" case. Particularly, if $M = 0$, then $xm = 0$ implies that $m = 0$ trivially, hence every element of R is M-regular for the zero module. On the other hand, every unit u of a ring satisfies $uR = R$, so we would like to restrict our attention to non-units acting on nonzero modules.

We will soon focus exclusively on the case that $(R,\mathfrak{m})$ is a local ring and M is a finitely generated R-module. If it were the case that $x \in \mathfrak{m}$ satisfies $xM = M$, it would follow by Nakayama's Lemma that $M = 0$, hence condition (i.) would be satisfied trivially. On the other hand, if $M \neq 0$, then $xM \neq M$ for any element $x \in \mathfrak{m}$ by the contrapositive of Nakayama's Lemma. Consequently, condition (ii.) in Definition 2.1.166 is satisfied by any element of $\mathfrak{m}$ (i.e., any non-unit of R).

Example 2.1.168. Every nonzero non-unit of $\mathbb{Z}$ is $\mathbb{Z}$-regular because $\mathbb{Z}$ is a domain that is not a field. In fact, this is the case with any domain that is not a field. On the other hand, for any nonzero element n of $\mathbb{Z}$, we have that $n\mathbb{Q} = \mathbb{Q}$, hence a nonzero integer is only weakly $\mathbb{Q}$-regular.

Definition 2.1.169. We say that a sequence $\underline{x} = (x_1, \ldots, x_n) \in R$ is an M-**regular sequence** if

(i.) x_1 is an M-regular element of R and

(ii.) x_{i+1} is an $M/(x_1, \ldots, x_i)M$-regular element of R for each integer $1 \leq i \leq n-1$.

Like before, we say that $\underline{x}$ is a **weakly** M-**regular** sequence if x_1 is weakly M-regular or x_{i+1} is weakly $M/(x_1, \ldots, x_i)M$-regular for some integer $1 \leq i \leq n-1$.

Unfortunately, a permutation of a (weakly) M-regular sequence may not be (weakly) M-regular.

Example 2.1.170. [BH93, Exercise 1.1.3] Consider the polynomial ring $S = k[x, y, z]$ over a field k. Observe that x is an S-regular element because it is a nonzero element of the domain S. Further, we have that $y - xy$ is an $S/(x)$-regular element because it is equal to y modulo x and $S/(x) \cong k[y, z]$. Last, we have that $z - xz$ is an $S/(x, y - xy)$-regular element because $(x, y - xy) = (x, y)$ implies that $S/(x, y - xy) \cong k[z]$ and $z - xz$ is equal to z modulo $(x, y - xy)$. We conclude therefore that $(x, y - xy, z - xz)$ is an S-regular sequence. On the other hand, the sequence $(y - xy, z - xz, x)$ is not S-regular because $(z - xz)y = z(y - xy)$ shows that $z - xz$ is not $S/(y - xy)$-regular.

If $(R, \mathfrak{m})$ is Noetherian local, then a permutation of an M-regular sequence is again M-regular.

Proposition 2.1.171. *[BH93, Proposition 1.1.6] Let $(R, \mathfrak{m})$ be Noetherian local ring. Let M be a finitely generated R-module. Any permutation of an M-regular sequence is M-regular.*

Proof. Every permutation can be realized as a product of transpositions, hence it suffices to show that (y, x) is an M-regular sequence whenever (x, y) is. Explicitly, we must show that y is not a zero divisor on M and x is not a zero divisor on M/yM. On the contrary, suppose that x is a zero divisor on M/yM. Consequently, there exists an element m in $M \setminus yM$ such that $xm = ym'$ for some element m' in M. But this implies that $ym' = 0$ in M/xM. Considering that (x, y) is an M-regular

sequence, we must have that $m' = xm''$ for some element m'' in M. Ultimately, then, we have that $xm = ym' = xym''$. Once again, by assumption that (x,y) is an M-regular sequence, we must have that $m = ym''$ — a contradiction. We conclude that x is not a zero divisor on M/yM.

We must now demonstrate that y is not a zero divisor on M. Consider the multiplication map $y\cdot : M \to M$ that sends $m \mapsto ym$ with kernel K. Our aim is to establish that $K = 0$. Given any element m in K, we claim that $m = xm'$ for some element m' in M by assumption that (x,y) is an M-regular sequence. Considering that $ym = 0$ is an element of xM, it follows that $ym = 0$ in M/xM; however, y is not a zero divisor on M/xM, so it must be the case that m is in xM. Consequently, the multiplication map $x\cdot : K \to K$ is surjective so that $K = xK = x^iK$ for all integers $i \geq 0$. We conclude that $K = 0$ by 2.1.20, as $K = \bigcap_{i\geq 0} K = \bigcap_{i\geq 0} x^iK \subseteq \bigcap_{i\geq 0} \mathfrak{m}^iK \subseteq \bigcap_{i\geq 0} \mathfrak{m}^iM = 0$. □

Before we continue, it is worth mentioning the following propositions.

Proposition 2.1.172. *Let $(R,\mathfrak{m})$ be a Noetherian local ring. If $\underline{x} = (x_1,\ldots,x_n)$ forms an R-regular sequence, then $R/\underline{x}R$ admits a finite free resolution as an R-module.*

Proof. We proceed by induction on n. If $x \in R$ is R-regular, then there exists a short exact sequence $0 \to R \xrightarrow{\cdot x} R \to R/xR \to 0$. Clearly, this is a finite free resolution of R/xR as an R-module.

We will assume inductively that the claim holds for some integer $n \geq 2$. Consider the R-regular sequence $\underline{x} = (x_1,\ldots,x_n)$. By Propositions 2.1.97 and 2.1.98, it suffices to show that $R/\underline{x}R$ has finite projective dimension as an R-module. Observe that $I = (\bar{x}_2,\ldots,\bar{x}_n)$ is generated by a $\bar{R} = R/x_1R$-regular sequence, hence $R/\underline{x}R = \bar{R}/I$ admits a finite free resolution as a $\bar{R}$-module by induction. Call this free resolution $F_\bullet : 0 \to F_n \to \cdots \to F_1 \to F_0 \to R/\underline{x}R \to 0$. Each of the free $\bar{R}$-modules F_i with $1 \leq i \leq n-1$ induces a short exact sequence $0 \to K_i \to F_i \to K_{i-1} \to 0$ of $\bar{R}$-modules, and we obtain the short exact sequences $0 \to F_n \to F_{n-1} \to K_{n-1} \to 0$ and $0 \to K_0 \to F_0 \to R/\underline{x}R \to 0$ at the left- and right-hand endpoints of $F_\bullet$. Even more, each of the free $\bar{R}$-modules F_i has finite projective dimension as an R-module by the base case of the induction: by definition, F_i is the direct sum of copies of $\bar{R} = R/x_1R$, so the direct sum of copies of a projective resolution of $\bar{R}$ as an R-module yields projective resolution of F_i as an R-module. Using Corollary 2.1.118 on the

short exact sequence $0 \to F_n \to F_{n-1} \to K_{n-1} \to 0$ shows that K_{n-1} has finite projective dimension as an R-module. By the same rationale, the short exact sequence $0 \to K_{n-1} \to F_{n-1} \to K_{n-2} \to 0$ guarantees that K_{n-2} has finite projective dimension as an R-module. Continuing in this manner, we find that $R/\underline{x}R$ has finite projective dimension as an R-module, as desired. $\square$

We have characterized nonzero elements of R whose action on any nonzero element of M results in a nonzero element of M as (weakly) M-regular (or as a non-zero divisor on M). We will now investigate those elements of R whose action on a given nonzero element of M is always zero.

Definition 2.1.173. Let M be a nonzero R-module. We define the R-**annihilator** of a nonzero element $m \in M$ as $\operatorname{ann}_R(m) = \{r \in R \mid rm = 0\}$. Often, we will refer to this simply as the annihilator of m. We define also the R-**annihilator** of the entire module M as $\operatorname{ann}_R(M) = \bigcap_{m \in M} \operatorname{ann}_R(m)$.

Observe that the annihilator of any nonzero element $m \in M$ is an ideal of R: indeed, if r and s belong to $\operatorname{ann}_R(m)$, then we have that $(r+s)m = rm + sm = 0$ and $(ar)m = a(rm) = a(0) = 0$ for all elements $a \in R$. Consequently, we may consider the case that $\operatorname{ann}_R(m)$ is a prime ideal of R.

Definition 2.1.174. Let M be a nonzero R-module. We say that a prime ideal P of R is an **associated prime** of M if there exists a nonzero element $m \in M$ such that $P = \operatorname{ann}_R(m)$.

Example 2.1.175. Let $S = k[x]$ be the univariate polynomial ring over a field k. Let $M = k[x]/(x^2)$. We will denote by $\bar{x}$ the class of x modulo x^2. Observe that $x\bar{x} = \bar{x}^2 = \bar{0}_k$, hence the ideal of S generated by x is contained in the annihilator of $\bar{x}$, i.e., $(x) \subseteq \operatorname{ann}_S(\bar{x})$. But (x) is a maximal ideal of S and $\operatorname{ann}_R(\bar{x})$ is a proper ideal of S, hence we have that $\operatorname{ann}_S(\bar{x}) = (x)$ is an associated prime of M. Observe that (x) is also a minimal prime ideal of S. We will soon see that this is no coincident.

Before we proceed, we should investigate sufficient conditions for the existence of associated primes of a nonzero module. Unfortunately, this requires additional tools that are not immediately relevant to us; instead, we state the following proposition without proof.

Proposition 2.1.176. *Every nonzero module M over a Noetherian ring R admits an associated prime. Further, if M is Noetherian, then M admits only finitely many associated primes.*

We denote by $\mathrm{Ass}_R(M)$ the collection of associated primes of a nonzero module M over a Noetherian ring R. By the previous proposition, if M is Noetherian, then $|\mathrm{Ass}_R(M)| < \infty$. Even more, the associated primes of a module and its localization are the same.

Proposition 2.1.177. *Let R be a commutative ring. Let M be an R-module M. If $P \in \mathrm{Ass}_R(M)$, then $PR_P \in \mathrm{Ass}_{R_P}(M_P)$. Conversely, if P is finitely generated and $PR_P \in \mathrm{Ass}_{R_P}(M_P)$, then $P \in \mathrm{Ass}_R(M)$.*

Proof. By Definition 2.1.174, if $P \in \mathrm{Ass}_R(M)$, then $P = \mathrm{ann}_R(m)$ for some nonzero element $m \in M$. Put another way, there exists a short exact sequence of R-modules $0 \to P \to R \to Rm \to 0$. By Proposition 6.2.4, we have that $0 \to PR_P \to R_P \to R_P \dfrac{m}{1_R} \to 0$ is exact so that $P \in \mathrm{Ass}_{R_P}(M_P)$.

Conversely, suppose that P is finitely generated and $PR_P \in \mathrm{Ass}_{R_P}(M_P)$. Consider a system of generators $x_1, \ldots, x_n$ of P. By Definition 2.1.174, there exists an element $\dfrac{m}{s}$ of M_P such that $PR_P = \mathrm{ann}_{R_P}\left(\dfrac{m}{s}\right)$. Observe that $\dfrac{x_i m}{s} = 0$ for each integer $1 \leq i \leq n$, from which it follows that there exist elements $t_1, \ldots, t_n \in R \setminus P$ such that $t_i x_i m = 0$ for each integer $1 \leq i \leq n$. Every element of P can be written as $r_1 x_1 + \cdots + r_n x_n$ for some elements $r_1, \ldots, r_n \in R$, hence we have that

$$(r_1 x_1 + \cdots + r_n x_n)(t_1 \cdots t_n m) = (r_1 t_2 \cdots t_n)(t_1 x_1 m) + \cdots + (t_1 \cdots t_{n-1} r_n)(t_n x_n m) = 0$$

and $P \subseteq \mathrm{ann}_R(t_1 \cdots t_n m)$. Considering that PR_P is a maximal ideal of R_P and $PR_P \subseteq \mathrm{ann}_{R_P}\left(\dfrac{m}{s}\right)$, equality holds. By Proposition 2.1.9, we conclude that $P = \mathrm{ann}_R(t_1 \cdots t_n m)$, i.e., $P \in \mathrm{Ass}_R(M)$. $\square$

We will now relate the associated primes of M and the M-regular elements of R.

Proposition 2.1.178. *Let R be Noetherian. Let M be an R-module. The following are equivalent.*

(i.) *The element $x \in R$ is a zero divisor on M.*

(ii.) *The element $x \in R$ belongs to some associated prime P of M.*

Put another way, the collection of zero divisors of M is the union of all associated primes of M.

Proof. Let $x \in R$ be a zero divisor on M. By Proposition 2.1.176, M admits an associated prime P. If $x = 0_R$, then x belongs to P because every ideal of R contains 0_R. We may assume that x is

nonzero. By hypothesis that x is a zero divisor on M, there exists a nonzero element $m \in M$ such that $xm = 0$, hence x belongs to $\text{ann}_R(m)$. Given that $\text{ann}_R(m)$ is prime, our proof is complete. We assume therefore that $\text{ann}_R(m)$ is not prime. By hypothesis that R is Noetherian, the collection

$$\mathfrak{A} = \{\text{ann}_R(m') \mid m' \in M, \text{ann}_R(m') \text{ is a proper ideal of } R, \text{and } \text{ann}_R(m) \subseteq \text{ann}_R(m')\}$$

has a maximal element P because it contains $\text{ann}_R(m)$ by construction. We claim that P is a prime ideal. Consider the case that some elements y and z of R satisfy $yz \in P$ and $z \notin P$. Observe that $P \subseteq \text{ann}_R(ym')$ because every element of P annihilates m' and so must annihilate ym'. On the other hand, we have that $z(ym') = (yz)m' = 0$ by assumption that $yz \in P$, hence z is an element of $\text{ann}_R(ym') \setminus P$. By the maximality of P and the fact that $\text{ann}_R(m) \subseteq \text{ann}_R(ym')$, we must have that $\text{ann}_R(ym') = R$ so that $ym' = 1_R(ym') = 0$ and y annihilates m', i.e., we have that $y \in P$. We conclude that P is an associated prime ideal of M that contains $\text{ann}_R(m)$ and x.

Conversely, if $x \in R$ belongs to some associated prime ideal P of M, then there exists a nonzero element $m \in M$ such that $xm = 0$, hence x is a zero divisor on M. □

Corollary 2.1.179. *Let R be Noetherian. Let M be an R-module. The following are equivalent.*

(1.) *The element $x \in R$ is M-regular.*

(2.) *The element $x \in R$ does not belong to any associated prime P of M.*

Corollary 2.1.180. *Let R be a Noetherian ring. Let M be an R-module. Let I be an ideal of R that consists of zero divisors of M. There exists an associated prime P of M such that $I \subseteq P$.*

Proof. We prove the contrapositive. Given that $I \not\subseteq P$ for all associated primes P of M, there exists an element $x \in I$ such that $x \notin P$ for any associated prime P by the Prime Avoidance Lemma. By Corollary 2.1.179, we conclude that x is M-regular, i.e., x is not a zero divisor on M. □

Corollary 2.1.181. *Let R be Noetherian. The total ring of fractions $Q(R)$ admits only finitely many maximal ideals; they are in bijection with the associated primes of R maximal under inclusion.*

Proof. By Proposition 2.1.11, the prime ideals of $Q(R)$ are in bijection with the prime ideals of R that consist of zero divisors of R. By Proposition 2.1.178 and Corollary 2.1.180, the prime ideals of R that consist of zero divisors of R are precisely the prime ideals of R that lie in some associated prime ideal of R. Consequently, the maximal ideals of $Q(R)$ are in bijection with the associated primes of R that are maximal under inclusion. By Proposition 2.1.176, the Noetherian ring R admits only finitely many associated primes, hence $Q(R)$ admits only finitely many maximal ideals. $\square$

One can also view the property that P is an associated prime of M as a homological condition.

Proposition 2.1.182. *Let M be a nonzero R-module. Consider the following conditions.*

(i.) *P is an associated prime of M.*

(ii.) *M contains an R-submodule that is isomorphic to R/P for some prime ideal P.*

(iii.) *There exists a nonzero R-module homomorphism $\psi : R/P \to M$ for some prime ideal P of R. Put another way, we have that $\mathrm{Hom}_R(R/P, M) \neq 0$ for some prime ideal P of R.*

We have that (i.) $\iff$ (ii.) $\implies$ (iii.). Conversely, if either (a.) P is a maximal ideal of R or (b.) the associated primes of M are the minimal primes of R, then (iii.) $\implies$ (i.).

Proof. By definition, if P is an associated prime of M, then there exists a nonzero element $m \in M$ such that $P = \mathrm{ann}_R(m)$. Consider the map $\varphi : R \to M$ defined by $\varphi(r) = rm$. One can easily verify that this is an R-module homomorphism, hence $\varphi(R)$ is an R-submodule of M. By definition, we have that $\ker \varphi = \{r \in R \mid rm = 0\} = \mathrm{ann}_R(m) = P$, and we conclude that $R/P \cong \varphi(R)$.

Conversely, if M contains an R-submodule that is isomorphic to R/P for some prime ideal P of R, then there exists an injective R-module homomorphism $\varphi : R/P \to M$. Consequently, we have that $P = \ker \varphi = \{r + P \mid r\varphi(1_R + P) = 0\} = \mathrm{ann}_R(\varphi(1_R + P))$ is an associated prime of M.

If M contains an R-submodule N such that $\varphi : R/P \to N$ is an R-module isomorphism, then the composite map $\psi : R/P \xrightarrow{\varphi} N \xrightarrow{\subseteq} M$ is a nonzero R-module homomorphism.

Last, we will assume that there exists a nonzero R-module homomorphism $\psi : R/P \to M$ for some prime ideal P of R. Recall that $\psi : R/P \to M$ is an R-module homomorphism if and only if

(a.) ψ is well-defined, i.e., $r+P = 0_R+P$ implies that $\psi(r+P) = 0$ and

(b.) ψ is R-linear, i.e., $\psi(r+P) = r \cdot \psi(1_R+P)$ for all elements $r \in R$.

Combined, these properties say that every nonzero R-linear homomorphism $R/P \to M$ is uniquely determined by the nonzero element $\psi(1_R+P) \in M$ and $\psi(1_R+P)$ must be annihilated by P. Consequently, we find that $P \subseteq \operatorname{ann}_R(\psi(1_R+P))$. Given that (a.) P is a maximal ideal of R, we conclude that $P = \operatorname{ann}_R(\psi(1_R+P))$ is an associated prime of M. On the other hand, if P is not maximal, it follows by Corollary 2.1.180 that $P \subseteq Q$ for some associated prime Q of M. Given that (b.) the associated primes of M are the minimal primes of R, we conclude that $P = Q$. □

We shall soon discuss the connection between regular sequences contained in the maximal ideal $\mathfrak{m}$ of a Noetherian local ring $(R,\mathfrak{m},k)$ and the nonzero R-linear maps $k \to M$. Before we are able to state this relationship explicitly, we investigate the deeper interplay between the M-regular elements of R contained in the annihilator of some R-module N and the R-linear maps $N \to M$.

Proposition 2.1.183. *[BH93, Proposition 1.2.3] Let M and N be R-modules. The following hold.*

(1.) *If* $\operatorname{ann}_R(N)$ *contains an M-regular element, then* $\operatorname{Hom}_R(N,M) = 0$.

(2.) *Conversely, if R is Noetherian and M and N are finitely generated, then* $\operatorname{Hom}_R(N,M) = 0$ *implies that* $\operatorname{ann}_R(N)$ *contains an M-regular element.*

Proof. (1.) Consider an R-module homomorphism $\varphi : N \to M$. For every element $n \in N$ and $x \in \operatorname{ann}_R(N)$, we have that $\varphi(xn) = \varphi(0) = 0$. Considering that φ is R-linear and x belongs to R, we have that $0 = \varphi(xn) = x\varphi(n)$. Given that x is M-regular, we have that $\varphi(n) = 0$. But this holds for every element $n \in N$, hence we conclude that φ is the zero map so that $\operatorname{Hom}_R(N,M) = 0$.

(2.) Let R be Noetherian, and let M and N be finitely generated. We will establish the contrapositive. We assume to this end that $\operatorname{ann}_R(N)$ consists of zero divisors of M. By Corollary 2.1.180, there exists an associated prime P of M such that $\operatorname{ann}_R(N) \subseteq P$. Observe that $R \setminus P \subseteq R \setminus \operatorname{ann}_R(N)$ does not contain any zero divisors of N, hence P belongs to $\operatorname{Supp}(N)$. Let k denote the residue field R_P/PR_P of the local ring (R_P, PR_P). By Nakayama's Lemma, we have that $N_P \otimes_{R_P} k \cong N_P/PN_P$

is a nonzero finite-dimensional k-vector space, hence it is isomorphic to $k^{\oplus n}$ for some integer $n \geq 1$. By forming the composite map $N_P \to N_P/PN_P \cong k^{\oplus n} \to k$, we obtain a surjective homomorphism $N_P \to k$. Observe that PR_P is an associated prime of M_P, hence there exists an element $m \in M_P$ such that $PR_P = \operatorname{ann}_{R_P}(m)$. Consequently, the multiplication map $\cdot m : R_P/PR_P \to M_P$ is a well-defined R-module homomorphism. By composition, we obtain a nonzero element of $\operatorname{Hom}_{R_P}(N_P, M_P) \cong \operatorname{Hom}_R(N,M)_P$ so that $\operatorname{Hom}_R(N,M)$ is nonzero. □

Example 2.1.184. Let $S = k[x,y]$ be the bivariate polynomial ring over a field k. Let $M = S/(x^2)$, and let $N = S/(x,y)$. Observe that x and y annihilate N, hence we have that $\operatorname{ann}_S(N) = (x,y)$. On the other hand, the element $y \in \operatorname{ann}_S(N)$ is M-regular. We conclude that $\operatorname{Hom}_S(N,M) = 0$.

Our next proposition is the basis for the proof of the main theorem of the next section.

Proposition 2.1.185. *Given any R-modules M and N and a weakly M-regular sequence $(x_1, \ldots, x_n)$ in $\operatorname{ann}_R(N)$, we have that $\operatorname{Hom}_R(N, M/(x_1, \ldots, x_n)M) \cong \operatorname{Ext}^n_R(N,M)$.*

Proof. We proceed by induction on n. Observe that $\operatorname{Ext}^0_R(N,M) \cong \operatorname{Hom}_R(N,M)$ by Proposition 2.1.110, hence the claim holds for $n = 0$. We will assume inductively that the claim holds for all integers $1 \leq i \leq n-1$. We note that x_i is an $M/(x_1, \ldots, x_{i-1})M$-regular element by hypothesis for each integer $1 \leq i \leq n$, hence Proposition 2.1.183 implies that $\operatorname{Ext}^{i-1}_R(N,M) = 0$ for each integer $1 \leq i \leq n$ by induction. By Proposition 2.1.110, the short exact sequence

$$0 \to M \xrightarrow{x_n \cdot} M \to M/x_nM \to 0$$

induces a long exact sequence of Ext. But as we observed in the previous paragraph, the lower Ext vanish by induction, hence we obtain an exact sequence that begins with

$$0 \to \operatorname{Ext}^{n-1}_R(N, M/x_nM) \xrightarrow{\psi} \operatorname{Ext}^n_R(N,M) \xrightarrow{\varphi} \operatorname{Ext}^n_R(N,M).$$

By construction, the R-modules $\operatorname{Ext}^i_R(N,-)$ preserve multiplication for all indices $i \geq 0$, hence we have that φ is multiplication by x_n. By hypothesis that x_n belongs to $\operatorname{ann}_R(N)$, we find that φ is the

zero map. We conclude that ψ is an isomorphism, i.e., $\mathrm{Ext}_R^{n-1}(N, M/x_nM) \cong \mathrm{Ext}_R^n(N,M)$. Using induction in the second equivalence, we obtain the desired result as follows.

$$\mathrm{Ext}_R^n(N,M) \cong \mathrm{Ext}_R^{n-1}(N, M/x_nM)$$

$$\cong \mathrm{Hom}_R\left(N, \frac{M/x_nM}{(x_1,\ldots,x_{n-1})M/x_nM}\right)$$

$$\cong \mathrm{Hom}_R(N, M/(x_1,\ldots,x_n)M) \qquad \square$$

2.2 Cohen-Macaulay Local Rings

2.2.1 Depth and the Cohen-Macaulay Condition

We will assume throughout this section that $(R,\mathfrak{m},k)$ is a Noetherian local ring with unique maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. We will also assume that M is a finitely generated R-module. Our next proposition illustrates the nice behavior of R and M in this setting.

Proposition 2.2.1. *Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Let M be a finitely generated R-module. The following properties hold.*

(1.) *R has finite (Krull) dimension. Further, we have that* $\dim(R) = \mathrm{ht}(\mathfrak{m})$.

(2.) *R admits finitely many associated primes. In particular, R admits an associated prime.*

(3.) *An element $x \in R$ is R-regular if and only if x does not belong to any associated prime of R.*

(4.) *M is a Noetherian R-module.*

(5.) *Every permutation of an M-regular sequence is an M-regular sequence.*

(6.) *M admits finitely many associated primes. In particular, M admits an associated prime.*

(7.) *An element $x \in R$ is M-regular if and only if x does not belong to any associated prime of M.*

(8.) *We have that* $\mathrm{Hom}_R(k,M) = 0$ *if and only if* $\mathfrak{m}$ *contains an* M*-regular element.*

(9.) *Given any* M*-regular sequence* $(x_1,\ldots,x_n) \in \mathfrak{m}$*, for all integers* $0 \leq i \leq n-1$*, we have that*

$$\mathrm{Ext}^i_R(k,M) \cong \mathrm{Hom}_R(k, M/(x_1,\ldots,x_i)M) = 0.$$

Proof. Observe that property (1.) holds by Corollary 2.1.43. Property (2.) holds by Proposition 2.1.176, and property (6.) holds by the same proposition as soon as we establish property (4.). Properties (3.) and (7.) hold by Corollary 2.1.179. Property (5.) holds by Proposition 2.1.170. Property (8.) holds by Proposition 2.1.183. Property (9.) holds by the proof of Proposition 2.1.185.

One can show that property (4.) is equivalent to the condition that M is finitely generated when R is a Noetherian ring. Explicitly, if M is finitely generated by n elements, then M is isomorphic to a quotient of the Noetherian R-module R^n, hence M is Noetherian. Conversely, if M is Noetherian, then M is finitely generated by the analog of the third condition of Definition 2.1.3. □

By hypothesis that R is Noetherian, every ascending chain of ideals of R eventually stabilizes. Consequently, we can recursively build M-regular sequences of elements in the maximal ideal $\mathfrak{m}$ of R. Observe that if $\mathfrak{m}$ is an associated prime of M, then every element $x \in \mathfrak{m}$ is a zero divisor on M. Conversely, if $\mathfrak{m}$ is not an associated prime of M, then there exists an M-regular element $x_1 \in \mathfrak{m}$. We can subsequently ask if there exists an M/x_1M-regular element $x_2 \in \mathfrak{m}$. Continuing in this way, we obtain an ascending chain of ideals $(x_1) \subseteq (x_1,x_2) \subseteq \cdots$ that must eventually stabilize. One natural question to ask of this is, "How many elements can we possibly fit in an M-regular sequence?" Our immediate task is to answer this question. We introduce the tools to do so next.

Definition 2.2.2. We say that an M-regular sequence $\underline{x} = (x_1,\ldots,x_n)$ is a **maximal M-regular sequence** if $\mathfrak{m}$ consists of zero divisors for $M/\underline{x}M$, i.e., $\mathfrak{m}$ is an associated prime of $M/\underline{x}M$.

Theorem 2.2.3 (Rees)**.** *Every maximal* M*-regular sequence in* $\mathfrak{m}$ *consists of the same number of*

terms. Particularly, this invariant is referred to as the **depth** *of M, and it is given by*

$$\operatorname{depth}(M) = \inf\{i \geq 0 \mid \operatorname{Ext}^i_R(k,M) \neq 0\}.$$

Proof. Consider a maximal M-regular sequence $\underline{x} = (x_1, \ldots, x_n)$ in $\mathfrak{m}$. By definition, each element x_{i+1} is $M/(x_1, \ldots, x_i)M$-regular for each integer $0 \leq i \leq n-1$. Consequently, we have that

$$\operatorname{Ext}^i_R(k,M) \cong \operatorname{Hom}_R(k, M/(x_1, \ldots, x_i)M) = 0$$

for each integer $0 \leq i \leq n-1$ by Proposition 2.2.1. On the other hand, by hypothesis that $\underline{x}$ is a maximal M-regular sequence in $\mathfrak{m}$, it follows that $\mathfrak{m}$ consists of zero divisors of $M/\underline{x}M$. By Corollary 2.1.180, we conclude that $\mathfrak{m}$ is an associated prime of $M/\underline{x}M$. By Proposition 2.1.182, we conclude that $\operatorname{Hom}_R(k, M/\underline{x}M) \neq 0$ so that $\operatorname{Ext}^n_R(k,M) \cong \operatorname{Hom}_R(k, M/\underline{x}M) \neq 0$. □

We refer to the k-vector space dimension of $\operatorname{Ext}^{\operatorname{depth}(M)}_R(k,M)$ as the (Cohen-Macaulay) **type** of M, denoted by $r(M) = \dim_k \operatorname{Ext}^{\operatorname{depth}(M)}_R(k,M)$. We will return to this invariant later.

Our next proposition yields a surprising formula for the injective dimension of any R-module of finite injective dimension. We omit the proof for the sake of brevity.

Theorem 2.2.4. *[BH93, Theorem 3.1.17] If* $\operatorname{injdim}_R(M) < \infty$, *then* $\operatorname{injdim}_R(M) = \operatorname{depth}(R)$.

We note the following necessary and sufficient condition for a module to have depth zero.

Corollary 2.2.5. *We have that* $\operatorname{depth}(M) = 0$ *if and only if* $\mathfrak{m}$ *is an associated prime of* M.

Proof. Observe that $\operatorname{depth}(M) = 0$ if and only if $\operatorname{Ext}^0_R(k,M) \neq 0$ if and only if $\operatorname{Hom}_R(k,M) \neq 0$ if and only if $\mathfrak{m}$ is an associated prime of M by Proposition 2.1.182. □

Corollary 2.2.6. *We have that* $\operatorname{depth}(M_P) = 0$ *if and only if* P *is an associated prime of* M.

Proof. By Corollary 2.2.5, it follows that $\operatorname{depth}(M_P) = 0$ if and only if PR_P is an associated prime of M_P if and only if P is an associated prime of M by Proposition 2.1.177. □

Example 2.2.7. Let k be a field. Let $k[\![x,y]\!]$ denote the ring of bivariate formal power series. Observe that $k[\![x,y]\!]$ is a Noetherian local ring: it is the completion of the Noetherian ring $k[x,y]$ at the homogeneous maximal ideal (x,y). Consider the Noetherian local ring $R = k[\![x,y]\!]/(x^2,xy)$. We claim that $\operatorname{depth}(R) = 0$. Each of the generators of the maximal ideal $\mathfrak{m} = (\bar{x},\bar{y})$ is a zero divisor on R, hence we conclude that $\mathfrak{m}$ is an associated prime of R and $\operatorname{depth}(R) = 0$ by Corollary 2.2.5.

Our next proposition illustrates that depth behaves well with respect to short exact sequences.

Lemma 2.2.8 (Depth Lemma)**.** *Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. For any short exact sequence of finitely generated R-modules $0 \to L \to M \to N \to 0$, the following inequalities hold.*

(1.) $\operatorname{depth}(L) \geq \min\{\operatorname{depth}(M), \operatorname{depth}(N)+1\}$

(2.) $\operatorname{depth}(M) \geq \min\{\operatorname{depth}(L), \operatorname{depth}(N)\}$

(3.) $\operatorname{depth}(N) \geq \min\{\operatorname{depth}(L)-1, \operatorname{depth}(M)\}$

Further, if $\operatorname{depth}(M) \geq \operatorname{depth}(N)+1$, *then we have that* $\operatorname{depth}(L) = \operatorname{depth}(N)+1$.

Proof. Consider a short exact sequence $0 \to L \to M \to N \to 0$ of finitely generated modules over a local ring $(R,\mathfrak{m},k)$. We have that $\operatorname{depth}(L) = \min\{i \mid \operatorname{Ext}^i_R(k,L) \neq 0\}$, hence we may apply $\operatorname{Hom}_R(k,-)$ to our short exact sequence to obtain a long exact sequence

$$0 \to \operatorname{Hom}_R(k,L) \to \operatorname{Hom}_R(k,M) \to \operatorname{Hom}_R(k,N)$$

$$\to \operatorname{Ext}^1_R(k,L) \to \operatorname{Ext}^1_R(k,M) \to \operatorname{Ext}^1_R(k,N) \to \cdots.$$

(i.) Given that $\operatorname{depth}(L) = d$, we have that $\operatorname{Ext}^d_R(k,L) \neq 0$ and $\operatorname{Ext}^i_R(k,L) = 0$ for all integers $0 \leq i \leq d-2$. Consequently, there are R-module isomorphisms $\operatorname{Ext}^i_R(k,M) \cong \operatorname{Ext}^i_R(k,N)$ for all integers $0 \leq i \leq d-1$, and the rest of our long exact sequence can be written as

$$0 \to \operatorname{Ext}^{d-1}_R(k,M) \to \operatorname{Ext}^{d-1}_R(k,N) \to \operatorname{Ext}^d_R(k,L) \to \operatorname{Ext}^d_R(k,M) \to \operatorname{Ext}^d_R(k,N) \to \cdots.$$

We claim that $\text{depth}(L) \geq \min\{\text{depth}(M), \text{depth}(N)+1\}$. On the contrary, we will assume that $\text{depth}(M) \geq \text{depth}(L)+1$ and $\text{depth}(N) \geq \text{depth}(L)$. But this implies that

$$\text{Ext}_R^{d-1}(k,M) = \text{Ext}_R^d(k,M) = 0$$

and $\text{Ext}_R^d(k,L) \cong \text{Ext}_R^{d-1}(k,N) = 0$ — a contradiction. We conclude that

$$\text{depth}(L) \geq \min\{\text{depth}(M), \text{depth}(N)+1\}.$$

We note that the other assertions are proved in a similar way. □

Even more, depth behaves well with respect to taking quotients by regular sequences.

Proposition 2.2.9. *Let $\underline{x} = (x_1, \ldots, x_n)$ be an M-regular sequence. We have that*

$$\text{depth}(M/\underline{x}M) = \text{depth}(M) - n.$$

Proof. By the proof of Proposition 2.1.185, we have that $\text{Ext}_R^i(k,M) \cong \text{Ext}_R^{i-n}(k, M/\underline{x}M)$ for all integers $i \geq n$. By hypothesis, we have that $\text{depth}(M) \geq n$, hence we conclude that

$$\begin{aligned}
\text{depth}(M) - n &= \inf\{i \geq 0 \mid \text{Ext}_R^i(k,M) \neq 0\} - n \\
&= \inf\{i - n \geq 0 \mid \text{Ext}_R^i(k,M) \neq 0\} \\
&= \inf\{i - n \geq 0 \mid \text{Ext}_R^{i-n}(k, M/\underline{x}M) \neq 0\} \\
&= \text{depth}(M/\underline{x}M),
\end{aligned}$$

where the first and last equalities hold by Theorem 2.2.3 and the third holds by isomorphism. □

Unlike with taking quotients, localizing at a prime ideal can sometimes increase depth.

Proposition 2.2.10. *Let P be a prime ideal of R. We have that*

(1.) $\text{depth}(M) \leq \dim(R/P)$ *if P is an associated prime of M and*

(2.) $\operatorname{depth}(M) \leq \dim(R/P) + \operatorname{depth}(M_P)$.

Proof. (1.) We proceed by induction on $\operatorname{depth}(M)$. Given that $\operatorname{depth}(M) = 0$, the claim holds trivially. Given that $\operatorname{depth}(M) = 1$, by Proposition 2.2.5, $\mathfrak{m}$ is not an associated prime of M, hence for any associated prime P of M, we have that $\mathfrak{m} \supsetneq P$ so that $\dim(R/P) \geq 1$, and the claim holds. Consider the case that $\operatorname{depth}(M) \geq 2$. By definition, there exists an M-regular element $x \in \mathfrak{m}$. Given an associated prime P of M, we have that $P = \operatorname{ann}_R(m)$ for some nonzero element $m \in M$, hence the collection $\mathfrak{C} = \{\operatorname{ann}_R(m) \mid m \in M \text{ is nonzero and } \operatorname{ann}_R(m) \subseteq P\}$ is nonempty. By Proposition 2.2.1(4.), M is Noetherian, hence there exists a maximal element of $\mathfrak{C}$, i.e., a maximal ideal $\operatorname{ann}_R(a)$ that is annihilated by P. On the contrary, if a belonged to xM, then there would exist a nonzero element $b \in M$ such that $a = xb$. Observe that P annihilates a, hence P annihilates xb, so P must annihilate b because x is M-regular. Consequently, we would find that $\operatorname{ann}_R(b) \subseteq P$ $\operatorname{ann}_R(a) \subsetneq \operatorname{ann}_R(b)$ — a contradiction. We conclude that a does not belong to xM, hence P annihilates $a + xM$ so that P consists of zero divisors of M/xM. By Corollary 2.1.180, P belongs to some associated prime Q of M/xM. We claim that $P \subsetneq Q$, from which it follows that

$$\dim(R/P) - 1 \geq \dim(R/Q) \geq \operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$$

by induction, and we conclude that $\operatorname{depth}(M) \leq \dim(R/P)$. Observe that $x \notin P$ by hypothesis that P annihilates m and x is M-regular, hence x belongs to $R \setminus P$ so that $(M/xM)_P = 0$ (cf. Example 2.1.39). On the other hand, as Q is an associated prime of M/xM, there exists a nonzero element $m' + xM \in M/xM$ such that $Q = \operatorname{ann}_R(m' + xM) = \{r \in R \mid rm' \in xM\}$. Consequently, for every element $s \in R \setminus Q$, we have that $sm' \notin xM$ so that $(M/xM)_Q \neq 0$. We conclude that $P \subsetneq Q$.

(2.) By convention, if $M_P = 0$, then $\operatorname{depth}(M_P)$ is infinite, and the claim holds. Our proof is also complete if $\operatorname{depth}(M) \leq \dim(R/P)$. We may assume therefore that $\operatorname{depth}(M) > \dim(R/P)$ and M_P is nonzero. Consequently, by (1.), P is not an associated prime of M, hence P cannot belong to any associated prime of M. By Corollary 2.1.180, there exists an M-regular element $x \in P$. By Proposition 2.2.9, we have that $\operatorname{depth}(M/xM) = \operatorname{depth}(M) - 1$ and $\operatorname{depth}(M_P/xM_P) = \operatorname{depth}(M_P) -$

1. By induction on $\operatorname{depth}(M)$, we conclude that $\operatorname{depth}(M) \leq \dim(R/P) + \operatorname{depth}(M_P)$. $\square$

Observe that the depth of a module measures its "homological bigness." On the other hand, the (Krull) dimension of a module measures its "topological bigness." Our immediate aim is to compare the two invariants. Before we do, we demonstrate that depth and dimension behave well with respect to taking the quotient by a regular sequence (known colloquially as "cutting down").

Definition 2.2.11. We define the (Krull) **dimension** of a module as $\dim(M) = \dim(R/\operatorname{ann}_R(M))$.

Proposition 2.2.12. *Let $\underline{x} = (x_1, \ldots, x_n)$ be an M-regular sequence. We have that*

$$\dim(M/\underline{x}M) = \dim(M) - n.$$

Proof. We omit the proof; rather, we refer the reader to the proof of Proposition 2.2.24. $\square$

Proposition 2.2.13. *We have that* $\operatorname{depth}(M) \leq \dim(M)$.

Proof. By Theorem 2.2.3, it follows that $\operatorname{depth}(M)$ is equal to the number of terms of any maximal M-regular sequence. Observe that for any maximal M-regular sequence $\underline{x} = (x_1, \ldots, x_n)$ in $\mathfrak{m}$, we have that $\dim(M/\underline{x}M) = \dim(M) - n$ by Proposition 2.2.12. By Definition 2.2.11, we have that $\dim(M/\underline{x}M) = \dim(R/\operatorname{ann}_R(M/\underline{x}M)) \geq 0$ so that $\operatorname{depth}(M) = n \leq \dim(M)$. $\square$

Our next example illustrates that this inequality may be strict.

Example 2.2.14. Let k be a field. Consider the Noetherian local ring $R = k[\![x,y]\!]/(x^2, xy)$ of Example 2.2.7. We claim that $\dim(R) = 1$. Observe that $\operatorname{ht}(x^2, xy) = \operatorname{ht}(x, xy) = \operatorname{ht}(x) = 1$ in $k[\![x,y]\!]$, hence $\dim(R) \leq \dim(k[\![x,y]\!]) - \operatorname{ht}(x^2, xy) = 2 - 1 = 1$ by Proposition 2.1.40(4.). On the other hand, $(\bar{x}, \bar{y}) \supsetneq (\bar{x})$ is a strictly descending chain of prime ideals in R so that $\dim(R) = 1 > 0 = \operatorname{depth}(R)$.

We note that Examples 2.1.175 and 2.2.7 are exemplary of a more general phenomenon.

Proposition 2.2.15. *Every minimal prime of R is an associated prime of R.*

Proof. Observe that a minimal prime ideal P of R must have $\mathrm{ht}(P) = 0$, hence we have that $\mathrm{depth}(R_P) \leq \dim(R_P) = \mathrm{ht}(P) = 0$. By Corollary 2.2.5, we have that PR_P is an associated prime of R_P, hence there exists an element r/s of R_P such that $PR_P = \mathrm{ann}_{R_P}(r/s)$. Using properties of localization, we conclude that $P = \mathrm{ann}_R(r)$ (cf. [Gat13, Proposition 6.7] for details). □

We say that an I of R is **regular** if it contains an R-regular element. Our next proposition gives a necessary and sufficient condition for regular ideals of a one-dimensional Noetherian local ring.

Proposition 2.2.16. *Let R be a one-dimensional Noetherian ring. Every regular ideal of R has finite colength. Conversely, if R is local and the unique maximal ideal of R is regular, then any ideal of finite colength must be regular.*

Proof. If I is a regular ideal of R, then there exists an R-regular element $x \in I$. By Proposition 2.2.12, we have that $\dim(R/xR) = 0$, hence R/xR is Artinian by Proposition 6.1.2. Consequently, R/xR has finite length as an R-module by Proposition 2.1.25. We note that the inclusion $xR \subseteq I$ induces a surjection $R/xR \to R/I$, hence by the additivity of length on short exact sequences, R/I has finite length as an R-module (cf. [Gat13, Proposition 3.22]). By definition, I has finite colength.

Conversely, if I has finite colength, then I is $\mathfrak{m}$-primary by Proposition 2.1.27. By hypothesis that R is Noetherian and $\mathfrak{m}$ is regular, it follows that $I \supseteq \mathfrak{m}^n$ contains an R-regular element. □

We have seen in Proposition 2.2.13 that M is at least as "topologically large" as it is "homologically large." Consequently, it is worth investigating when these two notions of size agree.

Definition 2.2.17. We say that a nonzero module M over a Noetherian local ring is **Cohen-Macaulay** if $\mathrm{depth}(M) = \dim(M)$. By convention, the zero module is Cohen-Macaulay, and a Noetherian local ring R is Cohen-Macaulay if it is Cohen-Macaulay as an R-module.

Example 2.2.18. Let k be a field. Let $S = k[\![x,y]\!]$ denote the bivariate ring of formal power series. Observe that (x,y) is an S-regular sequence, hence we have that $0 = \dim(S/(x,y)) = \dim(S) - 2$ by Proposition 2.2.12. On the other hand, we have that $2 \leq \mathrm{depth}(S) \leq \dim(S) = 2$ by Theorem 2.2.3 and Proposition 2.2.13. We conclude that $k[\![x,y]\!]$ is Cohen-Macaulay. Considering that $\mathfrak{m}$

is minimally generated by (x,y), we find that $\mu(\mathfrak{m}) = 2$, hence $k[\![x,y]\!]$ is a regular local ring by Definition 2.1.46. We will soon show that this is not a coincidence (cf. Corollary 2.2.27 for details).

Our next proposition illustrates that Cohen-Macaulay rings behave well with respect to "cutting down" by an R-regular sequence. Quite importantly, this allows us to reduce to the 0-dimensional case by taking the quotient of a Cohen-Macaulay ring by a maximal R-regular sequence.

Proposition 2.2.19. *Let $\underline{x} = (x_1, \ldots, x_n)$ be an R-regular sequence. We have that R is Cohen-Macaulay if and only if $R/\underline{x}R$ is Cohen-Macaulay.*

Proof. By Proposition 2.2.9, we have that $\operatorname{depth}(R/\underline{x}R) = \operatorname{depth}(R) - n$. By Proposition 2.2.12, we have that $\dim(R/\underline{x}R) = \dim(R) - n$. Consequently, we have that $\dim(R) = \operatorname{depth}(R)$ if and only if $\dim(R) - n = \operatorname{depth}(R) - n$ if and only if $\dim(R/\underline{x}R) = \operatorname{depth}(R/\underline{x}R)$. □

Our next proposition illustrates that the ideals of Cohen-Macaulay local rings exhibit behavior similar to the ideals of a domain that is a finitely generated algebra over a field. Particularly, Proposition 2.1.40(4.) holds for the ideals of a Cohen-Macaulay local ring.

Proposition 2.2.20. *Let $(R, \mathfrak{m}, k)$ be a Cohen-Macaulay local ring of dimension d.*

(1.) *For each prime ideal P of R, we have that R_P is Cohen-Macaulay.*

(2.) *For each prime ideal P of R, we have that* $\operatorname{ht}(P) + \dim(R/P) = \dim(R)$. *Consequently, for any ideal I of R, we have that* $\operatorname{ht}(I) + \dim(R/I) = \dim(R)$.

(3.) *We have that* $\operatorname{Ass}_R(R) = \operatorname{MinSpec}(R) = \{P \in \operatorname{Spec}(R) \mid \dim(R/P) = \dim(R)\}$.

Proof. (1.) We proceed by induction on the dimension d of R. Observe that if $d = 0$, every prime ideal of R has $\dim(R_P) = \operatorname{ht}(P) = 0$, and the claim holds by Proposition 2.2.13. We will assume the claim holds for $d-1$. Consider a strictly descending chain of prime ideals

$$\mathfrak{m} \supsetneq P_1 \supsetneq \cdots \supsetneq P_{n-1} \supsetneq P_n = P$$

of maximum length n. Observe that $\dim(R/P_1) = 1$. Certainly, the inequality $\geq$ holds by the Correspondence Theorem. On the other hand, if it were a strict inequality $>$, then we would obtain a longer strictly descending chain of prime ideals of R — a contradiction. On the other hand, we have that $\dim(R_{P_1}) \leq d-1$ because $\mathfrak{m}$ can be appended to any strictly descending chain of prime ideals contained in P_1. By Proposition 2.2.10, we find that

$$\operatorname{depth}(R_{P_1}) \geq \operatorname{depth}(R) - \dim(R/P_1) = \operatorname{depth}(R) - 1 = d - 1 \geq \dim(R_{P_1})$$

by hypothesis that R is Cohen-Macaulay. By a similar rationale (or induction on the length n), we find that $\operatorname{depth}(R_P) \geq \dim(R_P)$, and our claim holds by induction.

(2.) By part (1.), R_P is Cohen-Macaulay, from which it follows that $\dim(R_P) = \operatorname{depth}(R_P)$. By Proposition 2.1.40(3.), the inequality $\leq$ holds. Conversely, by Proposition 2.2.10, we have that $\operatorname{ht}(P) + \dim(R/P) = \dim(R_P) + \dim(R/P) = \operatorname{depth}(R_P) + \dim(R/P) \geq \operatorname{depth}(R) = \dim(R)$.

(3.) By Proposition 2.2.15, the inclusion $\supseteq$ holds. Conversely, if P is an associated prime of R, then $\operatorname{ht}(P) = \dim(R_P) = \operatorname{depth}(R_P) = 0$ by Corollary 2.2.5, hence P is a minimal prime of R. Given any minimal prime P of R, we have that $\dim(R) = \dim(R/P) + \operatorname{ht}(P) = \dim(R/P)$. □

2.2.2 Systems of Parameters and Regular Local Rings

Every ideal of a Noetherian local ring that is generated by a regular sequence can be extended to an ideal whose radical is equal to the maximal ideal. One of our main objectives in this section is to establish that for a Cohen-Macaulay local ring, the converse holds. We will assume throughout that $(R, \mathfrak{m}, k)$ is a Noetherian local ring with maximal ideal $\mathfrak{m}$, residue field $k = R/\mathfrak{m}$, and $\dim(R) = d$.

Definition 2.2.21. We say that a collection of elements $x_1, \ldots, x_d \in \mathfrak{m}$ is a **system of parameters** whenever there exists an integer $n \gg 0$ such that the ideal $I = (x_1, \ldots, x_d)$ satisfies $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$. By Proposition 2.1.41, this is equivalent to the condition that $\sqrt{I} = \mathfrak{m}$, i.e., I is $\mathfrak{m}$-primary. We refer to an ideal of R that is generated by a system of parameters as a **parameter ideal**. If the elements $x_1, \ldots, x_d$ are R-regular, moreover, we say that $(x_1, \ldots, x_d)$ is a **regular system of parameters**.

Proposition 2.2.22. *If I is a parameter ideal of R, then $\mu(I) = \dim_k(I/\mathfrak{m}I) \geq \dim(R) = d$.*

Proof. Observe that $d = \dim(R) = \mathrm{ht}(\mathfrak{m}) = \mathrm{ht}(\sqrt{I}) = \mathrm{ht}(I) \leq \mu(I)$ by Krull's Height Theorem. □

Equivalently, the quotient of R by a parameter ideal I satisfies $\dim(R/I) = 0$.

Proposition 2.2.23. *The following conditions are equivalent.*

(i.) *There exist elements $x_1, \ldots, x_d \in \mathfrak{m}$ such that $I = (x_1, \ldots, x_d)$ satisfies $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$.*

(ii.) *There exist elements $x_1, \ldots, x_d \in \mathfrak{m}$ such that $I = (x_1, \ldots, x_d)$ satisfies $\dim(R/I) = 0$.*

(iii.) *There exist elements $x_1, \ldots, x_d \in \mathfrak{m}$ such that $I = (x_1, \ldots, x_d)$ satisfies R/I is Artinian.*

Proof. We will assume first that condition (i.) holds. Consider a prime ideal P of R that contains I. Observe that $\mathfrak{m}^n \subseteq I \subseteq P$ implies that $\mathfrak{m} \subseteq P$, from which we conclude that $P = \mathfrak{m}$. Put another way, we have that $\mathrm{Spec}(R/I) = \{\mathfrak{m}/I\}$ so that $\dim(R/I) = 0$, as desired.

Conversely, suppose that condition (ii.) holds. Certainly, we have that $I \subseteq \mathfrak{m}$. On the other hand, if there were another prime ideal P of R such that $I \subseteq P \subsetneq \mathfrak{m}$, then we would obtain a strictly descending chain of ideals $\mathfrak{m}/I \supsetneq P/I$ of R/I of length one — a contradiction. We conclude that $\mathfrak{m}$ is the only prime ideal of R lying over I, hence we have that $\sqrt{I} = \mathfrak{m}$. Considering that R is Noetherian, this is equivalent to the condition that $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ by Proposition 2.1.41.

Last, condition (ii.) is equivalent to the condition that R/I is Artinian by Proposition 6.1.2. □

Our next proposition illustrates that the quotient of a ring by an ideal generated by elements of a system of parameters behaves similarly to the quotient of a ring by a regular sequence.

Proposition 2.2.24. *If $x_1, \ldots, x_i \in \mathfrak{m}$ belong to a system of parameters for R, then*

$$\dim(R/(x_1, \ldots, x_i)) = d - i.$$

Proof. We proceed by induction on i. We assume first that x_1 belongs to a system of parameters. By definition, there exist elements $y_2, \ldots, y_d \in \mathfrak{m}$ such that $I = (x_1, y_2, \ldots, y_d)$ is a parameter ideal. Let

$I' = (y_2, \ldots, y_d)$, $R' = R/x_1R$, and $\dim(R') = d'$. Observe that $R/I \cong R'/I'$, from which it follows that $\dim(R'/I') = \dim(R/I) = 0$ by Proposition 2.2.23. We conclude that I' is a parameter ideal of R', hence by Proposition 2.2.22, we must have that $d-1 \geq \mu(I') \geq \dim(R') = \dim(R/x_1R)$. Conversely, if the images of $z_1, \ldots, z_{d'} \in R$ generate a parameter ideal of R', then $x_1, z_1, \ldots, z_{d'}$ generate a parameter ideal of R. By the same rationale as before, we have that $d'+1 \geq \dim(R)$ so that $\dim(R/x_1R) \geq d-1$. We assume now that the claim holds for $i-1$. Let $x_1, \ldots, x_i$ belong to a system of parameters of R. Let $I' = (x_2, \ldots, x_i)$, and let $R' = R/x_1R$. By induction, we have that $\dim(R'/I') = \dim(R') - (i-1) = (d-1) - (i-1) = d-i$, and our proof is complete. □

We establish one of the main results of this section.

Proposition 2.2.25. *The following conditions are equivalent.*

(i.) *Every system of parameters of R is an R-regular sequence.*

(ii.) *There exists a system of parameters of R that is an R-regular sequence.*

(iii.) *R is Cohen-Macaulay.*

Proof. Clearly, condition (i.) implies condition (ii.). On the other hand, if there exists a system of parameters of R that is an R-regular sequence, then we must have that $\operatorname{depth}(R) \geq \dim(R)$. By Proposition 2.2.13, we conclude that R is Cohen-Macaulay, hence condition (ii.) implies condition (iii.). Last, we will assume that R is Cohen-Macaulay. We proceed by induction on the dimension d of R. We may assume that the claim holds for $d-1$ because the case $d = 0$ is vacuously true. Consider a system of parameters $x_1, \ldots, x_d \in \mathfrak{m}$. Observe that x_1 cannot belong to any minimal prime P of R; otherwise, we would have that $d-1 = \dim(R/x_1R) \geq \dim(R/P) = \dim(R) = d$ by Propositions 2.2.20 and 2.2.24 — a contradiction. Consequently, x_1 does not belong to any associated prime of R by Proposition 2.2.20. We conclude by Corollary 2.1.179 that x_1 is R-regular. By induction, we conclude that $(\bar{x}_2, \ldots, \bar{x}_d)$ is an R/x_1R-regular sequence, hence $(x_1, \ldots, x_d)$ is an R-regular sequence. Considering that this holds for any system of parameters, we are done. □

Recall that by Definition 2.1.46, a regular local ring $(R, \mathfrak{m}, k)$ is a Noetherian local ring for which $\dim(R) = \mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. Consequently, the maximal ideal of a regular local ring is generated by a system of parameters; moreover, it is generated by an R-regular sequence.

Proposition 2.2.26. *If $(R, \mathfrak{m})$ is a regular local ring, then $\mathfrak{m}$ is generated by an R-regular sequence.*

Proof. We proceed by induction on $d = \dim(R)$. Let $x_1 \in \mathfrak{m}$ be any minimal generator of $\mathfrak{m}$. By Proposition 2.1.144, the regular local ring R is a domain, so x_1 is a non-zero divisor of R. Because x_1 belongs to $\mathfrak{m}$, it is a non-unit, hence x_1R does not equal R and x_1 is R-regular. We conclude that $\mathfrak{m} = x_1R$ is generated by an R-regular sequence. We will assume therefore that the claim holds for $d-1$. Let $x_1, \ldots, x_d$ be a minimal system of generators of $\mathfrak{m}$. By definition, $x_1, \ldots, x_d$ is a system of parameters for $\mathfrak{m}$, hence by Proposition 2.2.24, we have that

$$\dim(\bar{R}) = \dim(R/x_1R) = d - 1 = \mu(\bar{x}_2, \ldots, \bar{x}_d) = \mu(\bar{\mathfrak{m}}).$$

Consequently, $(\bar{R}, \bar{\mathfrak{m}})$ is a regular local ring of dimension $d-1$. By induction, $(\bar{x}_2, \ldots, \bar{x}_d)$ is a $\bar{R}$-regular sequence. But x_1 is R-regular, hence $(x_1, \ldots, x_d)$ is an R-regular sequence. □

Corollary 2.2.27. *Every regular local ring is Cohen-Macaulay; the converse is not true.*

Proof. By Proposition 2.2.26, the unique maximal ideal of a regular local ring is generated by a regular sequence; such a Noetherian local ring is Cohen-Macaulay by Proposition 2.2.25.

Conversely, consider the Noetherian local ring $S = k[\![x, y]\!]/(x^2, y^2)$. Let $\bar{x}$ and $\bar{y}$ denote the class of x and y modulo (x^2, y^2). Observe that S has dimension zero, hence S is a Cohen-Macaulay local ring. Explicitly, the prime ideals of S correspond to prime ideals of $k[\![x, y]\!]$ that contain (x^2, y^2). But any such prime ideal must contain both x and y, hence the only prime ideal of S is $(\bar{x}, \bar{y})$. On the other hand, the maximal ideal of S is exactly $\bar{\mathfrak{m}} = (\bar{x}, \bar{y})$ with $\mu(\bar{\mathfrak{m}}) = 2 > 0 = \dim(S)$. □

By Proposition 2.2.24, the dimension of a Noetherian local ring modulo a subset S of a system of parameters drops by $|S|$. By the proof of Proposition 2.2.26, the quotient of a regular local ring

by a minimal generator of the maximal ideal is a regular local ring. Our next proposition illustrates that this property holds for any ideal generated by a subset of a regular system of parameters.

Proposition 2.2.28. *[BH93, Proposition 2.2.4] Let $(R,\mathfrak{m},k)$ be a regular local ring of dimension d. Let I be a proper ideal of R. The following statements are equivalent.*

(i.) *R/I is a regular local ring.*

(ii.) *I is generated by a subset of a regular system of parameters.*

Proof. Given that I is generated by a subset $\{x_1,\ldots,x_k\}$ of a (regular) system of parameters of R, it follows that $\dim(R/I) = d-k = \mu(\mathfrak{m}/I)$, hence R/I is a regular local ring.

Conversely, suppose that R/I is a regular local ring. By Proposition 2.1.144, I is a prime ideal of R. Further, we have that $\mu(\mathfrak{m}/I) = \dim(R/I) = d'$. Observe that $(\mathfrak{m}/I)^2 = (\mathfrak{m}^2+I)/I$, hence we have that $\mu(\mathfrak{m}/I) = \dim_k(\mathfrak{m}/(\mathfrak{m}^2+I))$. Consider the short exact sequence of k-vector spaces

$$0 \to \frac{I}{\mathfrak{m}^2\cap I} \xrightarrow{\varphi} \frac{\mathfrak{m}}{\mathfrak{m}^2} \xrightarrow{\psi} \frac{\mathfrak{m}}{\mathfrak{m}^2+I} \to 0$$

determined by $\varphi(x+\mathfrak{m}^2\cap I) = x+\mathfrak{m}^2$ and $\psi(x+\mathfrak{m}^2) = x+\mathfrak{m}^2+I$. By the Rank-Nullity Theorem, we have that $\dim_k(\mathfrak{m}/(\mathfrak{m}^2+I)) + \dim_k(I/(\mathfrak{m}^2\cap I)) = \dim_k(\mathfrak{m}/\mathfrak{m}^2) = \mu(\mathfrak{m}) = d$, from which it follows that $\dim_k(I/(\mathfrak{m}^2\cap I)) = d - \dim_k(\mathfrak{m}/(\mathfrak{m}^2+I)) = d-d'$. Consequently, by Nakayama's Lemma, we obtain elements $x_1,\ldots,x_{d-d'}$ of I that belong to a minimal generating set of $\mathfrak{m}$. By hypothesis that $(R,\mathfrak{m})$ is a regular local ring, it follows that $x_1,\ldots,x_{d-d'}$ belong to a regular system of parameters, hence we find that $\dim(R/(x_1,\ldots,x_{d-d'})) = d-(d-d') = d'$ by Proposition 2.2.24. On the other hand, we have that $\mu(\mathfrak{m}/(x_1,\ldots,x_{d-d'}) = d'$, hence we have that $R/(x_1,\ldots,x_{x-d'})$ is a regular local ring. Particularly, $(x_1,\ldots,x_{d-d'})$ is a prime ideal of R that is contained in the prime ideal I of R and satisfies $\dim(R/(x_1,\ldots,x_{d-d'}) = \dim(R/I)$. We conclude by the Correspondence Theorem that $I = (x_1,\ldots,x_{d-d'})$ is generated by a subset of a regular system of parameters. □

Regular local rings are in some sense the "best behaved" class of Noetherian local rings. By Corollary 2.2.27, every regular local ring is Cohen-Macaulay, but there exist Cohen-Macaulay local

rings that are not regular. Consequently, one might naturally wonder "how far" a Cohen-Macaulay local ring is from being regular. We aim to address this question in the coming sections.

We conclude this section with the following landmark result of Cohen.

Theorem 2.2.29 (Cohen Structure Theorem)**.** *[Coh46] A complete commutative unital Noetherian local ring is the homomorphic image of a complete Noetherian regular local ring. Explicitly, if $(R,\mathfrak{m},k)$ is a complete commutative unital Noetherian local ring, then one of the following holds.*

(1.) *If R contains a field, then $R \cong k[\![x_1,\ldots,x_n]\!]/I$ for some integer $n \geq 0$ and some ideal I.*

(2.) *If R has mixed characteristic $p > 0$ and $p \notin \mathfrak{m}^2$, then $R \cong C[\![x_1,\ldots,x_n]\!]/I$ for some integer $n \geq 0$ and local ring $(C,\mathfrak{n})$ that is a field or a complete discrete valuation ring with $\mathfrak{n} = pC$.*

2.2.3 Serre's Condition S_i

French mathematician Jean-Pierre Serre recognized that the depth of a finitely generated module over a Noetherian ring controls many of its nice properties (cf. [DG67, Theorem 5.8.6]).

Definition 2.2.30. We say that a finitely generated module M over a Noetherian ring R satisfies **Serre's Condition** S_i if for all prime ideals P of R, we have that $\operatorname{depth}(M_P) \geq \inf\{i, \operatorname{ht}(P)\}$.

For instance, the following observations can be made immediately.

Proposition 2.2.31. *If R satisfies Serre's Condition S_1, then $\operatorname{Ass}_R(R) = \operatorname{MinSpec}(R)$. Put another way, every associated prime ideal of R is a minimal prime ideal of R.*

Proof. By Proposition 2.2.15, the containment $\supseteq$ holds. Conversely, let P be an associated prime ideal of R. On the contrary, assume that P is not a minimal prime, i.e., $\dim(R_P) = \operatorname{ht}(P) \geq 1$. By hypothesis that R is S_1, we have that $0 = \operatorname{depth}(R_P) \geq \inf\{1, \dim(R_P)\} = 1$ — a contradiction. □

Proposition 2.2.32. *If M satisfies Serre's Condition S_n, then M_P is Cohen-Macaulay for all prime ideals P of R with $\operatorname{depth}(M_P) \leq n-1$. Conversely, if M_P is Cohen-Macaulay for all prime ideals P of R with $\operatorname{depth}(M_P) \leq n-1$, then $\operatorname{depth}(M_P) \geq \inf\{n, \dim(M_P)\}$. Particularly, if R_P is Cohen-Macaulay for all prime ideals P with $\operatorname{depth}(R_P) \leq n-1$, then R satisfies S_n.*

Proof. Given that M satisfies Serre's Condition S_n, we have that $\text{depth}(M_P) \geq \inf\{n, \dim(R_P)\}$ for all prime ideals P of R. Particularly, for any prime ideal P with $\text{depth}(M_P) \leq n-1$, we must have that $\text{depth}(M_P) \geq \dim(R_P) \geq \dim(M_P) \geq \text{depth}(M_P)$ so that M_P is Cohen-Macaulay. On the contrary, if it were the case that $\dim(R_P) \geq \text{depth}(M_P) + 1$, then we would have that $\inf\{n, \dim(R_P)\} = n$ so that $n-1 \geq \text{depth}(M_P) \geq n = \inf\{n, \dim(R_P)\}$ — a contradiction.

Conversely, if M_P is Cohen-Macaulay for all prime ideals P with $\text{depth}(M_P) \leq n-1$, then we have that $\text{depth}(M_P) = \dim(M_P)$ for all prime ideals P with $\text{depth}(M_P) \leq n-1$. Considering that a prime ideal P of R satisfies either $\text{depth}(M_P) \leq n-1$ or $\text{depth}(M_P) \geq n$, we conclude that $\text{depth}(M_P) \geq \inf\{n, \dim(M_P)\}$ for all prime ideals P of R. □

Proposition 2.2.33. *Let R be a Cohen-Macaulay ring. Let M be a finitely generated R-module. We have that M satisfies Serre's Condition S_1 if and only if $\text{Ass}_R(M) \subseteq \text{Ass}_R(R)$.*

Proof. We will assume first that $\text{Ass}_R(M) \subseteq \text{Ass}_R(R)$. Every prime ideal P of R is either an associated prime of M or not. If P is an associated prime of M, then P is an associated prime of R by assumption, hence we have that $\text{depth}(M_P) = \text{depth}(R_P) = 0$. Otherwise, P is not an associated prime of M, and we have that $\text{depth}(M_P) \geq 1$. We conclude that $\text{depth}(M_P) \geq \inf\{1, \text{depth}(R_P)\}$ for all prime ideals P of R. By hypothesis that R is Cohen-Macaulay, we conclude that M is S_1.

Conversely, if M satisfies Serre's Condition S_1, then $\text{depth}(M_P) \geq \inf\{1, \text{ht}(P)\}$ for all prime ideals P of R. Consequently, we have that $0 = \text{depth}(M_P) \geq \inf\{1, \dim(R_P)\} = \inf\{1, \text{depth}(R_P)\}$ for any associated prime P of M by Corollary 2.2.6 and hypothesis that R is Cohen-Macaulay. We conclude that $\text{depth}(R_P) = 0$, hence P is an associated prime of R so that $\text{Ass}_R(M) \subseteq \text{Ass}_R(R)$. □

We say that an R-module M is **torsion-free** if every non-zero divisor on R is a non-zero divisor on M, i.e., if $xr = 0_R$ implies that $r = 0_R$ for all elements $r \in R$, then $xm = 0$ implies that $m = 0$ for all elements $m \in M$. We provide a homological characterization of torsion-freeness next.

Proposition 2.2.34. *Let R be a commutative unital ring with total ring of fractions $Q(R)$. Let M be an R-module. We have that M is torsion-free if and only if $M \to M \otimes_R Q(R)$ is injective.*

Proof. By Proposition 6.2.7, we have that $M \otimes_R Q(R) \cong S^{-1}M$ for the multiplicatively closed subset S of R consisting of non-zero divisors of R. Consequently, we have that $M \to M \otimes_R Q(R)$ is injective if and only if $M \to S^{-1}M$ is injective. Observe that $M \to S^{-1}M$ is injective if and only if $\frac{m}{1_R} = 0$ is nonzero for every nonzero element $m \in M$ if and only if rm is nonzero for any nonzero element $m \in M$ and any non-zero divisor $r \in R$ if and only if M is torsion-free. □

Proposition 2.2.35. *Let R be a Noetherian commutative unital ring with total ring of fractions $Q(R)$. Let M be an R-module. If $\mathrm{Ass}_R(M) \subseteq \mathrm{Ass}_R(R)$, then M is torsion-free.*

Proof. On the contrary, suppose that M is not torsion-free. Consequently, there exists a non-zero divisor $r \in R$ and a nonzero element $m \in M$ such that $rm = 0$. Put another way, the ideal $\mathrm{ann}_R(m)$ of R is nonzero. By Corollary 2.1.180, there exists an associated prime Q of M such that $\mathrm{ann}_R(m) \subseteq Q$. By hypothesis, we conclude that Q is an associated prime of R containing the non-zero divisor r — a contradiction to Proposition 2.1.178. We conclude that M must be torsion-free. □

Corollary 2.2.36. *Let R be a Cohen-Macaulay ring. Every finitely generated R-module satisfying Serre's Condition S_1 is torsion-free.*

Proof. Combine Propositions 2.2.33 and 2.2.35 to obtain the desired result. □

By Proposition 2.1.86, every R-module M has a free resolution

$$F_\bullet : \cdots \xrightarrow{f_{n+1}} F_n \xrightarrow{f_n} F_{n-1} \xrightarrow{f_{n-1}} \cdots \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} M \to 0.$$

We refer to the R-module $\Omega_i = \ker f_{i-1}$ as an ith **syzygy** module of the R-module M. Over a Cohen-Macaulay local ring, every ith syzygy module satisfies Serre's Condition S_i.

Proposition 2.2.37. *Let R be a Noetherian local ring. Let Ω_i be an ith syzygy module of a finitely generated R-module (i.e., Ω_i is finitely generated). We have that $\mathrm{depth}(\Omega_i) \geq \min\{i, \mathrm{depth}(R)\}$. Even more, if R is Cohen-Macaulay, then Ω_i satisfies Serre's Condition S_i.*

Proof. We proceed by induction on i. Observe that if Ω_1 is a first syzygy, then there exists a finitely generated R-module M and an integer $n \geq 1$ such that $0 \to \Omega_1 \to R^n \to M \to 0$ is a short

exact sequence. By the Depth Lemma, it follows that $\operatorname{depth}(\Omega_1) \geq \min\{\operatorname{depth}(M)+1, \operatorname{depth}(R^n)\}$ so that $\operatorname{depth}(\Omega_1) \geq \{1, \operatorname{depth}(R)\}$ because it holds that $\operatorname{depth}(M) \geq 0$ and $\operatorname{depth}(R^n) = \operatorname{depth}(R)$.

We will assume now that the claim holds for any finitely generated ith syzygy. By definition, if Ω_{i+1} is a finitely generated $(i+1)$th syzygy, then there exists a finitely generated R-module M and positive integers $n_0, \ldots, n_i$ such that $0 \to \Omega_{i+1} \to R^{n_i} \to R^{n_{i-1}} \to \cdots \to R^{n_0} \to M \to 0$ is an exact sequence of R-modules. Consequently, there exists an ith syzygy Ω_i of M and a short exact sequence $0 \to \Omega_{i+1} \to R^{n_i} \to \Omega_i \to 0$. By the Depth Lemma and our inductive hypothesis, we conclude that $\operatorname{depth}(\Omega_{i+1}) \geq \min\{\operatorname{depth}(\Omega_i)+1, \operatorname{depth}(R^{n_i})\} \geq \min\{\min\{i, \operatorname{depth}(R)\}+1, \operatorname{depth}(R)\}$. One can readily verify that this implies that $\operatorname{depth}(\Omega_{i+1}) \geq \min\{i+1, \operatorname{depth}(R)\}$, as desired.

Last, if R is Cohen-Macaulay, then R_P is Cohen-Macaulay for all prime ideals P of R, hence we have that $\operatorname{ht}(P) = \dim(R_P) = \operatorname{depth}(R_P)$. By the above argument, we conclude that the localization of any ith syzygy at a prime ideal has depth at least $\min\{i, \operatorname{ht}(P)\}$ by Proposition 6.2.4. □

Given any element $m \in M$, we define the "evaluation at m" $\operatorname{ev}_m : \operatorname{Hom}_R(M,R) \to R$ by declaring that $\operatorname{ev}_m(\varphi) = \varphi(m)$. We say that an R-module is **reflexive** if the canonical R-module homomorphism $\psi : M \to \operatorname{Hom}_R(\operatorname{Hom}_R(M,R),R)$ defined by $\psi(m) = \operatorname{ev}_m$ is a bijection. One can show that a finitely generated reflexive module over a Noetherian ring is always a second syzygy. Further, a module is **torsionless** if and only if ψ is injective, so reflexive modules are always torsionless.

Proposition 2.2.38. *[BH93, Exercise 1.4.20(c.)] Let R be a Noetherian local ring. Every finitely generated reflexive R-module is a second syzygy module of some finitely generated R-module.*

Proof. We will henceforth write $M^* = \operatorname{Hom}_R(M,R)$. Observe that if M is a finitely generated R-module, then M^* is a finitely generated R-module by Proposition 6.4.2. Consequently, there exist finitely generated free R-modules F_0 and F_1 such that $F_1 \to F_0 \to M^* \to 0$ is an exact sequence of R-modules. By Proposition 2.1.80, if we apply the contravariant functor $\operatorname{Hom}_R(-,R)$ to this sequence, then we obtain an exact sequence of R-modules $0 \to M^{**} \to F_0^* \to F_1^*$. By assumption that M is reflexive and by Proposition 6.4.1, there is an induced exact sequence of R-modules $0 \to M \to F_0 \to F_1$. We conclude that $0 \to M \to F_0 \to F_1 \to \operatorname{coker}(F_0 \to F_1) \to 0$ is exact, hence

M is a second syzygy module of the finitely generated R-module $\operatorname{coker}(F_0 \to F_1)$. □

Combined with another criterion originally introduced by Krull, one can say even more about the structure of a finitely generated module over a Noetherian ring — especially when the module is the ring itself. We point the reader to Example 2.2.39 for a brief exposition on this idea.

Example 2.2.39. Let R be a Noetherian commutative unital ring. We say that R satisfies **Serre's Condition** R_i if R_P is a regular local ring for all prime ideals P of R with $\operatorname{ht}(P) \leq i$. Colloquially, if R satisfies R_i, then R is said to be **regular in codimension** i. Combined with Serre's Condition S_i, one can exhibit many nice properties of R given that R satisfies R_i and S_j. For instance, if R satisfies R_0 and S_1, then R is reduced. If R satisfies R_1 and S_2, then R is **normal**, i.e., R is reduced and integrally closed in its total ring of fractions $Q(R) = \left\{ \frac{r}{s} : r,s \in R \text{ and } s \text{ is a non-zero divisor of } R \right\}$.

2.2.4 Canonical Modules

We will assume throughout this section that $(R,\mathfrak{m},k)$ is a Noetherian local ring with unique maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. By Definition 2.2.11, the dimension of a finitely generated R-module M is $\dim(M) = \dim(R/\operatorname{ann}_R(M))$; the latter is at most $\dim(R)$ by Proposition 2.1.40. Previously, in Theorem 2.2.3, we established that $\operatorname{depth}(M) = \inf\{i \geq 0 \mid \operatorname{Ext}^i_R(k,M) \neq 0\}$ is a well-defined invariant that measures the maximum length of an M-regular sequence in $\mathfrak{m}$. By Proposition 2.2.13, we have that $\operatorname{depth}(M) \leq \dim(M)$. Equality holds if and only if M is Cohen-Macaulay by Definition 2.2.17. Combined, these inequalities show that $\operatorname{depth}(M) \leq \dim(M) \leq \dim(R)$. We say that a finitely generated R-module M is **maximal Cohen-Macaulay** if $\operatorname{depth}(M) = \dim(R)$. For instance, any Cohen-Macaulay local ring is a maximal Cohen-Macaulay module over itself. Generally, a finitely generated module M over a Noetherian (not necessarily local) ring R is maximal Cohen-Macaulay if M_P is maximal Cohen-Macaulay over R_P for all prime ideals P of R.

Before moving on, we provide two observations about maximal Cohen-Macaulay modules.

Proposition 2.2.40. *Let R be a (not necessarily local) integral domain. Let M be a Cohen-Macaulay R-module. If M is torsion-free, then M is maximal Cohen-Macaulay.*

Proof. By definition, if M is torsion-free, then for every nonzero element $m \in M$ and every non-zero divisor r of R, we have that rm is nonzero. By hypothesis that R is an integral domain, every nonzero element of R is a non-zero divisor of R. Consequently, we have that $rm = 0$ if and only if $r = 0_R$ or $m = 0$. We conclude that $\operatorname{ann}_R(M) = \{0_R\}$ so that $\operatorname{ann}_{R_P}(M_P) = 0$ for every prime ideal P of R and $\operatorname{depth}(M_P) = \dim(M_P) = \dim(R/\operatorname{ann}_{R_P}(M_P)) = \dim(R_P)$. □

Proposition 2.2.41. *Let R be a Cohen-Macaulay ring of positive dimension. Let M be a finitely generated R-module. If M is maximal Cohen-Macaulay, then M is torsion-free. Conversely, if $(R,\mathfrak{m})$ is local,* $\dim(R) = 1$, *and M is torsion-free, then M is maximal Cohen-Macaulay.*

Proof. We will assume first that M is maximal Cohen-Macaulay. Consequently, we have that $\operatorname{depth}(M_P) = \dim(R_P) = \operatorname{ht}(P)$ for each prime ideal P of R. We conclude that M satisfies Serre's Condition S_1, from which it follows that M is torsion-free by Corollary 2.2.36.

Conversely, suppose that $(R,\mathfrak{m})$ is local, $\dim(R) = 1$, and M is torsion-free. By the exposition at the beginning of the chapter, it suffices to show that $\operatorname{depth}(M)$ is nonzero, i.e., there exists an M-regular element $x \in \mathfrak{m}$. By hypothesis that R is Cohen-Macaulay and $\dim(R) = 1$, there exists an R-regular element $x \in \mathfrak{m}$; it is also M-regular by assumption that M is torsion-free. □

Our immediate interest is to illustrate that the maximal Cohen-Macaulay modules and the finitely generated modules of finite injective dimension over a Cohen-Macaulay local ring are "orthogonal" with respect to Ext. Crucially, this holds as a corollary of the following.

Theorem 2.2.42 (Ischebeck)**.** *[Isc69, Satz 2.6] Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Let M and N be nonzero finitely generated R-modules. If M has finite projective dimension or N has finite injective dimension, then* $\operatorname{depth}(R) - \operatorname{depth}(M) = \sup\{i \geq 0 \mid \operatorname{Ext}^i_R(M,N) \neq 0\}$.

Corollary 2.2.43. *Let $(R,\mathfrak{m},k)$ be a Cohen-Macaulay local ring. Let M and N be nonzero finitely generated R-modules. The following properties hold.*

(1.) *The R-module M is maximal Cohen-Macaulay if and only if* $\operatorname{Ext}^i_R(M,B) = 0$ *for all integers $i \geq 1$ and all finitely generated R-modules B of finite injective dimension.*

(2.) *The R-module N has finite injective dimension if and only if* $\operatorname{Ext}^i_R(A,N) = 0$ *for all integers* $i \geq 1$ *and all maximal Cohen-Macaulay R-modules A.*

Proof. (1.) By Theorem 2.2.42, we have that $\operatorname{depth}(R) - \operatorname{depth}(M) = \sup\{i \geq 0 \mid \operatorname{Ext}^i_R(M,N) \neq 0\}$ for all finitely generated R-modules B of finite injective dimension, hence the claim holds.

(2.) One direction is immediate: if N has finite injective dimension, then Theorem 2.2.42 guarantees that $\operatorname{Ext}^i_R(A,N) = 0$ for all integers $i \geq 1$ and all maximal Cohen-Macaulay R-modules A. Conversely, suppose that $\operatorname{Ext}^i_R(A,N) = 0$ for all integers $i \geq 1$ and all maximal Cohen-Macaulay R-modules A. Given any R-module M, there exists a free resolution $F_\bullet$ of M; its construction in Proposition 2.1.86 illustrates that for each free module F_i of $F_\bullet$ with $i \geq 0$, there exist R-modules K_{i-1} and K_i such that $0 \to K_i \to F_i \to K_{i-1} \to 0$ is a short exact sequence, where we adopt the notation $K_{-1} = M$. By Proposition 2.1.87, for each of these short exact sequences, there exists a long exact sequence of Ext; the form of this long exact sequence in tandem with our hypothesis that F_i is free and Proposition 2.1.110 yields isomorphisms $\operatorname{Ext}^n_R(K_i,N) \cong \operatorname{Ext}^{n+1}_R(K_{i-1},N)$ for each integer $n \geq 1$ and all integers $i \geq 0$. By the Depth Lemma, we have that K_i is maximal Cohen-Macaulay for all integers $i \geq d = \operatorname{depth}(R)$, hence by assumption, we have that $\operatorname{Ext}^n_R(K_d,N) = 0$ for all integers $n \geq 1$. Our previous isomorphism yields that $\operatorname{Ext}^{n+1}_R(K_{d-1},N) = 0$ for all integers $n \geq 1$. Continuing in this manner, we find that $\operatorname{Ext}^{n+d+1}_R(M,N) = 0$ for all integers $n \geq 1$; this holds for any R-module M, hence N has finite injective dimension by Proposition 2.1.113. □

Using their Intersection Theorem, Peskine and Szpiro proved the following conjecture for local rings that either (a.) have prime characteristic or (b.) are essentially of finite type over a field of characteristic zero (cf. [PS73]). Later, Paul C. Roberts established that the Intersection Theorem for all Noetherian local rings (cf. [Rob87]), hence we obtain the following theorem.

Theorem 2.2.44 (Bass's Conjecture of 1963)**.** *Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. If there exists a finitely generated R-module of finite injective dimension, then R is Cohen-Macaulay.*

One can also demonstrate that the converse holds as follows.

Proposition 2.2.45. *[LW12, Proposition 11.1] If $(R,\mathfrak{m},k)$ is a Cohen-Macaulay local ring, then there exists a finitely generated R-module of finite injective dimension.*

Proof. Consider a system of parameters $x_1,\ldots,x_n$ of R. By Proposition 2.2.23, the quotient ring $\bar{R} = R/\underline{x}$ of R by the parameter ideal $\underline{x} = (x_1,\ldots,x_n)$ is an Artinian local ring with unique maximal ideal $\bar{\mathfrak{m}} = \mathfrak{m}/\underline{x}$ and residue field k. By Proposition 6.6.12, the injective hull E of the residue field over $\bar{R}$ has finite length as an $\bar{R}$-module, hence it has finite length as an R-module by Proposition 2.1.26. Consequently, E is finitely generated as an R-module by Proposition 2.1.23 so that $\mathrm{Hom}_R(\bar{R},E)$ is finitely generated as an R-module by Proposition 6.4.2. By hypothesis that R is Cohen-Macaulay, the ideal $\underline{x}$ is generated by an R-regular sequence by Proposition 2.2.25, hence it has a finite free resolution $F_\bullet$ by Proposition 2.1.172. By applying the contravariant functor $\mathrm{Hom}_R(-,E)$ to $F_\bullet$, we obtain an injective resolution of $\bar{R}$ with finitely many nonzero terms. □

Combined, Bass's Conjecture of 1963 and Proposition 2.2.45 show that Cohen-Macaulayness is a necessary and sufficient condition for a Noetherian local ring to admit a finitely generated module of finite injective dimension. Consequently, we assume throughout the remainder of this section that $(R,\mathfrak{m},k)$ is a Cohen-Macaulay local ring, as our primary concern lies in the study maximal Cohen-Macaulay modules of finite injective dimension. Recall that the (Cohen-Macaulay) type of a finitely generated R-module M is $r(M) = \dim_k \mathrm{Ext}_R^{\mathrm{depth}(M)}(k,M)$, i.e., the k-vector space dimension of the first non-vanishing Ext module of k and M. By definition, if M is maximal Cohen-Macaulay, then $\mathrm{depth}(M) = \dim(R)$ so that $r(M) = \dim_k \mathrm{Ext}_R^{\dim(R)}(k,M)$. On the other hand, if M has finite injective dimension, then Theorem 2.2.4 implies that $\mathrm{injdim}_R(M) = \mathrm{depth}(R) = \dim(R)$. Ultimately, these invariants all coincide, hence $r(M)$ encodes much information. Our specific interest lies with maximal Cohen-Macaulay modules of finite injective dimension of type one.

Definition 2.2.46. Let $(R,\mathfrak{m},k)$ be a Cohen-Macaulay local ring. We say that a finitely generated R-module ω is a **canonical module** for R if ω satisfies all of the following conditions.

(1.) ω is maximal Cohen-Macaulay over R, i.e., $\mathrm{depth}(\omega) = \dim(R)$.

(2.) ω has finite injective dimension over R, i.e., $\mathrm{injdim}_R(\omega) = \mathrm{depth}(R)$.

(3.) ω has type one, i.e., $\dim_k \operatorname{Ext}_R^{\operatorname{depth}(\omega)}(k,\omega) = 1$.

By our previous exposition and Proposition 2.1.113, one can check whether a finitely generated module is a canonical module by the vanishing of its Ext modules with k in the first component.

Proposition 2.2.47 (Ext Vanishing Criterion for Canonical Modules)**.** *Let $(R,\mathfrak{m},k)$ be a Cohen-Macaulay local ring. A finitely generated R-module ω is a canonical module if and only if*

$$\operatorname{Ext}_R^i(k,\omega) \cong \begin{cases} k & \text{if } i = \dim(R) \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Definition 2.2.46, if ω is a finitely generated R-module that is a canonical module for R, then $\operatorname{depth}(\omega) = \dim(R) = \operatorname{depth}(R) = \operatorname{injdim}_R(\omega)$ and $\dim_k \operatorname{Ext}_R^{\dim(R)}(k,\omega) = 1$. By Theorem 2.2.3, we have that $\operatorname{depth}(\omega)$ is the smallest non-negative integer for which $\operatorname{Ext}_R^i(k,M)$ does not vanish. By Proposition 2.1.113, we have that $\operatorname{Ext}_R^i(k,\omega) = 0$ vanishes for all integers $i \geq \operatorname{injdim}_R(\omega) + 1$. Unravelling these details shows that $\operatorname{Ext}_R^i(k,\omega) = 0$ for all integers other than $i = \dim(R)$ and $\operatorname{Ext}_R^{\dim(R)}(k,\omega) \cong k$. Conversely, if the specified vanishing of Ext criterion is satisfied, then ω has finite injective dimension $\operatorname{depth}(\omega)$. By Theorem 2.2.4, we conclude that $\dim(R) = \operatorname{depth}(R) = \operatorname{injdim}(\omega) = \operatorname{depth}(\omega)$, i.e., ω is maximal Cohen-Macaulay of type one. □

Canonical modules always exist over Noetherian local rings of dimension zero.

Proposition 2.2.48. *Let $(R,\mathfrak{m},k)$ be a commutative unital Noetherian local ring of dimension zero. The injective hull $E(k)$ of the residue field is a canonical module for R.*

Proof. By definition, $E(k)$ is an injective R-module, hence it has finite injective dimension. By assumption that $\dim(R) = 0$, it follows that $E(k)$ is maximal Cohen-Macaulay. Last, by Proposition 6.6.12, we conclude that $E(k)$ is a finitely generated R-module of type one. □

One of the most important features of a canonical module of a Cohen-Macaulay local ring R is that it provides a duality on the category of R-modules that preserves depth and hence (maximal)

Cohen-Macaulayness. We collect this property and others in the following. We will omit the proofs of the next two theorems out of necessity, but the interested reader may look to [BH93, Section 3.3] for reference — especially [BH93, Theorems 3.3.4, 3.3.5, and 3.3.12].

Theorem 2.2.49. *Let $(R,\mathfrak{m})$ be a Cohen-Macaulay local ring that admits a canonical module ω.*

(1.) *If ω' is a canonical module for R, then there exists an R-module isomorphism $\varphi : \omega \to \omega'$. Put another way, a canonical module for R is unique up to isomorphism.*

(2.) *We have that $\mathrm{Hom}_R(\omega,\omega') \cong R$ for any canonical modules ω and ω' of R.*

(3.) *Let M be a Cohen-Macaulay R-module. Let $M^\vee = \mathrm{Ext}_R^{\mathrm{depth}(R)-\mathrm{depth}(M)}(M,\omega)$.*

  (a.) *The R-module $M^\vee$ is Cohen-Macaulay with $\mathrm{depth}(M^\vee) = \mathrm{depth}(M)$.*

  (b.) *We have that $\mathrm{Ext}_R^i(M,\omega) = 0$ for all integers $i \neq \mathrm{depth}(R) - \mathrm{depth}(M)$.*

  (c.) *We have that $(M^\vee)^\vee \cong M$, i.e., $(-)^\vee$ provides a duality on Cohen-Macaulay R-modules.*

(4.) *Let M be a maximal Cohen-Macaulay (MCM) R-module. Let $M^\vee = \mathrm{Hom}_R(M,\omega)$.*

  (a.) *The R-module $M^\vee$ is maximal Cohen-Macaulay.*

  (b.) *We have that $\mathrm{Ext}_R^i(M,\omega) = 0$ for all integers $i \geq 1$.*

  (c.) *We have that $(M^\vee)^\vee \cong M$, i.e., $(-)^\vee$ provides a duality on MCM R-modules.*

(5.) *We have that $\omega/\underline{x}\omega$ is a canonical module for $R/\underline{x}R$ for all R-regular sequences $\underline{x}$ of R.*

(6.) *We have that ω_P is a canonical module for R_P for all prime ideals P of R.*

(7.) *We have that $\widehat{\omega}_{\mathfrak{m}}$ is a canonical module for $\widehat{R}_{\mathfrak{m}}$.*

Theorem 2.2.50. *[BH93, Theorem 3.3.7] Let $(R,\mathfrak{m})$ be a Cohen-Macaulay local ring that admits a canonical module ω_R. Let $(S,\mathfrak{n})$ be a Cohen-Macaulay local ring. If there exists a local ring homomorphism $\varphi : (R,\mathfrak{m}) \to (S,\mathfrak{n})$ such that S is finitely generated as an R-module via the action $r \cdot s = \varphi(r)s$, then $\mathrm{Ext}_R^{\dim(R)-\dim(S)}(S,\omega_R)$ is a canonical module for S.*

Corollary 2.2.51. *Let $\varphi : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a module-finite extension of Cohen-Macaulay local rings. If R admits a canonical module ω_R, then $\mathrm{Hom}_R(S, \omega_R)$ is a canonical module for S.*

Proof. By Corollary 2.1.60, we find that S is integral over R. Consequently, Proposition 2.1.69 yields that $\dim(S) = \dim(R)$ so that $\dim(R) - \dim(S) = 0$. Even more, we have that $\varphi(\mathfrak{m}) \subseteq \mathfrak{n}$ by Proposition 2.1.70, hence any module-finite extension of local rings is a local ring homomorphism. By Theorem 2.2.50, we conclude that $\mathrm{Hom}_R(S, \omega_R)$ is a canonical module for S. □

Even more, if a Cohen-Macaulay local ring R admits a canonical module ω_R, then ω_R has the additional property that it "spans" the intersection between the collections of maximal Cohen-Macaulay R-modules and the finitely generated R-modules of finite injective dimension.

Proposition 2.2.52. *[LW12, Proposition 11.7] Let R be a Cohen-Macaulay local ring that admits a canonical module ω_R. Every maximal Cohen-Macaulay R-module of finite injective dimension can be written as a direct sum of finitely many copies of ω_R.*

Proof. By writing $M^\vee$ as the homomorphic image of a free R-module F by an R-module homomorphism with kernel K, we obtain a short exact sequence of R-modules $0 \to K \to F \to M^\vee \to 0$. By Theorem 2.2.49(4a.) and the Depth Lemma, we have that

$$\mathrm{depth}(R) \geq \mathrm{depth}(K) \geq \min\{\mathrm{depth}(F), \mathrm{depth}(M^\vee) + 1\} = \min\{\mathrm{depth}(R), \mathrm{depth}(R) + 1\},$$

i.e., $\mathrm{depth}(K) = \mathrm{depth}(R)$ and K is maximal Cohen-Macaulay. By applying $(-)^\vee = \mathrm{Hom}_R(-, \omega_R)$, we obtain a short exact sequence of R-modules $0 \to M \to F^\vee \to K^\vee \to 0$ by parts (4b.) and (4c.) of Theorem 2.2.49. Considering that $K^\vee$ is maximal Cohen-Macaulay and M has finite injective dimension by assumption, we conclude that $\mathrm{Ext}^1_R(K^\vee, M) = 0$ by Corollary 2.2.43. Consequently, Proposition 2.1.111 implies that the sequence $0 \to M \to F^\vee \to K^\vee \to 0$ splits so that M is a direct summand of $F^\vee$. Once again, by Theorem 2.2.49(4c.), we find that $M^\vee$ is a direct summand of the free R-module $(F^\vee)^\vee \cong F$, hence $M^\vee$ is a projective R-module by Proposition 2.1.81. Every finitely generated projective module over a local ring is free by Proposition 2.1.98; thus, $M^\vee$ is a

finitely generated free R-module, i.e., $M^\vee \cong R^n$ for some integer $n \geq 0$. Ultimately, the canonical duality of Theorem 2.2.49 yields that $M \cong (M^\vee)^\vee \cong (R^n)^\vee = \mathrm{Hom}_R(R^n, \omega_R) \cong \omega_R^n$. $\square$

We conclude this section with a discussion of two landmark results of Grothendieck. Unless otherwise mentioned, we will return to our initial assumption of this section that $(R, \mathfrak{m}, k)$ is a Noetherian local ring. Given any R-module M, we define the $\mathfrak{m}$-**torsion submodule**

$$\Gamma_\mathfrak{m}(M) = \{x \in M \mid \mathfrak{m}^k x = 0 \text{ for some integer } k \geq 1\}.$$

One can readily verify that $\Gamma_\mathfrak{m}(M)$ is a nonempty subset of M that is closed under addition and closed under multiplication by elements of R, hence $\Gamma_\mathfrak{m}(R)$ is an R-submodule of M, and the terminology is justified. Even more, if $\varphi : M \to N$ is an R-module homomorphism, then the induced map $\Gamma_\mathfrak{m}(\varphi) : \Gamma_\mathfrak{m}(M) \to \Gamma_\mathfrak{m}(N)$ that sends $x \mapsto \varphi(x)$ is a well-defined R-module homomorphism: indeed, if $x \in \Gamma_\mathfrak{m}(M)$, then there exists an integer $k \geq 1$ such that $\mathfrak{m}^k x = 0$, hence we have that $\mathfrak{m}^k \varphi(x) = \varphi(\mathfrak{m}^k x) = \varphi(0) = 0$ by assumption that φ is an R-module homomorphism. Observe that for any R-module homomorphisms $\varphi : M \to N$ and $\psi : M \to N$, the induced map on the $\mathfrak{m}$-torsion submodules satisfies $\Gamma_\mathfrak{m}(\varphi + \psi) = \Gamma_\mathfrak{m}(\varphi) + \Gamma_\mathfrak{m}(\psi)$. Put another way, $\Gamma_\mathfrak{m}(-)$ is **additive** on maps.

Proposition 2.2.53. *Let $(R, \mathfrak{m}, k)$ be a commutative unital Noetherian local ring. The map $\Gamma_\mathfrak{m}(-)$ that sends an R-module M to its $\mathfrak{m}$-torsion submodule $\Gamma_\mathfrak{m}(M)$ and sends an R-module homomorphism $\varphi : M \to N$ to the R-module homomorphism $\Gamma_\mathfrak{m}(\varphi) : \Gamma_\mathfrak{m}(M) \to \Gamma_\mathfrak{m}(N)$ defined by $x \mapsto \varphi(x)$ is an additive covariant left-exact functor on the category of R-modules.*

Proof. By the paragraph preceding the statement of the proposition, we conclude that $\Gamma_\mathfrak{m}(-)$ is an additive covariant functor on the category of R-modules. Consider a short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$. By definition of the functor $\Gamma_\mathfrak{m}(-)$, it follows immediately that the induced map $\Gamma_\mathfrak{m}(\alpha)$ is injective and $\mathrm{img}\,\Gamma_\mathfrak{m}(\alpha) \subseteq \ker \Gamma_\mathfrak{m}(\beta)$ by our respective assumptions that α is injective and $\mathrm{img}\,\alpha \subseteq \ker \beta$. Consequently, it suffices to show that $\ker \Gamma_\mathfrak{m}(\beta) \subseteq \mathrm{img}\,\Gamma_\mathfrak{m}(\alpha)$. Observe that if $b \in \ker \Gamma_\mathfrak{m}(\beta)$, then $b \in \ker \beta$ so that $b = \alpha(a)$ for some element $a \in A$. On the other

hand, there exists an integer $k \geq 1$ such that $0 = \mathfrak{m}^k b = \mathfrak{m}^k \alpha(a) = \alpha(\mathfrak{m}^k a)$. Considering that α is injective, we conclude that $\mathfrak{m}^k a = 0$ so that $a \in \Gamma_{\mathfrak{m}}(A)$ and $b = \alpha(a) \in \operatorname{img} \Gamma_{\mathfrak{m}}(\alpha)$, as desired. $\square$

Given any R-module M, Proposition 2.1.109 guarantees the existence of an injective resolution $Q^\bullet : 0 \to M \to Q^0 \xrightarrow{q^0} Q^1 \xrightarrow{q^1} \cdots \xrightarrow{q^n} Q^{n+1} \xrightarrow{q^{n+1}} \cdots$ of M. Consider the induced cochain complex

$$\Gamma_{\mathfrak{m}}(Q^\bullet) : 0 \to \Gamma_{\mathfrak{m}}(Q^0) \xrightarrow{\Gamma_{\mathfrak{m}}(q^0)} \Gamma_{\mathfrak{m}}(Q^1) \xrightarrow{\Gamma_{\mathfrak{m}}(q^1)} \cdots \xrightarrow{\Gamma_{\mathfrak{m}}(q^n)} \Gamma_{\mathfrak{m}}(Q^n) \xrightarrow{\Gamma_{\mathfrak{m}}(q^{n+1})} \cdots .$$

We define the **local cohomology** modules $H^i(\Gamma_{\mathfrak{m}}(Q^\bullet)) \cong \ker \Gamma_{\mathfrak{m}}(Q^i) / \operatorname{img} \Gamma_{\mathfrak{m}}(Q^{i-1})$ for each integer $i \geq 0$. Conventionally, these are written as $H^i_{\mathfrak{m}}(M)$. they are independent of the choice of an injective resolution of M. By [Rot09, Theorem 6.37 and Proposition 6.40], the local cohomology functors $H^i_{\mathfrak{m}}(-)$ are the right-derived functors of the $\mathfrak{m}$-torsion functors $\Gamma_{\mathfrak{m}}(-)$, and the local cohomology modules $H^i_{\mathfrak{m}}(M)$ are independent of the choice of injective resolution of M.

Before we illustrate the many desirable properties of the local cohomology modules, we need an observation in the form of a lemma. We will reference without construction the **direct limit** of the direct system $\{\operatorname{Hom}_R(R/\mathfrak{m}^k, M)\}_{k \geq 0}$ of R-modules under inclusion, but we invite the reader to review the exposition following [Rot09, Example 5.22] for a thorough investigation of the object.

Lemma 2.2.54. *Let $(R, \mathfrak{m}, k)$ be a commutative unital Noetherian local ring. Let M be an R-module. We have that $\Gamma_{\mathfrak{m}}(M) \cong \varinjlim \operatorname{Hom}_R(R/\mathfrak{m}^k, M)$.*

Proof. Consider the R-modules $(0 :_M \mathfrak{m}^k) = \{x \in M \mid \mathfrak{m}^k x = 0\}$ for each integer $k \geq 1$. Clearly, we have that $(0 :_M \mathfrak{m}^k) \subseteq (0 :_M \mathfrak{m}^\ell)$ for all integers $\ell \geq k$, hence we have that $\Gamma_{\mathfrak{m}}(M) \cong \varinjlim (0 :_M \mathfrak{m}^k)$, where the latter is the direct limit of the direct system $\{(0 :_M \mathfrak{m}^k)\}_{k \geq 0}$ under inclusion. By the proof of Proposition 2.1.182, we may identify the R-modules $\operatorname{Hom}_R(R/\mathfrak{m}^k, M)$ and $(0 :_M \mathfrak{m}^k)$. Consequently, there are injective R-module homomorphisms $i_{\ell,k} : \operatorname{Hom}_R(R/\mathfrak{m}^k, M) \to \operatorname{Hom}_R(R/\mathfrak{m}^\ell, M)$ for all integers $\ell \geq k$. Under this identification, it holds that $\Gamma_{\mathfrak{m}}(M) \cong \varinjlim \operatorname{Hom}_R(R/\mathfrak{m}^k, M)$. $\square$

Proposition 2.2.55. *Let $(R, \mathfrak{m}, k)$ be a commutative unital Noetherian local ring.*

(1.) *The R-modules $H^i_{\mathfrak{m}}(M)$ are Artinian for each integer $i \geq 0$. Particularly, for each integer $i \geq 0$, we have that $H^i_{\mathfrak{m}}(M)$ has finite length over R and must therefore be finitely generated.*

(2.) *We have that $H^i_{\mathfrak{m}}(M) = 0$ for all $i \leq -1$ and $H^0_{\mathfrak{m}}(M) \cong \Gamma_{\mathfrak{m}}(M)$ for all R-modules M.*

(3.) *We have that $H^i_{\mathfrak{m}}(Q) = 0$ for all $i \geq 1$ and all injective R-modules Q.*

(4.) *Every short exact sequences of R-modules $0 \to M' \to M \to M'' \to 0$ induces an exact sequence $\cdots \to H^{i-1}_{\mathfrak{m}}(M'') \to H^i_{\mathfrak{m}}(M') \to H^i_{\mathfrak{m}}(M) \to H^i_{\mathfrak{m}}(M'') \to H^{i+1}_{\mathfrak{m}}(M') \to \cdots$.*

(5.) *For any R-module M and any integer $i \geq 0$, we have that*

$$H^i_{\mathfrak{m}}(M) \cong \varinjlim \mathrm{Ext}^i_R(R/\mathfrak{m}^k, M).$$

Proof. Each of the properties (1.), (2.), (3.), and (4.) is purely functorial and holds by the general theory of right-derived functors (cf. [Rot09, Section 6.2.3]). Last, for any injective resolution $Q^\bullet$ of M, it holds that $\varinjlim \mathrm{Ext}^i_R(R/\mathfrak{m}^k, M) \cong \varinjlim H^i(\mathrm{Hom}_R(R/\mathfrak{m}^k, Q^\bullet))$ by definition of the Ext modules, where $H^i(\mathscr{C})$ denotes the ith cohomology module of the chain complex $\mathscr{C}$. By [Rot09, Proposition 5.33], the direct limit is an exact functor, hence the cohomology modules commute with the direct limit, i.e., we have that $\varinjlim H^i(\mathrm{Hom}_R(R/\mathfrak{m}^k, Q^\bullet)) \cong H^i(\varinjlim \mathrm{Hom}_R(R/\mathfrak{m}^k, Q^\bullet))$ by [Iye+07, Exercise 4.34]. We note that the direct system consisting of the chain complexes $\mathrm{Hom}_R(R/\mathfrak{m}^k, Q^\bullet)$ and the chain maps $\partial_{\ell,k}$ such that $\partial^i_{\ell,k}$ is the R-module homomorphism induced by the isomorphisms $\mathrm{Hom}_R(R/\mathfrak{m}^k, Q^i) \cong (0 :_{Q^i} \mathfrak{m}^k)$ and the inclusions $(0 :_{Q^i} \mathfrak{m}^k) \subseteq (0 :_{Q^i} \mathfrak{m}^\ell)$ for every pair of integers $\ell \geq k$ yields an isomorphism of chain complexes $\varinjlim \mathrm{Hom}_R(R/\mathfrak{m}^k, Q^\bullet) \cong \Gamma_{\mathfrak{m}}(Q^\bullet)$ by Lemma 2.2.54. Ultimately, we conclude that $H^i(\varinjlim \mathrm{Hom}_R(R/\mathfrak{m}^k, Q^\bullet) \cong H^i(\Gamma_{\mathfrak{m}}(Q^\bullet)) = H^i_{\mathfrak{m}}(M)$. □

Out of a desire for simplicity, we state the following facts without proof.

Proposition 2.2.56. *[BH93, Proposition 3.5.4] Let $(R, \mathfrak{m})$ be a Noetherian local ring. Let M be a finitely generated R-module.*

(1.) *We have that $H^i_{\mathfrak{m}}(M) = 0$ if and only if $i \leq \mathrm{depth}(M) - 1$.*

(2.) *We have that* $H^i_{\mathfrak{m}}(M) \cong H^i_{\mathfrak{m}}(M) \otimes_R \widehat{R} \cong H^i_{\mathfrak{m}\widehat{R}}(\widehat{M})$ *for all integers* $i \geq 0$, *where* $\widehat{R}$ *and* $\widehat{M}$ *denote the completions of* R *and* M *with respect to the* $\mathfrak{m}$*-adic topology.*

Theorem 2.2.57 (Grothendieck's Vanishing Theorem)**.** *Let* $(R, \mathfrak{m})$ *be a Noetherian local ring. Let* M *be a finitely generated* R*-module.*

(1.) *We have that* $H^i_{\mathfrak{m}}(M) = 0$ *for all integers* $i \leq \operatorname{depth}(M) - 1$ *and* $i \geq \dim(M) + 1$.

(2.) *Both of the* R*-modules* $H^{\operatorname{depth}(M)}_{\mathfrak{m}}(M)$ *and* $H^{\dim(M)}_{\mathfrak{m}}(M)$ *are nonzero.*

Theorem 2.2.58 (Grothendieck's Local Duality Theorem)**.** *[BH93, Theorem 3.5.8] Let* $(R, \mathfrak{m}, k)$ *be a complete Cohen-Macaulay local ring with canonical module* ω_R. *Let* $E(k)$ *be the injective hull of the residue field. For any finitely generated* R*-module* M *and any integer* $i \geq 0$, *we have that*

$$H^i_{\mathfrak{m}}(M) \cong \operatorname{Hom}_R(\operatorname{Ext}^{\dim(R)-i}_R(M, \omega_R), E(k)) \text{ and}$$
$$\operatorname{Ext}^i_R(M, \omega_R) \cong \operatorname{Hom}_R(H^{\dim(R)-i}_{\mathfrak{m}}(M), E(k)).$$

Remark 2.2.59. Grothendieck's Local Duality Theorem generalizes to any Cohen-Macaulay local ring that admits a canonical module ω_R. Essentially, this is because the completion with respect to the $\mathfrak{m}$-adic topology does not alter the local cohomology modules, and it behaves well with respect to Ext and taking the injective hull of the residue field, as well (cf. [BH93, Corollary 3.5.9]).

We conclude this section by using the above facts to show that the completion with respect to the $\mathfrak{m}$-adic topology preserves and detects the Cohen-Macaulay property.

Proposition 2.2.60. *Let* $(R, \mathfrak{m})$ *be a Noetherian local ring. The following are equivalent.*

(i.) R *is Cohen-Macaulay.*

(ii.) $\widehat{R}_{\mathfrak{m}}$ *is Cohen-Macaulay.*

Proof. By Corollary 2.1.155, we have that $\dim(R) = \dim(\widehat{R}_{\mathfrak{m}})$. By the third part of Proposition 2.2.56, it follows that $H^i_{\mathfrak{m}}(R)$ is nonzero if and only if $H^i_{\mathfrak{m}\widehat{R}_{\mathfrak{m}}}(\widehat{R}_{\mathfrak{m}})$ is nonzero. By Grothendieck's

Vanishing Theorem, if R is Cohen-Macaulay, then $H^i_{\mathfrak{m}\widehat{R}_\mathfrak{m}}(\widehat{R}_\mathfrak{m})$ is nonzero if and only if $i = \dim(\widehat{R}_\mathfrak{m})$. By the second part of Proposition 2.2.56, we conclude that $\dim(\widehat{R}_\mathfrak{m}) - 1 \leq \operatorname{depth}(\widehat{R}_\mathfrak{m}) - 1$ so that $\widehat{R}_\mathfrak{m}$ is Cohen-Macaulay. We omit the proof of the converse, as it holds analogously. □

2.2.5 Gorenstein Local Rings

We say that a Noetherian local ring is **Gorenstein** if any of the following conditions holds.

Theorem 2.2.61. *[BH93, Theorem 3.2.10] Let R be a Noetherian local ring. The following conditions are equivalent.*

(i.) *R has finite injective dimension as an R-module.*

(ii.) *R is Cohen-Macaulay, and the Cohen-Macaulay type of R is one.*

Example 2.2.62. By Example 2.1.47, a field k is a regular local ring, hence k is a Cohen-Macaulay local ring by Corollary 2.2.27. Even more, we have that $\operatorname{Hom}_k(k,k) \cong k$ is nonzero by Proposition 2.1.78, hence k has Cohen-Macaulay type one. We conclude that every field is Gorenstein.

Consequently, a Gorenstein local ring is Cohen-Macaulay, but the converse may not hold.

Example 2.2.63. Consider the Noetherian local ring $S = \mathbb{C}[\![x,y]\!]/(x,y)^2$. Let $\bar{x}$ denote the image of x in S. Observe that the unique prime ideal of S is $\mathfrak{m} = (\bar{x},\bar{y})$, hence $0 \leq \operatorname{depth}(S) \leq \dim(S) = 0$ and S is Cohen-Macaulay; however, $\operatorname{Ext}_S^{\operatorname{depth}(S)}(S/\mathfrak{m}, S) = \operatorname{Hom}_S(S/\mathfrak{m}, S) \cong (0 :_S \mathfrak{m})$ is spanned by $\{\bar{x},\bar{y}\}$ as a $\mathbb{C}$-vector space, hence we have that $r(S) = \dim_\mathbb{C} \operatorname{Hom}_S(\mathbb{C}, S) = 2 > 1$.

Completion with respect to the $\mathfrak{m}$-adic topology preserves and detects the Gorenstein property.

Proposition 2.2.64. *Let $(R,\mathfrak{m})$ be a Noetherian local ring. The following are equivalent.*

(i.) *R is Gorenstein.*

(ii.) *$\widehat{R}_\mathfrak{m}$ is Gorenstein.*

Proof. By Proposition 2.2.60, we have that R is Cohen-Macaulay if and only if $\widehat{R}_{\mathfrak{m}}$ is Cohen-Macaulay. By Propositions 6.4.4 and 2.1.165, we conclude that $\dim_k \operatorname{Ext}_R^{\operatorname{depth}(R)}(k,R) = 1$ if and only if $\dim_k \operatorname{Ext}_R^{\operatorname{depth}(\widehat{R}_{\mathfrak{m}})}(k,\widehat{R}_{\mathfrak{m}}) = 1$. Ultimately, Theorem 2.2.61 yields the result. □

Over a Gorenstein local ring, one can establish that a finitely generated module has finite projective dimension if and only if it has finite injective dimension (cf. [BH93, Exercise 3.1.25]). Conversely, Foxby demonstrated that a Noetherian local ring that admits a finitely generated module of finite projective dimension and finite injective dimension must be Gorenstein (cf. [Fox72]).

Theorem 2.2.65 (Foxby)**.** *Let R be a Noetherian local ring. The following are equivalent.*

(i.) *R is a Gorenstein local ring.*

(ii.) *There exists an R-module that has finite projective dimension and finite injective dimension.*

Other than the above, one of the primary reasons to study Gorenstein local rings is that they are directly related with the Cohen-Macaulay local rings that admit canonical modules.

Theorem 2.2.66. *[BH93, Theorem 3.3.6] Let R be a Cohen-Macaulay local ring. The following conditions are equivalent.*

(i.) *R admits a canonical module.*

(ii.) *R is the homomorphic image of a Gorenstein local ring.*

Consequently, any Gorenstein local ring admits a canonical module; in fact, the canonical module of a Gorenstein local ring is especially simple, as our next theorem illustrates.

Theorem 2.2.67. *[BH93, Theorem 3.3.7] Let R be a Cohen-Macaulay local ring that admits a canonical module ω_R. The following statements are equivalent.*

(i.) *R is a Gorenstein local ring.*

(ii.) *We have that $\omega_R \cong R$ as R-modules.*

Corollary 2.2.68. *Let R be a Cohen-Macaulay local ring that admits a canonical module ω_R. The following statements are equivalent.*

(i.) *R is a Gorenstein local ring.*

(ii.) *We have that $\omega_R \cong R^n$ as R-modules for some integer $n \geq 1$.*

Proof. By Theorem 2.2.67, it suffices to prove that (ii.) implies (i.). By Definition 2.2.46, the canonical module ω_R has finite injective dimension. Consequently, if $\omega_R \cong R^n$ for some integer $n \geq 1$, then R^n has finite injective dimension so that R has finite injective dimension over R by Corollary 2.1.114. By Theorem 2.1.113, we conclude that R is Gorenstein. □

Under certain conditions, the canonical module ω_R of Cohen-Macaulay local ring R can be identified with an ideal of R — provided that ω_R exists. We refer to ω_R as a **canonical ideal** of R if this is the case. One family of Cohen-Macaulay local rings for which this holds are the **generically Gorenstein** local rings for which R_P is Gorenstein for all minimal prime ideals P of R.

Proposition 2.2.69. *[BH93, Proposition 3.3.18] Let $(R, \mathfrak{m})$ be a Cohen-Macaulay local ring that admits a canonical module ω_R. The following conditions are equivalent.*

(1.) *The R-module ω_R has a rank.*

(2.) *The rank of the R-module ω_R is one.*

(3.) *R is generically Gorenstein.*

If any of these conditions holds, then ω_R is isomorphic to an ideal Ω_R of R that is either equal to R or has height one. If the latter holds, then R/Ω_R is a Gorenstein local ring.

Proof. Let P be a minimal prime ideal of R. By Definition 2.1.49, we have that $\dim(R_P) = 0$, hence R_P is an Artinian local ring by Proposition 6.1.2. By Proposition 6.3.11, if ω_R has a rank, then $\omega_{R_P} \cong (\omega_R)_P$ is a free R_P-module for every minimal prime ideal P of R. Even more, we have that ω_{R_P} is a canonical module for R_P by Theorem 2.2.49. Considering that the injective hull E of

the residue field R_P/PR_P of the Artinian local ring R_P is a canonical module for R_P by Proposition 2.2.48, we must have that $\omega_{R_P} \cong E$ by Theorem 2.2.49. On the other hand, the injective hull of a domain is indecomposable by Corollary 6.6.11, hence $(\omega_R)_P$ must have rank one for all minimal prime ideals P of R. By Proposition 6.3.11, we conclude that $\operatorname{rank}(\omega_R) = 1$.

By Proposition 6.3.11, if $\operatorname{rank}(\omega_R) = 1$, then $\omega_{R_P} \cong (\omega_R)_P$ is a free R_P-module of rank one for all minimal prime ideals P of R. We conclude that R_P is generically Gorenstein by Theorem 2.2.67.

Last, if R is generically Gorenstein, then R_P is Gorenstein for all minimal prime ideals P of R so that $(\omega_R)_P \cong \omega_{R_P} \cong R_P$ for all minimal prime ideals P of R. By Proposition 2.2.20, the associated and the minimal prime ideals of the Cohen-Macaulay local ring R coincide, hence $(\omega_R)_P$ is a free R_P-module for all associated prime ideals P of R. By Proposition 6.3.11, ω_R has a rank.

Consequently, if any of the above conditions holds, then $\omega_R \otimes_R Q(R) \cong Q(R)$ for the total ring of fractions $Q(R)$ by definition of rank (cf. the section The Total Ring of Fractions of the appendix). By Proposition 2.2.41, the maximal Cohen-Macaulay module ω_R is torsion-free, hence there exists an injective R-module homomorphism $\omega_R \to \omega_R \otimes_R Q(R)$ by Proposition 2.2.34; the composition $\omega_R \to \omega_R \otimes_R Q(R) \cong Q(R)$ is also injective. By definition, ω_R is a finitely generated R-module, so its image in $Q(R)$ is finitely generated over $Q(R)$. Clearing the denominator of any element of the image of ω_R in $Q(R)$ yields an element of $Q(R)$ that is the isomorphic image of an element of R by Proposition 6.3.1. Considering that the product of non-zero divisors is a non-zero divisor and the non-zero divisors of R are invertible in $Q(R)$, it follows that "clearing the denominators" is an isomorphism of ω_R onto an R-submodule of $Q(R)$, hence ω_R is isomorphic to an ideal Ω_R of R.

Last, we will demonstrate that $\operatorname{ht}(\Omega_R) = 1$ and that R/Ω_R is Gorenstein. Observe that our proof is complete if $\Omega_R = R$, hence we may assume that Ω_R is a proper ideal of R. Considering that $\Omega_R \cong \omega_R$ as R-modules and the latter has rank one, it follows that Ω_R has rank one. By Proposition 6.3.12, we find that Ω_R contains a non-zero divisor x of R; it must be a non-unit by assumption that Ω_R is a proper ideal of R, hence Ω_R satisfies $\operatorname{ht}(\Omega_R) \geq \operatorname{ht}(xR) = 1$ by Proposition 2.2.15. Conversely, the short exact sequence of R-modules $0 \to \Omega_R \to R \to R/\Omega_R \to 0$ implies that $\operatorname{depth}(R/\Omega_R) \geq \min\{\operatorname{depth}(R) - 1, \operatorname{depth}(\Omega_R)\} = \min\{\operatorname{depth}(R) - 1, \operatorname{depth}(\omega_R)\} = \operatorname{depth}(R) - 1$

by the Depth Lemma and the fact that ω_R is maximal Cohen-Macaulay. By assumption that R is Cohen-Macaulay, the previous two inequalities respectively yield that $\operatorname{depth}(R/\Omega_R) \geq \dim(R) - 1$ and $\dim(R) - 1 \geq \dim(R) - \operatorname{ht}(\Omega_R) \geq \dim(R/\Omega_R)$ by Proposition 2.2.20, from which we conclude that $\dim(R) - 1 \leq \operatorname{depth}(R/\Omega_R) \leq \dim(R/\Omega_R) \leq \dim(R) - 1$ by Proposition 2.2.13 so that $\operatorname{ht}(\Omega_R) = 1$ and R/Ω_R is Cohen-Macaulay. By Proposition 2.1.87, we obtain a short exact sequence

$$0 \to \operatorname{Hom}_R(R/\Omega_R, \Omega_R) \to \operatorname{Hom}_R(R, \Omega_R) \to \operatorname{Hom}_R(\Omega_R, \Omega_R) \to \operatorname{Ext}^1_R(R/\Omega_R, \Omega_R)$$

by applying $\operatorname{Hom}_R(-, \Omega_R)$ to the short exact sequence $0 \to \Omega_R \to R \to R/\Omega_R \to 0$. Observe that $\operatorname{Ext}^1_R(R, \Omega_R)$ is zero by Proposition 2.1.110, hence the map $\operatorname{Hom}_R(\Omega_R, \Omega_R) \to \operatorname{Ext}^1_R(R/\Omega_R, \Omega_R)$ is surjective. Elsewhere, we have that $\operatorname{Hom}_R(R, \Omega_R) \cong \Omega_R$ and $\operatorname{Hom}_R(\Omega_R, \Omega_R) \cong R$ by Proposition 2.1.78 and Theorem 2.2.49, respectively. Even more, we have that $\operatorname{Hom}_R(R/\Omega_R, \Omega_R) = 0$ by Proposition 2.1.183. Combined, the observations of this paragraph yield $\operatorname{Ext}^1_R(R/\Omega_R, \Omega_R) \cong R/\Omega_R$, from which we conclude that R/Ω_R is Gorenstein by Theorems 2.2.50 and 2.2.67. □

Conversely, a Cohen-Macaulay local ring with a canonical ideal is generically Gorenstein.

Proposition 2.2.70. *Let R be a Cohen-Macaulay local ring. If R admits a canonical ideal ω_R, then R is generically Gorenstein.*

Proof. We may assume that ω_R is a proper ideal of R. We must establish that R_P is Gorenstein for every minimal prime ideal P of R. Consider the short exact sequence $0 \to \omega_R \to R \to R/\omega_R \to 0$. By Propositions 6.2.4 and 6.2.10, we obtain a short exact sequence $0 \to \omega_{R_P} \to R_P \to R_P/\omega_{R_P} \to 0$ for any minimal prime ideal P of R. Observe that ω_{R_P} is a canonical ideal for the zero-dimensional ring R_P, and every nonzero finitely generated R_P-module is maximal Cohen-Macaulay. By Theorem 2.2.49, we have that $\operatorname{Ext}^i_{R_P}(R_P/\omega_{R_P}, \omega_{R_P}) = 0$ for all integers $i \geq 1$. By Proposition 2.1.111, it follows that ω_{R_P} is a direct summand of the free R_P-module R_P, hence ω_{R_P} is a projective R_P-module by Proposition 2.1.81. Considering that R_P is a Noetherian local ring, we conclude that ω_{R_P} is a free R_P-module by Proposition 2.1.98 so that R_P is Gorenstein by Proposition 2.2.68. □

Later, in our discussion on Canonical Blow-Up of One-Dimensional Singularities, we will devote specific attention to the case that R is a one-dimensional Cohen-Macaulay local ring with a canonical ideal ω_R. Our next proposition illustrates two desirable properties of ω_R.

Proposition 2.2.71. *Let R be a Cohen-Macaulay local ring. If R admits a canonical ideal ω_R, then ω_R is a regular ideal. Even more, if $\dim(R) = 1$, then ω_R has finite colength.*

Proof. We may assume that ω_R is a proper ideal of R. By Proposition 2.2.70, it follows that R is generically Gorenstein, hence ω_R has rank one by Proposition 2.2.69. We conclude that ω_R contains a non-zero divisor x of R by Proposition 6.3.12. By assumption that ω_R is a proper ideal, x must be a non-unit, hence x is R-regular and ω_R is a regular ideal of R. By Proposition 2.2.16, in a one-dimensional Noetherian local ring, every regular ideal has finite colength. □

Proposition 2.2.72. *Let R be a one-dimensional Cohen-Macaulay local ring that admits a canonical module ω_R. If ω_R is reflexive, then R is Gorenstein.*

Proof. By Proposition 2.2.38, if ω_R is reflexive, then there exist positive integers m and n and a finitely generated R-module M such that $0 \to \omega_R \to R^m \to R^n \to M \to 0$ is an exact sequence of R-modules. Consequently, if we let $K = \ker(R^n \to M)$, then there exist short exact sequences of R-modules $0 \to \omega_R \to R^m \to K \to 0$ and $0 \to K \to R^n \to M \to 0$. By the Depth Lemma, we have that $\operatorname{depth}(K) \geq \min\{\operatorname{depth}(R), \operatorname{depth}(M) + 1\} = \min\{\operatorname{depth}(R), 1\} = 1$. Conversely, by the exposition at the beginning of the section on Canonical Modules, we have that $\operatorname{depth}(K) \leq \dim(R) = 1$. We conclude that K is a maximal Cohen-Macaulay module. By Theorem 2.2.49, we have that $\operatorname{Ext}^i_R(K, \omega_R) = 0$ and $\operatorname{Ext}^i_R(R^m, \omega_R) = 0$ for all integers $i \geq 1$. By applying the left-exact functor $\operatorname{Hom}_R(-, \omega_R)$ to our first sequence above and using Proposition 2.1.87, we obtain a short exact sequence of R-modules $0 \to \operatorname{Hom}_R(K, \omega_R) \to \operatorname{Hom}_R(R^m, \omega_R) \to \operatorname{Hom}_R(\omega_R, \omega_R) \to 0$. Once again, by Theorem 2.2.49, $\operatorname{Hom}_R(\omega_R, \omega_R) \cong R$ is a projective R-module, hence we have that $\operatorname{Hom}_R(R^m, \omega_R) \cong \operatorname{Hom}_R(\omega_R, \omega_R) \oplus \operatorname{Hom}_R(K, \omega_R)$ by Propositions 2.1.81 and 2.1.111. Each of the direct summands is maximal Cohen-Macaulay by Theorem 2.2.49, hence we may apply

$\mathrm{Hom}_R(-,\omega_R)$ to conclude that $R^m \cong \omega_R \oplus K$. Consequently, we find that ω_R is a projective R-module. By Corollary 2.1.99, ω_R is free, hence R is Gorenstein by Corollary 2.2.68. $\square$

Until now, we have dealt explicitly with Noetherian local rings throughout this section; however, one can define a notion of a non-local Gorenstein ring. Explicitly, we say that a Noetherian ring R is Gorenstein if R_P is a Gorenstein local ring for each prime ideal P of R. We use this to provide next a crucial characterization of one-dimensional generically Gorenstein rings.

Theorem 2.2.73. *[HK71] Let $(R,\mathfrak{m})$ be a one-dimensional Cohen-Macaulay local ring with total ring of fractions $Q(R)$ and $\mathfrak{m}$-adic completion $\widehat{R}$. The following statements are equivalent.*

(i.) *$Q(\widehat{R})$ is Gorenstein.*

(ii.) *R possesses a canonical module ω_R such that $\omega_R \subseteq R$, hence ω_R is a canonical ideal.*

Particularly, if R is analytically unramified (i.e., $\widehat{R}$ is reduced), then R has a canonical ideal.

Proof. We will assume first that $Q(\widehat{R})$ is a Gorenstein ring. By definition, for each prime ideal P of $Q(\widehat{R})$, we have that $Q(\widehat{R})_P$ is a Gorenstein local ring. By the proof of Corollary 2.1.11, the prime ideals of $Q(\widehat{R})$ are in bijection (via the localization map) with the prime ideals of $\widehat{R}$ that lie in some associated prime ideal of $\widehat{R}$. Consequently, for each associated prime ideal P of $\widehat{R}$, we have that $Q(\widehat{R})_P \cong \widehat{R}_P$ by the proof of Corollary 6.2.6. By Theorem 2.2.67, for each associated prime ideal P of $\widehat{R}$, there exists a canonical module $\omega_{Q(\widehat{R})_P}$ for $Q(\widehat{R})_P$ such that $\omega_{Q(\widehat{R})_P} \cong Q(\widehat{R})_P \cong \widehat{R}_P$. By assumption that R is a Cohen-Macaulay local ring, it follows that $\widehat{R}$ is a Cohen-Macaulay local ring by Proposition 2.2.60 and Corollary 2.1.149, hence the associated prime ideals of $\widehat{R}$ are precisely the minimal prime ideals of $\widehat{R}$ by Proposition 2.2.20. Ultimately, we conclude by Proposition 2.2.69 that $\widehat{R}$ is generically Gorenstein, hence $\widehat{R}$ admits a canonical ideal $\Omega_{\widehat{R}}$. If $\Omega_{\widehat{R}} = \widehat{R}$, then $\widehat{R}$ is Gorenstein so that R is Gorenstein by Proposition 2.2.64, hence we may assume that $\Omega_{\widehat{R}}$ is a proper ideal of $\widehat{R}$. Observe that the ideal $\Omega_{\widehat{R}} \cap R$ of R satisfies $\Omega_{\widehat{R}} \cong (\Omega_{\widehat{R}} \cap R)\widehat{R}$ because the canonical ideal of $\widehat{R}$ is $\mathfrak{m}\widehat{R}$-primary by Proposition 2.1.27, hence $\Omega_{\widehat{R}} \cap R$ is a canonical ideal for R.

Conversely, suppose that R admits a canonical ideal ω_R. Observe that $\omega_R\widehat{R}$ is a canonical ideal for $\widehat{R}$ by Theorem 2.2.49 and Proposition 2.1.159, hence $\widehat{R}$ is generically Gorenstein by Proposition

2.2.70. We conclude that $\widehat{R}_P \cong (\omega_R \widehat{R})_P = \omega_R \widehat{R}_P$ is a canonical module for $\widehat{R}_P$ for every associated prime ideal P of R. By the first paragraph, $Q(\widehat{R})_P$ is Gorenstein for each prime ideal P of $Q(\widehat{R})$.

Last, suppose that R is analytically unramified. By definition and Proposition 2.2.60, we have that $\widehat{R}$ is a reduced Cohen-Macaulay local ring, hence $Q(\widehat{R})$ is isomorphic to a finite direct product of fields by Proposition 2.1.57. By Proposition 2.1.10, every localization of $Q(\widehat{R})$ at a prime ideal is a field. By Example 2.2.62, a field is Gorenstein, hence $\widehat{Q}(R)$ is Gorenstein by definition. □

2.3 Graph Theory

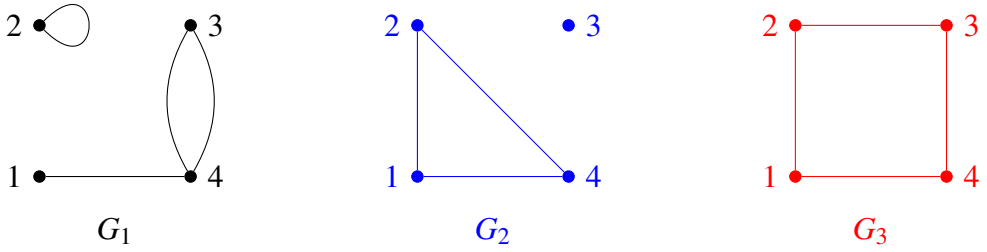
2.3.1 Basic Properties and Invariants of Graphs

Given a set V and a set E consisting of (possibly repeated) unordered pairs of elements of V, the pair $G = (V, E)$ is a **graph**. We refer to members of V as **vertices**; the elements of E are called **edges**. Edges of the form $\{v, v\}$ are called **loops**, and any edge that appears more than once in E is a **multiple edge**. Graphs that have neither loops nor multiple edges are said to be **simple**.

Unless otherwise stated, we will assume throughout this section that V is a nonempty set. Given a vertex v, if there exists a vertex w such that $\{v, w\}$ is an edge, then we say that v is an **endpoint** of the edge $\{v, w\}$ or that v is **adjacent** to the vertex w or that the edge $\{v, w\}$ is **incident** to the vertices v and w. Each vertex of a graph G possesses a unique **degree** that is equal to the number of vertices to which it is adjacent (or equivalently, the number of edges that are incident to it). Certainly, a vertex can possess degree zero if it is not an endpoint of any edge. We refer to such a vertex as an **isolated** vertex. Graphs that admit no isolated vertices are called **connected**. We say that G is a **finite graph** if V is finite, and we identify V with $[n] = \{1, 2, \ldots, n\}$ such that $n = |V|$.

Given any two graphs $G = (V(G), E(G))$ and $H = (V(H), E(H))$, a **graph isomorphism** is a bijection $f : V(G) \to V(H)$ such that $\{v, w\}$ is an edge of G if and only if $\{f(v), f(w)\}$ is an edge of H. Put another way, it is an "edge-preserving" bijection of the vertex sets of G and H.

Example 2.3.1. Below are three examples of non-isomorphic finite graphs on four vertices.

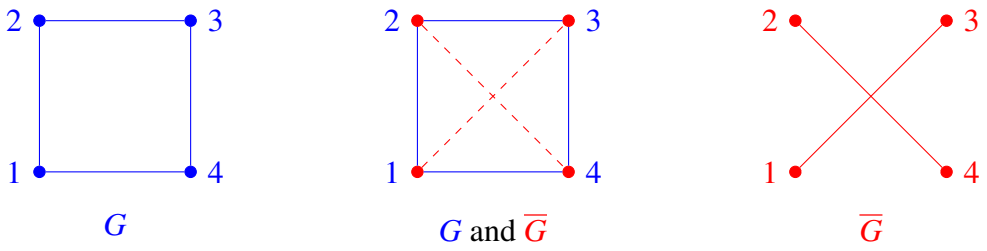


Observe that the graph G_1 is not simple because $\{2,2\}$ is a loop and $\{3,4\}$ is a multiple edge; however, both of the graphs G_2 and G_3 are simple. One can distinguish between them because 3 is an isolated vertex of G_2, but G_3 is connected. Last, the degree of each vertex of G_3 is two.

Given any set $V' \subseteq V$, one may consider the **induced subgraph** $G[V']$ obtained by taking all vertices in V' and all edges of G with the property that both endpoints lie in V'. Even more, if there exists a sequence of vertices $(v_1, v_2, \ldots, v_n)$ of G such that $\{v_i, v_{i+1}\}$ is an edge for each integer $1 \leq i \leq n-1$ and $\{v_1, v_n\}$ is an edge, we say that the induced subgraph $G[V']$ on $V' = \{v_1, v_2, \ldots, v_n\}$ is an **induced cycle** of length n. Observe that in Example 2.3.1, the induced subgraph $G_2[V']$ on $V' = \{1,2,4\}$ is the blue triangle; it is an induced cycle of length three. We say that a graph G is **chordal** if there are no induced cycles in G with length four or more.

Computing an induced subgraph is merely one way of obtaining a new graph from one that is given. Let G be a simple graph on the vertex set V. We define the **complement graph** $\overline{G}$ as the simple graph on the vertex set V with an edge $\{i, j\}$ if and only if $\{i, j\}$ is not an edge of G. Put another way, if we realize the graph G pictorially in blue, then the complement graph $\overline{G}$ is obtained by drawing all of missing edges of G in red. Our next example illustrates this.

Example 2.3.2. Below is a finite simple graph and its complement graph.

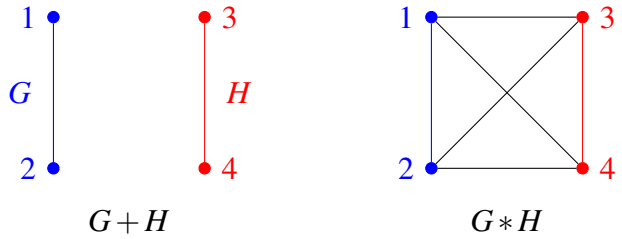


Crucially, the complement of an induced subgraph of G is the induced subgraph of $\overline{G}$ on the appropriate vertex set. Explicitly, for any set $V' \subseteq V$ and any elements $v, w \in V'$, we have that $\{v, w\}$ is an edge of $G[V']$ if and only if $\{v, w\}$ is an edge of G if and only if $\{v, w\}$ is not an edge of $\overline{G}$ if and only if $\{v, w\}$ is not an edge of $\overline{G}[V']$, from which it follows that $(G[V'])^c = \overline{G}[V']$.

If G and H are two graphs on the respective disjoint vertex sets $V(G)$ and $V(H)$, their **graph union** is the graph $G+H$ with vertices $V(G) \cup V(H)$ and edges $E(G) \cup E(H)$. Pictorially, the graph union $G+H$ is G and H sitting beside one another in the plane. Because of this simple description, many of the graph invariants we will soon describe behave predictably for the graph join.

Essentially, the graph union $G+H$ is the "least connected" graph on the vertex set $V(G) \cup V(H)$ that possesses all edges of both G and H. Conversely, the **graph join** $G * H$ of G and H is the graph with vertices $V(G) \cup V(H)$ and edges $E(G) \cup E(H) \cup \{\{i, j\} \mid i \in V(G) \text{ and } j \in V(H)\}$. Put another way, the graph join $G * H$ is obtained pictorially by placing G and H next to one another in the plane and drawing all edges between a vertex of G and a vertex of H; it is in this sense the "most connected" graph on the vertex set $V(G) \cup V(H)$ that possesses all edges of both G and H.

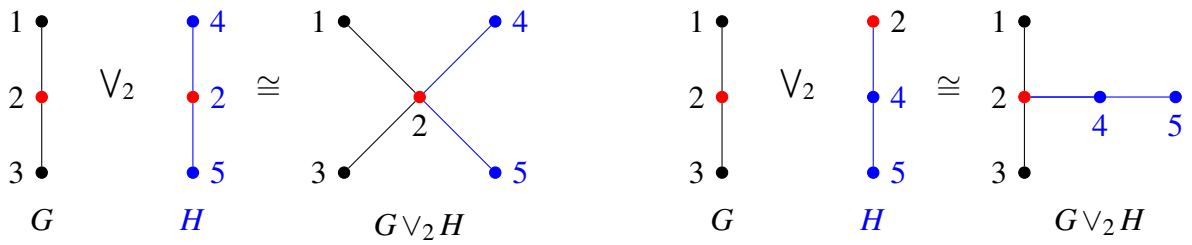
Example 2.3.3. Below are two simple graphs on disjoint vertex sets, their union, and their join.



$G+H$ $\qquad$ $G*H$

Last, we may obtain a new graph by "gluing" two given graphs along a common vertex. Let G and H be any graphs on the respective vertex sets $V(G)$ and $V(H)$ such that $V(G) \cap V(H) = \{v\}$. We define the **wedge graph** $G \vee_v H$ with respect to v as the graph with vertices $V(G) \cup V(H)$ and edges $E(G) \cup E(H)$. Generally, the vertex v determines $G \vee_v H$ because for any labeling of the vertices of G, the wedge graph $G \vee_v H$ depends upon the labeling of the vertices of H.

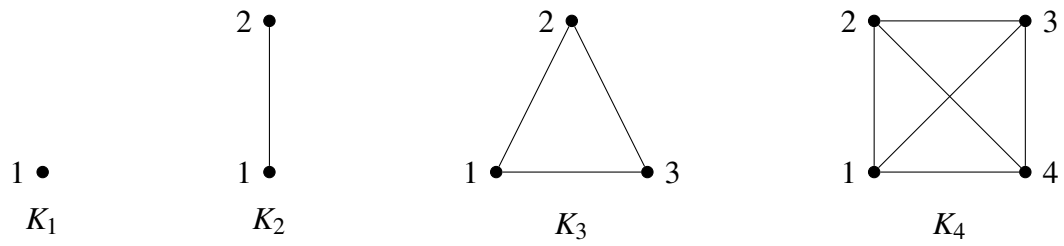
Example 2.3.4. Below are two non-isomorphic graphs that are obtained by wedging together two graphs G and H but with different labelings of H each time.



Observe that in the wedge graph $G \vee_v H$ with respect to v, the degree of v in $G \vee_v H$ is equal to the sum of the degree of v in G and the degree of v in H. Consequently, we distinguish the two wedge graphs in the previous example by the degree of the wedge vertex: in the labeling of H on the left-hand side, the wedge vertex has degree two, but in the labeling of H on the right-hand side, the wedge vertex has degree one. On the other hand, if for any pair of vertices v and w of G, there exists a graph automorphism $f : G \to G$ such that $w = f(v)$, then we say that G is **vertex-transitive**. Crucially, the wedge graph of two vertex-transitive graphs is independent of the wedge vertex. Even more, each of the vertices of a vertex-transitive graph must possess the same degree. We refer to a graph whose vertices have common degree d as d-**regular**.

Given a simple graph G on n vertices, the maximum degree of a vertex v is $n-1$: this occurs precisely when v is adjacent to all other vertices of G. Consequently, the degree of each vertex of any "maximally connected" simple graph on n vertices must be $n-1$, hence it is $(n-1)$-regular. By the Handshaking Lemma, such a graph must possess $\binom{n}{2} = \frac{n(n-1)}{2}$ edges. We refer to any $(n-1)$-regular simple graph on n vertices as a **complete graph**. Considering that any two vertices of a complete graph are adjacent, every labeling of the vertices of a complete graph induces a graph automorphism. Because of this, we distinguish the unique (up to labeling of the vertices) $(n-1)$-regular simple graph on n vertices as the complete graph K_n on n vertices.

Example 2.3.5. Below are the complete graphs on $n = 1, 2, 3$, and 4 vertices.



If $Q \subseteq V$ is nonempty and $G[Q]$ is isomorphic to the complete graph $K_{|Q|}$, we say that Q is a **clique**. Put another way, a nonempty set of vertices Q is a clique if and only if for any vertices $i, j \in Q$, the pair $\{i, j\}$ is an edge of G. Certainly, any edge of a graph forms a clique. Example 2.3.1 illustrates that $Q = \{1, 2, 4\}$ is a clique of G_2. Cliques are preserved under graph isomorphism, hence the **clique number** $\omega(G) = \max\{|Q| : Q \text{ is a clique of } G\}$ is a well-defined graph invariant.

Conversely, we say that a nonempty set $I \subseteq V$ forms an **independent vertex set** if for any vertices $i, j \in I$, the pair $\{i, j\}$ is not an edge of G. Consequently, a nonempty set of vertices I is an independent vertex set of G if and only if I is a clique of $\overline{G}$. Observe that in Example 2.3.1, the set $I = \{1, 3\}$ is an independent vertex set of G_3. By our previous discussion, we may define the **independence number** $\alpha(G) = \max\{|I| : I \text{ is an independent vertex set of } G\} = \omega(\overline{G})$.

Considering that an independent vertex set seeks to avoid edges, it is natural to ask for a collection C of vertices for which every edge of G is incident to some vertex in C. Explicitly, we say that a nonempty set $C \subseteq V$ is a **vertex cover** of G if for any edge $\{i, j\}$ of G, we have that either $i \in C$ or $j \in C$. Even more, if $C \setminus \{v\}$ is not a vertex cover for any vertex $v \in C$, then we say that C is a **minimal vertex cover** Like before, vertex covers are preserved under graph isomorphism, so we may consider the **vertex cover number** $\tau(G) = \min\{|C| : C \text{ is a vertex cover of } G\}$.

Our next proposition demonstrates the connection among these invariants.

Proposition 2.3.6. *[Wes00, Lemma 3.1.21] If G is a graph on n vertices, then $\alpha(G) + \tau(G) = n$.*

Every graph G admits a collection of edges $X \subseteq E(G)$ such that every vertex of G is incident to some edge of X. We refer to such a collection of edges as a **vertex edge cover** of G. Generalizing this to cliques of larger size yields the notion of a **vertex clique cover**, i.e., a collection of cliques $Q_1, \ldots, Q_k$ such that $V(G) = \cup_{i=1}^{k} Q_i$. Considering that the set of edges $E(G)$ is a trivial vertex clique cover of G and cliques are preserved under graph isomorphism, the **vertex clique cover number** $\theta(G) = \min\{X \mid X \text{ is a vertex clique cover of } G\}$ is a well-defined invariant of G.

Given a graph G, a sequence $(v_1, v_2, \ldots, v_{n+1})$ of distinct vertices of G is called a **path** of length n whenever there exist edges $\{v_i, v_{i+1}\}$ for each integer $1 \leq i \leq n$. Given any two vertices v and w of G, the shortest path between v and w is the path $(v_1, v_2, \ldots, v_{n+1})$ such that $v_1 = v$, $v_{n+1} = w$,

and $n = \min\{k \mid \text{there exists a path of length } k \text{ from } v \text{ to } w\}$; its length $d(v,w)$ is unique. Given any vertex v of G, the maximum length of a shortest path in G that begins with v is the **eccentricity** $\varepsilon(v) = \max\{d(v,w) \mid w \in V(G)\}$ of v. We refer to the maximum eccentricity of any vertex of G as the **diameter** $\delta(G)$ of G. Put another way, we have that $\delta(G) = \max\{\varepsilon(v) \mid v \in V(G)\}$.

Generalizing the notion of a finite simple graph is that of a **simplicial complex** Δ. We say that Δ is a simplicial complex on the vertex set $[n] = \{1,2,\ldots,n\}$ if Δ is a nonempty subset of $2^{[n]}$ such that for every pair $\sigma, \tau \in 2^{[n]}$ with $\tau \subseteq \sigma$, if σ belongs to Δ, then τ belongs to Δ. Put another way, Δ is closed under taking subsets. We note that the familiar geometric objects of line segments, triangles, and tetrahedra are simplicial complexes. We will return to this in the next section.

2.3.2 The Edge Ring of a Finite Simple Graph

Crucially, for any field k, the collection of finite simple graphs on the vertex set $[n]$ is in bijection with the collection of quadratic squarefree monomials ideals of the polynomial ring $k[x_1,\ldots,x_n]$.

$$\{G = ([n],E) \mid G \text{ is simple}\} \leftrightarrow \{I \subseteq k[x_1,\ldots,x_n] \mid I \text{ is a squarefree quadratic monomial ideal}\}$$
$$G \mapsto I(G) = (x_i x_j \mid \{i,j\} \text{ is an edge of } G)$$

Consequently, the properties of any quadratic squarefree monomial ideal of $k[x_1,\ldots,x_n]$ are intimately connected with that of the corresponding simple graph on n vertices.

Every simple graph on n vertices gives rise to a quotient of a polynomial ring in n variables. Explicitly, for a field k, a simple graph $G = (V,E)$ on n vertices can be related to the quotient ring $k(G) = k[x_1,\ldots,x_n]/I(G)$ by the squarefree monomial ideal $I(G) = (x_i x_j \mid (i,j) \in E)$. We refer to $I(G)$ as the **edge ideal** of G and to $k(G)$ as the **edge ring** of G. Likewise, every simplicial complex on n vertices induces a quotient of a polynomial ring in n variables. For simplicity, we use the same residue field k. Explicitly, we define the **Stanley-Reisner ring** $k[\Delta] = k[x_1,\ldots,x_n]/I_\Delta$, where

$$I_\Delta = (x_{i_1}x_{i_2}\cdots x_{i_k} \mid \{i_1,i_2,\ldots,i_k\} \subseteq 2^{[n]} \setminus \Delta)$$

is the **Stanley-Reisner ideal** of $k[x_1,\ldots,x_n]$ generated by the monomials corresponding to subsets of $2^{[n]}$ that do not belong to Δ. Often, the elements of Δ are referred to as **faces**, hence I_Δ is generated by monomials corresponding to non-faces of Δ. We do not assume that all of the integers of $[n]$ correspond to vertices of Δ, hence it is possible that x_i belongs to I_Δ for some integer $1 \leq i \leq n$ so that $k[\Delta]$ is a quotient of a polynomial ring in fewer than n variables.

Using the definition of independent vertex set, one can readily verify that for a finite graph G, the set Δ_G consisting of the independent vertex sets of G is a simplicial complex, eponymously called the **independence complex** of G. Our next theorem shows that the edge ideal of G and the Stanley-Reisner ideal of Δ_G are equal. Consequently, the so-called Stanley-Reisner theory can be employed to understand properties of the edge ring $k(G)$ and vice-versa.

Theorem 2.3.7. *[MRS18, Theorem 4.4.9] Let k be a field. Let G be a finite graph. Let Δ_G be the independence complex of G. We have that $I(G) = I_{\Delta_G}$ so that $k(G) = k[\Delta_G]$.*

2.4 Semigroup Theory

2.4.1 Semigroups and Semigroup Rings

Generally, a **semigroup** $(S,\cdot)$ consists of a (possibly empty) set S equipped with an associative binary operation $\cdot : S \times S \to S$ defined by $(s,t) \mapsto s \cdot t$. We refer to a semigroup S as **commutative** if $s \cdot t = t \cdot s$ for any pair of elements $s,t \in S$. Considering that the structure of a semigroup is not restrictive, it is not surprising that semigroups admit pathological examples like the empty set $\emptyset$ equipped with the empty function or the singleton $\{s\}$ equipped with the trivial function $s \cdot s = s$. We will focus our attention primarily on semigroups with at least two elements.

We say that a semigroup F is **free** of **rank** n if there exist elements $e_1,\ldots,e_n \in F$ such that

(i.) every element of F can be written as a product of the elements $e_1,\ldots,e_n$ and

(ii.) if $e_{i_1}\cdots e_{i_m} = e_{j_1}\cdots e_{j_n}$, then $m = n, i_1 = j_1, \ldots,$ and $i_m = j_n$.

We refer to the elements $e_1, \ldots, e_n$ as the **free generators** of the free semigroup F. Observe that $\mathbb{Z}^n_{\geq 0}$ is a free semigroup of rank n for each positive integer n. Explicitly, addition of vectors in $\mathbb{Z}^n_{\geq 0}$ is an associative binary operation, and the standard basis vectors $\mathbf{e}_i = \langle \delta_{i,1}, \ldots, \delta_{i,n} \rangle$ constitute a set of free generators of $\mathbb{Z}^n_{\geq 0}$, where $\delta_{i,j}$ is the Kronecker delta. We shall soon see that $\mathbb{Z}^n_{\geq 0}$ is the *unique* (in a rigorous sense) free commutative semigroup of rank n for each positive integer n.

We say that a binary relation $\sim : S \times S \to S$ on a semigroup S is a **congruence** whenever $\sim$ is an equivalence relation such that $s \sim t$ implies that $s \cdot u \sim t \cdot u$ for all elements u of S.

Proposition 2.4.1. *Let S be a nonempty semigroup with at least two elements. Let $\sim$ be a congruence on S. The set $Q = S/\sim$ of equivalence classes of S modulo $\sim$ forms a semigroup with respect to the operation $\bar{s} * \bar{t} = \overline{s \cdot t}$, where $\bar{s} = \{r \in S \mid r \sim s\}$ denotes the equivalence class of s.*

Proof. We must first establish that $\bar{s} * \bar{t} = \overline{s \cdot t}$ is a well-defined binary operation. Let $s \sim u$ and $t \sim v$ be representatives of the equivalence classes $\bar{s}$ and $\bar{t}$, respectively. By hypothesis that S is a semigroup and $\sim$ is a congruence, we have that $s \cdot t = u \cdot t = u \cdot v$ is an element of S. Consequently, we find that $\bar{s} * \bar{t} = \overline{s \cdot t} = \overline{u \cdot v} = \bar{u} * \bar{v}$. Last, the associativity $*$ holds by the associativity of $\cdot$. $\square$

Given two nonempty semigroups S and T, we say that a map $\varphi : S \to T$ is a **semigroup homomorphism** whenever $\varphi(s \cdot t) = \varphi(s) \cdot \varphi(t)$ for any pair of elements $s, t \in S$. Given any semigroup homomorphism φ, we may consider $\ker \varphi = \{(s,t) \in S \times S \mid \varphi(s) = \varphi(t)\}$. One can verify that $s \sim_\varphi t$ if and only if $(s,t) \in \ker \varphi$ is an equivalence relation with the property $s \sim t$ implies that $s \cdot u \sim t \cdot u$ for all elements u of S, hence we refer to $\ker \varphi$ as the **kernel congruence** of φ. If φ is injective (i.e., $\ker \varphi$ is the diagonal of $S \times S$), we say that φ is an **isomorphism**.

Proposition 2.4.2. *Let F be a free semigroup with free generators $e_1, \ldots, e_n$. Let S be a nonempty semigroup. Given any elements $s_1, \ldots, s_n \in S$, there exists a unique semigroup homomorphism $\varphi : F \to S$ that satisfies $\varphi(e_i) = s_i$ for each integer $1 \leq i \leq n$. Particularly, the following hold.*

(1.) *Every pair of free semigroups of the same rank are isomorphic.*

(2.) *Every nonempty finitely generated semigroup is the homomorphic image of a free semigroup.*

Proof. Consider the map $\gamma : F \to S$ defined by $\gamma(e_{i_1} \cdots e_{i_k}) = s_{i_1} \cdots s_{i_k}$. By hypothesis that F is a free semigroup with free generators $e_1, \ldots, e_n$, this map well-defined and satisfies $\gamma(e_i) = s_i$ for each integer $1 \leq i \leq n$. Consequently, we may define $\varphi : F \to S$ by $\varphi(e_{i_1} \cdots e_{i_k}) = \gamma(e_{i_1}) \cdots \gamma(e_{i_k})$. Once again, by hypothesis that $e_1, \ldots, e_n$ are free generators of F, this map is well-defined and satisfies $\varphi(e_i) = s_i$. Further, it is a semigroup homomorphism. Explicitly, we have that

$$\varphi(e_{i_1} \cdots e_{i_k} \cdot e_{j_1} \cdots e_{j_\ell}) = \gamma(e_{i_1}) \cdots \gamma(e_{i_k}) \cdot \gamma(e_{j_1}) \cdots \gamma(e_{j_\ell}) = \varphi(e_{i_1} \cdots e_{i_k}) \cdot \varphi(e_{j_1} \cdots e_{j_\ell}).$$

Clearly, the homomorphism φ is unique. Consequently, for any pair of free semigroups F and G with respective free generators $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$, there exist unique semigroup homomorphisms $\varphi : F \to G$ and $\psi : G \to F$ satisfying $\varphi(e_i) = f_i$ and $\psi(f_i) = e_i$. Observe that φ and ψ are inverse mappings, hence they are both isomorphisms. Last, if S is finitely generated by $s_1, \ldots, s_n$, then it is the homomorphic image of the free semigroup F of rank n via the map $e_i \mapsto s_i$. □

Corollary 2.4.3. *Let S be a nonempty finitely generated semigroup. There exists a free semigroup F and a semigroup homomorphism $\varphi : F \to S$ such that $S \cong F/\ker\varphi$.*

Proof. Consider a system of generators $s_1, \ldots, s_n$ of S. Let F be the free semigroup with free generators $e_1, \ldots, e_n$. By Proposition 2.4.2, the map $\varphi : F \to S$ induced by the assignment $\varphi(e_i) = s_i$ is a well-defined surjective semigroup homomorphism. Consequently, we may define $\gamma : F/\ker\varphi \to S$ by $\gamma(\overline{e_{i_1} \cdots e_{i_k}}) = \varphi(e_{i_1} \cdots e_{i_k}) = s_{i_1} \cdots s_{i_k}$. Observe that by definition of $\ker\varphi$, we have that $\overline{e_{i_1} \cdots e_{i_k}} = \overline{e_{j_1} \cdots e_{j_\ell}}$ if and only if $\varphi(e_{i_1} \cdots e_{i_k}) = \varphi(e_{j_1} \cdots e_{j_\ell})$, hence γ is an isomorphism. □

Every semigroup induces a ring in the following manner. Let R be an arbitrary ring, and let S be an arbitrary semigroup. Consider the free R-module $R[S]$ generated by S. Explicitly, a typical element of $R[S]$ is of the form $\sum_{s \in S} x_s s$ for some unique elements x_s of R such that $x_s \neq 0_R$ for only finitely many elements $s \in S$. We define addition and multiplication in $R[S]$ by

$$\sum_{s \in S} x_s s + \sum_{s \in S} y_s s = \sum_{s \in S} (x_s + y_s) s \text{ and } \left(\sum_{s \in S} x_s s \right) \left(\sum_{t \in S} y_t t \right) = \sum_{s,t \in S} x_s y_t (s \cdot t).$$

Under these operations, $R[S]$ is a ring called the **semigroup ring** corresponding to R and S. Our next proposition follows immediately by the addition and multiplication defined above.

Proposition 2.4.4. *Let $R[S]$ be the semigroup ring corresponding to R and S.*

(1.) *If R admits a multiplicative identity 1_R and S admits a multiplicative identity 1_S, then $1_R 1_S$ is the unique multiplicative identity of $R[S]$.*

(2.) *If R and S are both commutative, then $R[S]$ is a commutative ring.*

Our next several results are well-known and form the basis for the next section.

Theorem 2.4.5. *[Gil84, Theorem 7.1] If R is a commutative ring and S and T are commutative semigroups, then $R[S\times T]\cong R[S]\otimes_R R[T]$ as R-algebras, where $S\times T$ is the commutative semigroup of ordered pairs $\{(s,t)\mid s\in S \text{ and } t\in T\}$ whose binary operation is defined componentwise.*

Proposition 2.4.6. *Let $\mathbb{Z}_{\geq 0}$ denote the additive semigroup of non-negative integers. Given any ring R, the map $\varphi : R[\mathbb{Z}_{\geq 0}]\to R[x]$ defined by $\sum_{k=0}^{n} r_k k \mapsto \sum_{k=0}^{n} r_k x^k$ is an R-algebra isomorphism.*

Corollary 2.4.7. *Given any ring R, we have that $R[\mathbb{Z}_{\geq 0}^n]\cong R[x_1,\ldots,x_n]$ as R-algebras.*

Theorem 2.4.8. *[Her69, Theorem 2.1.5] Let S be a finitely generated commutative semigroup S. For any surjective semigroup homomorphism $\varphi : \mathbb{Z}_{\geq 0}^n \to S$, $\ker\varphi$ induces a ring isomorphism*

$$R[S]\cong R[\mathbb{Z}_{\geq 0}^n/\ker\varphi]\cong R[x_1,\ldots,x_n]/(\underline{x}^{\mathbf{a}}-\underline{x}^{\mathbf{b}}\mid \varphi(\mathbf{a})=\varphi(\mathbf{b})),$$

where $\mathbf{a}=(a_1,\ldots,a_n)$ and $\mathbf{b}$ denote vectors in $\mathbb{Z}_{\geq 0}^n$ and $\underline{x}^{\mathbf{a}}=x_1^{a_1}\cdots x_n^{a_n}$.

2.4.2 Numerical Semigroups

We say that a semigroup $(S,\cdot)$ is a **monoid** if it possesses a multiplicative identity, i.e., an element 1_S such that $s\cdot 1_S = s = 1_S\cdot s$ for all elements $s\in S$. If $T\subseteq S$ is closed under the operation of S and

contains 1_S, then T is a **submonoid** of S. We refer to a monoid as **commutative** if it is commutative as a semigroup. By convention, a commutative monoid is written with additive notation and identity element 0. Our prototypical example of a commutative monoid is $(\mathbb{Z}_{\geq 0}, +)$.

Given any subset S of $\mathbb{Z}_{\geq 0}$, we say that S is a **numerical semigroup** provided that S is a monoid and $\mathbb{Z}_{\geq 0} \setminus S$ is finite. By definition, there is a largest positive integer not contained in S; it is the **Frobenius number** $\mathrm{F}(S) = \max\{n \in \mathbb{Z}_{\geq 0} \mid n \notin S\}$. On the other hand, the least nonzero element of S is its **multiplicity** $e(S) = \min\{n \geq 1 \mid n \in S\}$. We define the **pseudo-Frobenius numbers**

$$\mathrm{PF}(S) = \{n \in \mathbb{Z}_{\geq 0} \setminus S \mid n + s \in S \text{ for all nonzero elements } s \in S\}$$

of S, and we denote by $r(S) = |\mathrm{PF}(S)|$ the **type** of S. Observe that the Frobenius number of S is the largest pseudo-Frobenius number of S, hence there is no coincident in naming conventions.

Before we proceed, we note that every submonoid of $\mathbb{Z}_{\geq 0}$ is finitely generated and admits a unique finite minimal system of generators. Recall that a subset G of a monoid S forms a **system of generators** of S if every element of S can be written as a finite sum of elements of G. Even more, if G is minimal with respect to inclusion among all systems of generators of S, we say that G is a **minimal** system of generators of S. We denote $S^* = S \setminus \{0\}$ and $S^* + S^* = \{s + t \mid s, t \in S^*\}$.

Proposition 2.4.9. *[GR09, Lemma 2.3 and Theorem 2.7] For any submonoid S of $\mathbb{Z}_{\geq 0}$, the set $S^* \setminus (S^* + S^*)$ constitutes the unique finite minimal system of generators of S.*

We refer to $\mu(S) = |S^* \setminus (S^* + S^*)|$ as the **embedding dimension** of S. By the Pigeonhole Principle, we have that $\mu(S) \leq e(S)$. Explicitly, $e(S)$ is the smallest element of $S^* \setminus (S^* + S^*)$, and the least non-negative residues modulo $e(S)$ are precisely $0, 1, \ldots, e(S) - 1$. Each element of $S^* \setminus (S^* + S^*)$ is congruent to exactly one least non-negative residue modulo $e(S)$, and no distinct elements of $S^* \setminus (S^* + S^*)$ are congruent modulo $e(S)$, hence the inequality holds. We say that S has **maximal embedding dimension** if $\mu(S) = e(S)$.

By Proposition 2.4.9 and Bézout's Lemma, we obtain the following proposition.

Proposition 2.4.10. *[GR09, Lemma 2.1] Let S be a submonoid of $\mathbb{Z}_{\geq 0}$. We have that S is a numerical semigroup if and only if* $\gcd(a_1,\ldots,a_n)=1$, *where* $S^* \setminus (S^*+S^*) = \{a_1,\ldots,a_n\}$.

We will henceforth denote by $\langle a_1,\ldots,a_n\rangle$ the numerical semigroup with unique minimal generating set $a_1<\cdots<a_n$, multiplicity a_1, and embedding dimension n.

We may prescribe a partial order $\leq_S$ of $\mathbb{Z}$ by declaring that $a \leq_S b$ if and only if $b-a \in S$. Under this relation, the pseudo-Frobenius numbers have an elegant description.

Proposition 2.4.11. *Let S be a numerical semigroup with the partial ordering $\leq_S$. We have that*

$$\mathrm{PF}(S) = \mathrm{Maximal}_{\leq_S}(\mathbb{Z}_{\geq 0} \setminus S).$$

Proof. Let m be an element of $\mathbb{Z}_{\geq 0} \setminus S$ that is maximal with respect to $\leq_S$. Let s be a nonzero element of S. Considering that $(m+s)-m = s \in S$, it follows that $m \leq_S m+s$. By hypothesis, we must have that $m+s$ belongs to S, hence m is pseudo-Frobenius and $\mathrm{Maximal}_{\leq_S}(\mathbb{Z}_{\geq 0} \setminus S) \subseteq \mathrm{PF}(S)$.

Conversely, let $n \in \mathrm{PF}(S)$. On the contrary, suppose that $m \in \mathbb{Z}_{\geq 0} \setminus S$ and $n \leq_S m$. By definition of $\leq_S$, we have that $m-n$ is in S so that $m = n+(m-n)$ is in S by hypothesis that n is pseudo-Frobenius — a contradiction. We conclude that $n \in \mathbb{Z}_{\geq 0} \setminus S$ is maximal with respect to $\leq_S$. □

Given any nonzero element $n \in S$, we define the **Apéry set** $\mathrm{Ap}(n,S) = \{s \in S \mid s-n \notin S\}$ of S with respect to n. Our next fact illustrates that computing $\mathrm{Ap}(n,S)$ amounts to finding for each integer $0 \leq i \leq n-1$ the least element of S congruent to i modulo n.

Proposition 2.4.12. *[GR09, Lemmas 2.4 and 2.6] Let S be a numerical semigroup. Let $w(i)$ denote the least element of S congruent to i modulo n. We have that* $\mathrm{Ap}(n,S) = \{0, w(1),\ldots,w(n-1)\}$. *Further, for any element $s \in S$, there exist unique integers $k \geq 0$ and $0 \leq i \leq n-1$ with $s = kn+w(i)$.*

Combined, the previous two propositions yield a method to find the pseudo-Frobenius numbers.

Proposition 2.4.13. *[GR09, Proposition 2.20] Let S be a numerical semigroup. If n belongs to S^*,*

then $\mathrm{PF}(S) = \{x - n \mid x \in \mathrm{Ap}(n,S)$ *is maximal with respect to* $\leq_S\}$. *Particularly, we have that*

$$\mathrm{PF}(S) = \{x - e(S) \mid x \in \mathrm{Ap}(e(S),S) \text{ is maximal with respect to } \leq_S\}.$$

Example 2.4.14. Consider the numerical semigroup $S = \langle 4, 11, 13, 18\rangle$. We have that $e(S) = 4$ and $\mu(S) = 4$, hence S has maximal embedding dimension. Observe that $\mathrm{Ap}(e(S),S) = \{0, 11, 13, 18\}$. Computing the pairwise differences of the positive elements of $\mathrm{Ap}(e(S),S)$ shows that they are all incomparable with respect to $\leq_S$, hence we have that $\mathrm{Maximal}_{\leq_S}\mathrm{Ap}(e(S),S) = \{11, 13, 18\}$ and $\mathrm{PF}(S) = \{7, 9, 14\}$. We conclude that $\mathrm{F}(S) = 14$ and $r(S) = |\mathrm{PF}(S)| = 3$.

Using Propositions 2.4.11 and 2.4.13, one can prove the following.

Proposition 2.4.15. *[GR09, Proposition 2.13] Given relatively prime positive integers* a *and* b, *the numerical semigroup* $S = \langle a,b\rangle$ *has* $\mathrm{F}(S) = ab - a - b$ *and* $|\mathbb{Z}_{\geq 0} \setminus S| = \frac{1}{2}(ab - a - b + 1)$.

Observe that if every pair of distinct elements of $\mathrm{Ap}(e(S),S)$ is comparable with respect to $\leq_S$ (i.e., $x - y \in S$ for all distinct elements $x, y \in \mathrm{Ap}(e(S),S)$), then $\mathrm{Maximal}_{\leq_S}(\mathrm{Ap}(e(S),S))$ consists of the largest element of $\mathrm{Ap}(e(S),S)$ so that $|\mathrm{PF}(S)| = 1$ by Proposition 2.4.13. Our immediate goal is to classify such numerical semigroups via their equivalent properties.

Definition 2.4.16. [GR09, Proposition 4.4] We say that a numerical semigroup S is **symmetric** if $\mathrm{F}(S)$ is odd and for every integer $n \in \mathbb{Z}_{\geq 0}$, we have that $n \in S$ or $\mathrm{F}(S) - n \in S$.

One naturally wonders why the condition that $\mathrm{F}(S)$ is odd is necessary in this definition. In fact, if $\mathrm{F}(S) = 2k$ for some integer $k \geq 1$, then k must not belong to S; otherwise, $\mathrm{F}(S)$ would belong to S — a contradiction. Consequently, the positive integer $k = \mathrm{F}(S) - k$ does not belong to S.

We record the following equivalent conditions for a symmetric numerical semigroup.

Proposition 2.4.17. *[Vil15, Proposition 8.7.3] A numerical semigroup* S *is symmetric if and only if* $|\mathbb{Z}_{\geq 0} \setminus S| = \frac{1}{2}(\mathrm{F}(S) + 1)$. *Particularly, if* $\mathrm{F}(S)$ *is even, then* S *is not symmetric.*

Proposition 2.4.18. *[Vil15, Proposition 8.7.4] A numerical semigroup* S *is symmetric if and only if* $\mathrm{PF}(S) = \{\mathrm{F}(S)\}$. *Particularly, if* $|\mathrm{Maximal}_{\leq_S}\mathrm{Ap}(e(S),S)| > 1$, *then* S *is not symmetric.*

The simplest examples of symmetric numerical semigroups are those with two generators.

Proposition 2.4.19. *A numerical semigroup of embedding dimension two is symmetric.*

Proof. Observe that $\mu(S) = 2$ if and only if $S = \langle a, b\rangle$ for some relatively prime positive integers a and b. By Proposition 2.4.15, we have that $|\mathbb{Z}_{\geq 0} \setminus S| = \frac{1}{2}(ab - a - b + 1) = \frac{1}{2}(\mathrm{F}(S) + 1)$. By Proposition 2.4.17, we conclude that S is symmetric. □

We say that a nonempty set $I \subseteq \mathbb{Z}$ is a **relative ideal** of a numerical semigroup S provided that $I \supseteq S + I = \{s + i \mid s \in S, i \in I\}$ and there exists an element $s \in S$ such that $s + I \subseteq S$, i.e., I possesses a smallest element. If $I \subseteq S$ satisfies $I \supseteq S + I$, then I is a **proper ideal** of S. Clearly, S^* is the largest (with respect to inclusion) proper ideal of S; it is the **maximal ideal** of S.

We note that a proper ideal of any commutative semigroup S can be defined in the same way, so in the remainder of this section, we may assume that S is a commutative semigroup.

We say that a proper ideal $I \subseteq S$ is **finitely generated** if there exist elements $x_1, \ldots, x_k \in I$ such that $I = \{x_1, \ldots, x_k\} + S = \{x_i + s \mid 1 \leq i \leq n \text{ and } s \in S\}$. Given any nonzero element $x \in S$, the proper ideal $I = x + S$ is finitely generated by x; it is the **principal ideal** generated by x. Observe that S^* is finitely generated by the unique finite minimal system of generators $S^* \setminus (S^* + S^*)$.

Definition 2.4.20. Let $x_1, \ldots, x_k$ be distinct nonzero elements of a commutative semigroup S. We denote by $(x_1, \ldots, x_k) = \{x_1, \ldots, x_k\} + S$ the proper ideal of S **generated by** $x_1, \ldots, x_k$.

We conclude with a few results that illuminate the structure of the ideals of a commutative semigroup. Particularly, we note that the ideals of a numerical semigroup are finitely generated.

Definition 2.4.21. Let S be a commutative semigroup. We say that S satisfies the **ascending chain condition** on proper ideals if every ascending chain of proper ideals $I_1 \subseteq I_2 \subseteq \cdots$ of S eventually stabilizes, i.e., there exists an integer $n \gg 0$ such that $I_k = I_n$ for all integers $k \geq n$.

Definition 2.4.22. [Aub53, Theorem 3] We say that a commutative semigroup S is **Noetherian** if either of the following equivalent properties hold.

(i.) S satisfies the ascending chain condition on proper ideals.

(ii.) Every proper ideal I of S is finitely generated.

Theorem 2.4.23. *[Mil21, Corollary 3.3] Every numerical semigroup is Noetherian.*

Corollary 2.4.24. *Every ideal of a numerical semigroup is finitely generated.*

Proof. Every proper ideal of a numerical semigroup S is finitely generated. Consequently, every relative ideal I of S is finitely generated. Explicitly, there exists an element $s \in S$ such that $s+I \subseteq S$. Considering that $s+I$ is a proper ideal of S, there exist elements $x_1,\ldots,x_k \in I$ such that $s+I$ is generated by $s+x_1,\ldots,s+x_k$. But this implies that I is generated by $x_1,\ldots,x_k$. □

2.4.3 Numerical Semigroup Rings

We will henceforth assume that k is an infinite field and that t is an indeterminate. Given any numerical semigroup S, we define the **numerical semigroup ring** $k[\![S]\!] = k[\![t^s \mid s \in S]\!]$ corresponding to S. Clearly, if $S = \langle a_1,\ldots,a_n\rangle$, then $k[\![S]\!] = k[\![t^{a_1},\ldots,a^n]\!]$. Observe that $k[\![S]\!]$ is a complete local domain with maximal ideal $\mathfrak{m} = (t^{a_1},\ldots,t^{a_n})$ and integral closure $k[\![t]\!]$, hence $k[\![S]\!]$ is a one-dimensional Cohen-Macaulay local ring. By a result of Nagata in [Nag50], the integral closure of any numerical semigroup ring is module-finite. Consequently, a numerical semigroup ring is an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k.

Considering that a numerical semigroup S is a finitely generated commutative semigroup, one might wonder how our present definition of a numerical semigroup ring coincides with the definition guaranteed by Theorem 2.4.8. We resolve this matter in the following proposition.

Proposition 2.4.25. *Let k be an infinite field. Let $S = \langle a_1,\ldots,a_n\rangle$ be a numerical semigroup. The ideal $I_S = (\underline{x}^{\mathbf{a}} - \underline{x}^{\mathbf{b}} \mid (a_1,\ldots,a_n)\cdot\mathbf{a} = (a_1,\ldots,a_n)\cdot\mathbf{b})$ of $k[x_1,\ldots,x_n]$ is equal to the kernel of the ring homomorphism $k[\![x_1,\ldots,x_n]\!] \to k[\![S]\!]$ induced by the assignment $x_i \mapsto t^{a_i}$, where $\underline{x}^{\mathbf{a}} = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ for $\mathbf{a} = (\alpha_1,\ldots,\alpha_n)$ and $\cdot$ denotes the dot product. Consequently, the numerical semigroup ring $k[\![S]\!]$ defined in this section is equal to the numerical semigroup ring defined in Theorem 2.4.8.*

Proof. Let $\varphi : k[\![x_1,\ldots,x_n]\!] \to k[\![S]\!]$ denote the map induced by the assignment $x_i \mapsto t^{a_i}$. By the First Isomorphism Theorem, we have that $k[\![S]\!] \cong k[\![x_1,\ldots,x_n]\!]/\ker\varphi$. On the other hand, observe that φ

induces a surjective semigroup homomorphism $\widetilde{\varphi} : \mathbb{Z}_{\geq 0}^n \to S$ defined by $\widetilde{\varphi}(\mathbf{a}) = (a_1, \ldots, a_n) \cdot \mathbf{a}$. By Theorem 2.4.8, we have that $k[\![S]\!] \cong k[\mathbb{Z}_{\geq 0}^n / \ker \widetilde{\varphi}] \cong k[x_1, \ldots, x_n]/I_S$. Considering that $I_S \subseteq \ker \varphi$ and $k[\![x_1, \ldots, x_n]\!]/I_S \cong k[\![x_1, \ldots, x_n]\!]/\ker \varphi$, we conclude that $I_S = \ker \varphi$, as desired. □

By the previous proposition, it follows that a numerical semigroup ring corresponding to the numerical semigroup S is equal to the quotient of the ring of formal power series in $\mu(S)$ indeterminates by some **toric ideal**, i.e., a prime ideal generated by differences of monomials. Generally, it is impossible to determine the minimal number of generators of the ideal I_S of Proposition 2.4.25 (cf. [Bre75]); however, if $\mu(S) \leq 3$, there is a simple description of I_S (cf. [Her69] or [GS19]).

Clearly, the embedding dimension of the numerical semigroup ring $k[\![S]\!]$ is equal to the embedding dimension of the numerical semigroup S, hence there is no coincidence in terminologies used. Even more, the Hilbert-Samuel multiplicity of $k[\![S]\!]$ is equal to the multiplicity of S.

Proposition 2.4.26. *Let k be an infinite field. Let $S = \langle a_1, \ldots, a_n \rangle$. We have that $e(k[\![S]\!]) = e(S)$, where $e(k[\![S]\!])$ is the Hilbert-Samuel multiplicity of $k[\![S]\!]$ and $e(S)$ is the multiplicity of S.*

Proof. Let $R = k[\![S]\!] = k[\![t^{a_1}, \ldots, t^{a_n}]\!]$. Observe that for each integer $1 \leq i \leq n$, the monomial t^{a_i} of R satisfies the monic polynomial $X^{a_1} - t^{a_1 a_i}$, hence the elements $t^{a_1}, \ldots, t^{a_n}$ are integral over $t^{a_1}R$. Consequently, we have that $\mathfrak{m} = (t^{a_1}, \ldots, t^{a_n}) \subseteq \overline{t^{a_1}R} \subseteq \mathfrak{m}$. By [HS06, Proposition 11.2.1], we find that $e(R) = e_R(\mathfrak{m}) = e_R(t^{a_1}R)$. Considering that R is Cohen-Macaulay of dimension one and $t^{a_1}R$ is a system of parameters of R, it follows that $e_R(t^{a_1}R) = \ell_R(R/t^{a_1}R)$ by [HS06, Proposition 11.1.10]. Because R contains all monomials of degree $\geq \mathrm{F}(S)+1$, the field of fractions of R is equal to the field of fractions F of $\overline{R}$ and $\operatorname{rank}(\overline{R}) = \dim_F(F \otimes_R \overline{R}) = \dim_F(F) = 1$. By [BH93, Corollary 4.7.11], we find that $\ell_R(R/t^{a_1}R) = \ell_R(\overline{R}/t^{a_1}\overline{R})/\operatorname{rank}(\overline{R}) = \ell_R(\overline{R}/t^{a_1}\overline{R})$. By [Jon22, Lemma 10.52.12], we have that $\ell_R(\overline{R}/t^{a_1}\overline{R}) = \ell_{\overline{R}}(\overline{R}/t^{a_1}\overline{R}) = a_1$. Putting this all together yields

$$e(k[\![S]\!]) = e(R) = e_R(t^{a_1}R) = \ell_R(R/t^{a_1}R) = \ell_R(\overline{R}/t^{a_1}\overline{R}) = \ell_{\overline{R}}(\overline{R}/t^{a_1}\overline{R}) = a_1 = e(S). \qquad \square$$

One can also compute the a-invariant of a numerical semigroup ring.

Proposition 2.4.27. *[Vil15, Proposition 8.7.7] Let S be a numerical semigroup. The degree (as a rational function) of the Hilbert series of $k[\![S]\!]$ is* $\mathrm{F}(S)$.

Proof. By definition, the numerical semigroup ring $k[\![S]\!]$ is generated as a k-vector space by the monomials t^s such that $s \in S$. Consequently, we may consider $k[\![S]\!]$ as a graded k-vector space with $k[\![S]\!]_s = k\langle t^s \rangle$ if $s \in S$ and $k[\![S]\!]_s = 0$ if $s \notin S$. By definition of $\mathrm{F}(S)$, all integers $i \geq \mathrm{F}(S)+1$ belong to S, so there exists a polynomial $f(x)$ of degree $\leq \mathrm{F}(S)-1$ with coefficients 0 and 1 such that

$$H_{k[\![S]\!]}(x) = \sum_{i=0}^{\infty} \dim_k(k[\![S]\!]_i)x^i = f(x) + \sum_{i=0}^{\infty} x^i - \sum_{i=0}^{\mathrm{F}(S)} x^i = f(x) + \frac{1}{1-x} - \sum_{i=0}^{\mathrm{F}(S)} x^i. \qquad \square$$

Like we have previously noted, the study of non-Gorenstein Cohen-Macaulay local rings is an active area of research. Consequently, we seek to determine when a numerical semigroup ring is Gorenstein. Recall that a Cohen-Macaulay local ring is Gorenstein if and only if it has Cohen-Macaulay type 1. Our next theorem yields the type of a numerical semigroup ring.

Theorem 2.4.28 (Fröberg)**.** *[Vil15, Theorem 8.7.5] Let S be a numerical semigroup. We have that $r(k[\![S]\!]) = |\mathrm{PF}(S)|$, where $r(-)$ denotes Cohen-Macaulay type of $k[\![S]\!]$.*

Theorem 2.4.29 (Herzog)**.** *[Vil15, Theorem 8.7.6] Let S be a numerical semigroup. We have that $k[\![S]\!]$ is Gorenstein if and only if S is symmetric.*

Proof. This follows at once from Theorem 2.4.28 and Proposition 2.4.18. $\square$

Theorem 2.4.30 (Herzog)**.** *[Her69, Theorem 4.2.1] Let S be a numerical semigroup of embedding dimension three. We have that $k[\![S]\!]$ is a complete intersection if and only if it is Gorenstein.*

Chapter 3

Canonical Blow-Up of One-Dimensional Singularities

Abstract

We study the canonical blow-ups $B(\omega_R)$ of analytically unramified one-dimensional Cohen-Macaulay local rings $(R,\mathfrak{m},k)$ with infinite residue field k and canonical ideal ω_R. If $B(\omega_R)$ is Gorenstein, we say that R has the **Gorenstein canonical blow-up** (GCB) property. We provide equivalent conditions for GCB rings, and we show Arf rings, nearly Gorenstein rings of minimal multiplicity, far-flung Gorenstein rings, and numerical semigroup rings of multiplicity three are GCB. We study related numerical semigroup rings and give examples.

3.1 Introduction

We assume throughout this chapter that $(R,\mathfrak{m},k)$ is an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k, total ring of fractions $Q(R)$, and integral closure $\overline{R}$. Under these conditions, it is known that R admits a canonical ideal $\omega_R \subseteq R$ (cf. [HK71]) and every $\mathfrak{m}$-primary ideal of R has a principal reduction (cf [HS06, Corollary 8.3.9]).

Recall that a regular ideal I of R is **stable** if $I \cong I^2$ as R-modules. Lipman illustrated in [Lip71] that the stable ideals of R are precisely those whose blow-ups are as simple as possible. We say that I is a **trace ideal** if $I = \sum_{f\in \mathrm{Hom}_R(I,R)} f(I) = \mathrm{tr}(I)$. Recent works of Dao-Lindo [DL21] and Dao-Maitra-Sridhar [DMS21] have illuminated a fundamental relationship among the stable ideals, trace ideals, and blow-ups of R. Even more, efforts by Herzog, Stamate, et al. in [HHS19] and [HKS21] to study the canonical trace ideal $\mathrm{tr}(\omega_R)$ have produced two interesting new classes of Cohen-Macaulay local rings: **nearly Gorenstein** and **far-flung Gorenstein** rings, respectively.

Using this inspiration, we study the canonical blow-up $B(\omega_R) = \bigcup_{n\geq 0}\{\alpha \in Q(R) \mid \alpha\omega_R^n \subseteq \omega_R^n\}$. In Section 3.2, we demonstrate that for a regular ideal I of R, $B(I)$ is Gorenstein if and only if $B(I) \cong \mathrm{Hom}_R(B(I), \omega_R)$. We obtain as a corollary that R is Gorenstein if and only if $B(\omega_R) = R$. Further, we establish several equivalent conditions for $B(\omega_R)$ to be Gorenstein using the **blow-up class** of the canonical ideal ω_R, which we define as the smallest power of ω_R that is isomorphic as an R-module to all higher powers of ω_R. We say that R has the **Gorenstein canonical blow-up** (GCB) property if $B(\omega_R)$ is Gorenstein. Our main result of this section is the following theorem.

Theorem. Let $(R, \mathfrak{m}, k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with canonical ideal ω_R. If k is infinite, then $B(\omega_R)$ is Gorenstein if any of the following hold.

(a.) R is Arf.

(b.) R is a nearly Gorenstein ring of minimal multiplicity.

(c.) R is an almost Gorenstein ring of minimal multiplicity.

(d.) R is a far-flung Gorenstein ring.

Proof. Corollary 3.2.14 illustrates that (a.) Arf rings are GCB. Proposition 3.2.19 establishes that (b.) nearly Gorenstein rings of minimal multiplicity are GCB; it is well-known that (b.) and (c.) are equivalent. Corollary 3.2.23 demonstrates that (d.) far-flung Gorenstein rings are GCB. □

We interest ourselves also with the stronger condition that $B(\omega_R)$ is regular, in which case we say that R has the **regular canonical blow-up** (RCB) property. We note that this is equivalent to the case that $B(\omega_R) = \overline{R}$, as regular rings are integrally closed and $\overline{R}$ is regular. We provide further equivalent conditions under which R is RCB in terms of the conductor $(R : \overline{R})$ and the blow-up class of ω_R. We conclude by establishing that far-flung Gorenstein rings are RCB.

We devote Section 3.3 to the study of numerical semigroups, which give rise to a class of one-dimensional complete Noetherian local domains and provide a setting in which we are able to exhibit several examples. By definition, a numerical semigroup S is a submonoid of $\mathbb{Z}_{\geq 0}$ such that $\mathbb{Z}_{\geq 0} \setminus S$ is finite; the integer $\mathrm{F}(S) = \max\{n \in \mathbb{Z}_{\geq 0} \mid n \notin S\}$ is called the **Frobenius number**

of S, and the integer $e(S) = \min\{n \mid n \in S \setminus \{0\}\}$ is the **multiplicity** of S. We consider also the set $\mathrm{PF}(S) = \{n \in \mathbb{Z}_{\geq 0} \setminus S \mid n + s \in S \text{ for all nonzero elements } s \in S\}$ of **pseudo-Frobenius numbers** of S. We say that a nonempty set $I \subseteq \mathbb{Z}$ is a (relative) **ideal** of S if $S + I \subseteq S$ and there exists an element $s \in S$ such that $s + I \subseteq S$. Every (relative) ideal I of a numerical semigroup S is finitely generated by some elements $x_1 < \cdots < x_k$ in I. Particularly, the relative canonical ideal of S is given by $\Omega = \{-n \mid n \in \mathbb{Z} \setminus S\}$; it is finitely generated by the elements $\{-x \mid x \in \mathrm{PF}(S)\}$. We define the **blow-up** numerical semigroup $B_S(I) = S + \mathbb{Z}_{\geq 0}\langle x_i - x_1 \mid 1 \leq i \leq k\rangle$ of S with respect to I and the **canonical blow-up** $B_S(\Omega) = S + \mathbb{Z}_{\geq 0}\langle \mathrm{F}(S) - x \mid x \in \mathrm{PF}(S)\rangle$. Our main result is the following.

Theorem 3.3.15. Every numerical semigroup of multiplicity at most 3 is GCB.

We conclude this section with several examples of numerical semigroups. We illustrate in particular that GCB rings are not necessarily Arf, nearly Gorenstein, almost Gorenstein, or far-flung Gorenstein by exhibiting numerical semigroups that have certain properties but not others.

Last, in Section 3.4, we generalize far-flung Gorenstein numerical semigroups. We say that S is **divisive** if $\mathrm{F}(S) - 1$ is a pseudo-Frobenius number. By definition, far-flung Gorenstein numerical semigroups are divisive (cf. [HKS21, Proposition 6.1]), and every divisive numerical semigroup is GCB. We classify divisive numerical semigroups generated by intervals in Theorem 3.4.12 and divisive numerical semigroups of maximal embedding dimension in Theorem 3.4.14.

3.2 The Gorenstein Canonical Blow-Up (GCB) Property

Unless otherwise noted, we will assume henceforth that $(R, \mathfrak{m}, k)$ is an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k, total ring of fractions $Q(R)$, integral closure $\overline{R}$, and conductor $(R : \overline{R}) = \{\alpha \in Q(R) \mid \alpha\overline{R} \subseteq R\}$. By Proposition 2.2.73, such a ring R admits a canonical ideal ω_R. Even more, every $\mathfrak{m}$-primary ideal of R has a principal reduction (cf [HS06, Corollary 8.3.9]). Our main tool throughout this section is the following.

Definition 3.2.1. Let I be an ideal of R. We define the **blow-up** of I as

$$B(I) = \bigcup_{n\geq 0} (I^n : I^n) = \bigcup_{n\geq 0} \{\alpha \in Q(R) \mid \alpha I^n \subseteq I^n\}.$$

We define the **conductor** of $B(I)$ into R as $b(I) = (R : B(I))$.

Remark 3.2.2. Recall that an ideal I of R is **regular** if there exists an R-regular element $x \in I$. If I is regular, then $b(I) = (R : B(I)) \cong \mathrm{Hom}_R(B(I), R)$ as R-submodules of $Q(R)$. Consequently, if $B(I)$ is finitely generated, then $b(I)$ is finitely generated, as well.

Remark 3.2.3. By Proposition 2.2.70, every Cohen-Macaulay local ring $(R, \mathfrak{m})$ that admits a canonical ideal ω_R is generically Gorenstein. By Proposition 2.2.71, the canonical ideal ω_R is regular. Even more, by the same proposition, ω_R has finite colength.

By Propositions 2.2.16 and 2.1.27, every regular ideal of R is $\mathfrak{m}$-primary and admits a regular principal reduction. Our next definition applies to the case that the reduction number is one.

Definition 3.2.4. [Lip71, Definition 1.3 and Lemma 1.11] Let R be a Noetherian ring. Let I be a regular ideal of R. We say that I is **stable** if any of the following equivalent statements hold.

(1.) We have that $B(I) = (I : I)$.

(2.) There exists an element $x \in I$ such that $I^2 = xI$.

(3.) There exists an R-regular element $x \in I$ such that $\dfrac{I}{x} = \left\{ \dfrac{i}{x} : i \in I \right\}$ is a ring.

(4.) There exists an R-regular element $x \in I$ such that $B(I) = \dfrac{I}{x}$.

Put another way, the previous definition illustrates that the stable ideals of R are precisely those ideals whose blow-ups are as simple as possible. Observe that property (2.) of Definition 3.2.4 shows that a stable ideal satisfies $I \cong I^2$ as R-modules, hence we have that $I^k \cong I$ for all integers $k \geq 1$. Our next definition generalizes this property to ideals that are not necessarily stable.

Definition 3.2.5. Let R be a Noetherian ring. Let I be a regular ideal of R. We define the **blow-up class** of I as $\mathfrak{b}_I = I^n$ such that n is the smallest integer for which $I^k \cong I^n$ for all integers $k \geq n$.

Of course, it is unclear that the blow-up class of an arbitrary regular ideal of R is well-defined. Our next lemma illustrates that $\mathfrak{b}_I$ exists in the case that I admits a principal reduction.

Lemma 3.2.6. *Let R be a Noetherian ring. Let I be a regular ideal. If I admits a principal reduction $x \in I$, then the blow-up class $\mathfrak{b}_I$ of I is well-defined. Further, it is a stable ideal.*

Proof. By hypothesis that $x \in I$ is a principal reduction of I, there exists a least integer $n \gg 0$ such that $I^{n+1} = xI^n$. Observe that x is a non-zero divisor on R by assumption that I is regular, hence $I^n \cong I^{n+1}$ and $\mathfrak{b}_I$ is well-defined. Particularly, we have that $I^{2n} = x^n I^n$, hence $\mathfrak{b}_I$ is stable. □

We will soon establish an intimate connection among canonical blow-up class $\mathfrak{b}_{\omega_R}$, its dual $\mathfrak{b}_{\omega_R}^{\vee}$, and the canonical blow-up $B(\omega_R)$. Before we state our next proposition, we recall the following.

Definition 3.2.7. Let M be an R-module. We define the **trace ideal** of M as

$$\operatorname{tr}(M) = \sum_{\varphi \in M^*} \varphi(M) = \{\varphi(x) \mid x \in M \text{ and } \varphi \in M^*\},$$

where $M^* = \operatorname{Hom}_R(M,R)$. We will adopt this star notation throughout this section. One can also view $\operatorname{tr}(M)$ as the image of the map $M \otimes_R M^* \to R$ defined by $x \otimes \varphi \mapsto \varphi(x)$.

Remark 3.2.8. For each ideal I of R, we have that $R \subseteq B(I) \subseteq Q(R)$, hence $B(I)$ is a birational ring extension of R and $Q(B(I)) = Q(R)$. Further, we have that

$$b(I) = (R : B(I)) \subseteq (R : B(I))B(I) \subseteq (R : B(I))Q(R) = (R : B(I))$$

so that $b(I) = (R : B(I))B(I)$. By [KT19, Proposition 2.4], we have that $b(I) = \operatorname{tr}(B(I))$.

Proposition 3.2.9. *Let $(R, \mathfrak{m}, k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k. Let I be a regular ideal of R. The following properties hold.*

(1.) *We have that $B(I) \cong \mathfrak{b}_I$ as R-modules. Consequently, $B(I)$ is a finitely generated R-module, so it is an integral extension of R; in particular, we have that* $\dim(B(I)) = \dim(R) = 1$.

(2.) *We have that* $B(I)$ *is Gorenstein if and only if* $B(I) \cong B(I)^\vee = \mathrm{Hom}_R(B(I), \omega_R)$ *if and only if* $\mathfrak{b}_I \cong \mathfrak{b}_I^\vee = \mathrm{Hom}_R(\mathfrak{b}_I, \omega_R)$, *where* ω_R *is the canonical ideal of* R.

(3.) *We have that* $\mathfrak{b}_{\omega_R} \cong \mathrm{tr}(\mathfrak{b}_{\omega_R})^* \cong (R : b(\omega_R))$.

Proof. (1.) Considering that the residue field k of R is infinite, it follows that I admits a principal reduction $x \in I$. By hypothesis that I is regular, x is a non-zero divisor of R. By Lemma 3.2.6, $\mathfrak{b}_I = I^n$ exists and is stable, hence we have that $B(\mathfrak{b}_I) = (\mathfrak{b}_I : \mathfrak{b}_I) = (I^n : I^n) = B(I^n) = B(I)$, from which it follows by Definition 3.2.4 that $\mathfrak{b}_I = xB(I)$ and $B(I) \cong \mathfrak{b}_I$ as R-modules.

(2.) By Definition 3.2.4 and Lemma 3.2.6, we have that $B(I) = R[I^n/x^n]$, hence the natural map $R \to B(I)$ is a local homomorphism of one-dimensional Cohen-Macaulay local rings; thus, $B(I)$ admits a canonical module $B(I)^\vee = \mathrm{Hom}_R(B(I), \omega_R)$ by Proposition 2.2.50. Consequently, $B(I)$ is Gorenstein if and only if $B(I) \cong B(I)^\vee$ if and only if $\mathfrak{b}_I \cong \mathfrak{b}_I^\vee$ by part (1.) above.

(3.) By part (1.) and Remark 3.2.2 above, we have that $B(\omega_R) \cong \mathfrak{b}_{\omega_R}$ and $b(\omega_R) \cong B(\omega_R)^*$ so that $\mathfrak{b}_{\omega_R}^* = B(\omega_R)^* \cong b(\omega_R) = \mathrm{tr}(B(\omega_R)) = \mathrm{tr}(\mathfrak{b}_{\omega_R})$. By [DMS21, Corollary 4.29], we note that $\mathfrak{b}_{\omega_R}$ is reflexive, and we conclude that $\mathfrak{b}_{\omega_R} \cong \mathfrak{b}_{\omega_R}^{**} \cong \mathrm{tr}(\mathfrak{b}_{\omega_R})^* \cong (R : \mathrm{tr}(\mathfrak{b}_{\omega_R})) = (R : b(\omega_R))$. □

Combined, our previous results establish the following.

Theorem 3.2.10. *Let* $(R, \mathfrak{m}, k)$ *be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field* k *and canonical ideal* ω_R. *The following are equivalent.*

(1.) $B(\omega_R)$ *is Gorenstein.*

(2.) *We have that* $\mathfrak{b}_{\omega_R} \cong \mathfrak{b}_{\omega_R}^\vee$.

(3.) *We have that* $\mathfrak{b}_{\omega_R} \cong \mathfrak{b}_{\omega_R}^*$.

(4.) *We have that* $\mathrm{tr}(\mathfrak{b}_{\omega_R})$ *is stable.*

Proof. Conditions (1.) and (2.) are equivalent by Proposition 3.2.9. By Lemma 3.2.6, $\mathfrak{b}_{\omega_R}$ is ω_R-Ulrich so that $\mathfrak{b}_{\omega_R}^* = \mathrm{Hom}_R(\mathfrak{b}_{\omega_R}, R) \cong \mathrm{Hom}_R(\mathfrak{b}_{\omega_R}, \omega_R) = \mathfrak{b}_{\omega_R}^\vee$ by [DMS21, Corollary 4.27]; thus, (2.) and (3.) are equivalent. Last, (3.) and (4.) are equivalent by [DL21, Corollary 4.10]. □

Remark 3.2.11. We thank Souvik Dey for pointing out that the equivalence of conditions (1.) and (4.) of Theorem 3.2.10 was established in [GMP13, Corollary 3.8]; however, it is worth noting that our proof invokes the theory of stable ideals and ω_R-Ulrich modules in a novel way.

Definition 3.2.12. Let $(R,\mathfrak{m},k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k and canonical ideal ω_R. If any of the equivalent conditions of Theorem 3.2.10 hold, we say that R has the **Gorenstein canonical blow-up** (GCB) property. We will abbreviate this when it is convenient by saying simply that R is GCB.

Recall that a one-dimensional Cohen-Macaulay ring is **Arf** if every integrally closed regular ideal is stable. We recall the following theorem of Dao and Lindo.

Theorem 3.2.13. *[DL21, Theorem 7.4] Let R be a one-dimensional Cohen-Macaulay local ring such that any regular ideal has a principal reduction. The following conditions are equivalent.*

(1.) *R is Arf.*

(2.) *Any regular trace ideal is stable.*

Corollary 3.2.14. *Let $(R,\mathfrak{m},k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k and canonical ideal ω_R. If R is Arf, then R is GCB.*

Proof. By Theorem 3.2.13, if R is Arf, then every regular trace ideal is stable. Particularly, the regular trace ideal $\mathrm{tr}(\mathfrak{b}_{\omega_R})$ is stable, hence $B(\omega_R)$ is Gorenstein by Corollary 3.2.15. □

Considering that $B(\omega_R)$ is a finitely generated R-module by Proposition 3.2.9, it follows that $R \subseteq B(\omega_R) \subseteq \overline{R}$. One naturally wonders under what conditions equality holds on one side of these containments or the other. Our next theorem deals with the case that $B(\omega_R) = R$.

Theorem 3.2.15. *Let $(R,\mathfrak{m},k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k and canonical ideal ω_R. The following are equivalent.*

(1.) *R is Gorenstein.*

(2.) *We have that $B(\omega_R) = R$.*

(3.) *We have that* $b(\omega_R) = R$.

Proof. We can verify immediately that (1.) $\implies$ (2.) $\implies$ (3.): if R is Gorenstein, then we have that $\omega_R = R$ so that $B(\omega_R) = B(R) = R$ by Theorem 2.2.67. If $B(\omega_R) = R$, then $b(\omega_R) = (R : B(\omega_R)) = (R : R) = R$. We will assume that $b(\omega_R) = R$. By Lemma 3.2.6, there exists an integer $n \gg 0$ such that ω_R^n is stable. By Proposition 3.2.9, we have that $B(\omega_R) \cong \omega_R^n$ as R-modules. By hypothesis that $b(\omega_R) = R$, our previous two observations imply that $R = b(\omega_R) = (R : B(\omega_R)) \cong (R : \omega_R^n)$. By [DMS21, Corollary 4.20], on the other hand, we have that $R = b(\omega_R) = \operatorname{tr}(B(\omega_R)) = \operatorname{tr}(B(\omega_R^n)) \subseteq \operatorname{tr}(\omega_R^n)$, hence equality holds. By [KT19, Proposition 2.4], we have that $R = \operatorname{tr}(\omega_R^n) = (R : \omega_R^n)\omega_R^n$. But this implies that $\omega_R^n = R\omega_R^n \cong (R : \omega_R^n)\omega_R^n = R$, hence R is ω_R-Ulrich by Lemma 3.2.6. Consequently, [DMS21, Corollary 4.7] implies that ω_R is principal with R-regular generator w, from which it follows that $\omega_R \cong R$ as R-modules, and we conclude that R is Gorenstein. □

We turn our attention now to the case that R is "close to" being Gorenstein.

Definition 3.2.16. [BF97, Definition-Proposition 20] Let $(R, \mathfrak{m})$ be a one-dimensional Cohen-Macaulay local ring such that $\overline{R}$ is finitely generated as an R-module and R admits a canonical module $R \subseteq C \subseteq \overline{R}$. We say that R is **almost Gorenstein** if $\mathfrak{m}C = \mathfrak{m}$.

Definition 3.2.17. [HHS19, Definition 2.2] Let $(R, \mathfrak{m})$ be a Cohen-Macaulay local ring that admits a canonical module ω_R. We say that R is **nearly Gorenstein** if $\operatorname{tr}(\omega_R) \supseteq \mathfrak{m}$.

Recall that a maximal Cohen-Macaulay R-module M is I-Ulrich for an $\mathfrak{m}$-primary ideal I if and only if $e_R(I, M) = \ell_R(M/IM)$ (cf. [DMS21, Definition 4.1]). We obtain the following.

Proposition 3.2.18. *Let* $(R, \mathfrak{m}, k)$ *be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field* k *and canonical ideal* ω_R*. The following are equivalent.*

(1.) *R is almost Gorenstein.*

(2.) $\mathfrak{m}$ *is* ω_R*-Ulrich.*

(3.) *We have that* $b(\omega_R) \supseteq \mathfrak{m}$.

Proof. If R is Gorenstein, then $b(\omega_R) = R \supseteq \mathfrak{m}$ by Theorem 3.2.15. If R is almost Gorenstein but not Gorenstein, then $\mathfrak{m} \cong \omega_R\mathfrak{m}$ is ω_R-Ulrich. By [DMS21, Corollary 4.11], this shows that $\mathfrak{m} \subseteq b(\omega_R)$. We conclude that (1.) implies (2.) and (3.).

Conversely, if $\mathfrak{m}$ is ω_R-Ulrich, then [DMS21, Theorem 4.6] implies that $\mathfrak{m} = \mathfrak{m}(\omega_R/x)$ for any principal reduction $x \in \omega_R$. Because $\omega_R/x \cong \omega_R$ via multiplication by x, it follows that R is almost Gorenstein. On the other hand, if $\mathfrak{m} \subseteq b(\omega_R) = \operatorname{tr}(B(\omega_R)) \subseteq R$, then we must have that $\mathfrak{b}^*_{\omega_R} \cong b(\omega_R) = R$ or $\mathfrak{b}^*_{\omega_R} \cong \mathfrak{m}$. Considering that $\mathfrak{b}_{\omega_R}$ is reflexive by [DMS21, Corollary 4.29], the former implies that $B(\omega_R) \cong \mathfrak{b}_{\omega_R} \cong \mathfrak{b}^{**}_{\omega_R} = R^* \cong R$ so that R is Gorenstein. If R is not Gorenstein, then R is not regular, and $\mathfrak{m}$ is a regular reflexive trace ideal by [DMS21, Corollary 3.2]. We conclude that $\mathfrak{m}$ is ω_R-Ulrich by [DMS21, Corollary 4.21], hence R is almost Gorenstein. □

Observe that a one-dimensional almost Gorenstein ring is nearly Gorenstein, as the inclusion $\mathfrak{m} \subseteq R$ yields that $\mathfrak{m} \subseteq \operatorname{tr}(\mathfrak{m}) = \operatorname{tr}(\mathfrak{m}C) = \mathfrak{m}\operatorname{tr}(C) \subseteq \operatorname{tr}(C)$ for any canonical module C of R that satisfies $R \subseteq C \subseteq \overline{R}$. Conversely, a one-dimensional nearly Gorenstein ring of minimal multiplicity is almost Gorenstein (cf. [HHS19, Theorem 6.6] or [DL21, Corollary 8.4]). We show next that if R has minimal multiplicity and either of these equivalent conditions holds, then R is GCB.

Corollary 3.2.19. *Let $(R,\mathfrak{m},k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k and canonical ideal ω_R. Consider the following conditions.*

(1.) *R is nearly Gorenstein*

(2.) *R is almost Gorenstein.*

If R has minimal multiplcity and either of these conditions holds, then R is GCB.

Proof. We note that it suffices to establish that condition (1.) implies that R is GCB. Before we do so, we recall that by [BH93, Exercise 4.6.14], if R has minimal multiplicity, then there exists an R-regular element $x \in \mathfrak{m}$ such that $\mathfrak{m}^2 = x\mathfrak{m}$. By Definition 3.2.4, it follows that $\mathfrak{m}$ is stable.

If R is Gorenstein, then $B(\omega_R) = R$ is Gorenstein by Theorem 3.2.15. Consequently, we may assume that R is almost Gorenstein but not Gorenstein. By Proposition 3.2.18, we have that $\operatorname{tr}(\mathfrak{b}_{\omega_R}) = \operatorname{tr}(B(\omega_R)) = b(\omega_R) = \mathfrak{m}$ is stable, hence $B(\omega_R)$ is Gorenstein by Theorem 3.2.10. □

Remark 3.2.20. Even under the additional assumption that R has minimal multiplicity, the GCB property does not imply that R is almost Gorenstein. Consider the numerical semigroup ring $R = k[\![t^3, t^7, t^8]\!]$ for an infinite field k. Observe that the numerical semigroup $S = \mathbb{Z}_{\geq 0}\langle 3, 7, 8\rangle$ has maximal embedding dimension three by Proposition 2.4.9, hence R has minimal multiplicity. We will soon establish that $B(\omega_R) = k[\![t]\!]$ (cf. Theorem 3.3.15), hence R has the GCB property; however, the numerical semigroup S is not almost symmetric, hence R is not almost Gorenstein.

Further, the hypothesis that R has minimal multiplicity cannot be dropped. Consider the almost Gorenstein numerical semigroup ring $R = k[\![t^4, t^7, t^9]\!]$ for an infinite field k. We will soon establish that $B(\omega_R) = k[\![t^4, t^5, t^7]\!]$ is not Gorenstein (cf. Proposition 3.3.22).

One can also consider the condition that the canonical blow-up is regular.

Theorem 3.2.21. *Let $(R, \mathfrak{m}, k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k, total ring of fractions $Q(R)$, integral closure $\overline{R}$, conductor $(R : \overline{R}) = \{\alpha \in Q(R) \mid \alpha\overline{R} \subseteq R\}$, and canonical ideal ω_R. The following are conditions equivalent.*

(1.) *$B(\omega_R)$ is regular.*

(2.) *We have that $B(\omega_R) = \overline{R}$.*

(3.) *We have that $b(\omega_R) = (R : \overline{R})$.*

(4.) *We have that $\mathfrak{b}^*_{\omega_R} \cong (R : \overline{R})$.*

(5.) *We have that $\mathfrak{b}_{\omega_R} \cong (R : \overline{R})$.*

(6.) *We have that $\omega_R^n \cong (R : \overline{R})$ for some integer $n \gg 0$.*

Proof. Observe that the implications (2.) $\implies$ (3.) $\iff$ (4.) and (5.) $\iff$ (6.) hold by definition or by previously established results. Consequently, it suffices to show that (1.) $\iff$ (2.) and (3.) $\implies$ (2.) $\implies$ (5.) $\implies$ (4.). If $B(\omega_R)$ is regular, then it is integrally closed by Corollary 2.1.74, hence $R \subseteq B(\omega_R) \subseteq \overline{R}$ imply that $B(\omega_R) = \overline{R}$. Conversely, $\overline{R}$ is a principal ideal ring by Proposition 2.1.163, hence it is regular. Consequently, if $B(\omega_R) = \overline{R}$, then $B(\omega_R)$ is regular.

We will assume now that $b(\omega_R) = (R : \overline{R})$. Considering that $\overline{R}$ is a finitely generated R-module by Proposition 2.1.162, we find that $\overline{R}$ is reflexive by [DMS21, Corollaries 4.10 and 4.28] so that

$$\overline{R} = (R : (R : \overline{R})) \cong b(\omega_R)^* \cong \mathfrak{b}_{\omega_R}^{**} \cong \mathfrak{b}_{\omega_R} \cong B(\omega_R),$$

where $\mathfrak{b}_{\omega_R}^{**} \cong \mathfrak{b}_{\omega_R}$ holds by [DMS21, Corollary 4.29] and $\mathfrak{b}_{\omega_R} \cong B(\omega_R)$ holds by Proposition 3.2.9.

If $B(\omega_R) = \overline{R}$, then $B(\omega_R)$ is Gorenstein. By Theorem 3.2.10, we conclude that the regular trace ideal $\operatorname{tr}(\mathfrak{b}_{\omega_R}) = b(\omega_R) \cong \mathfrak{b}_{\omega_R}^*$ is stable. By [DMS21, Corollary 3.8], it follows that $\mathfrak{b}_{\omega_R}^* \cong \mathfrak{b}_{\omega_R}^{**} \cong \mathfrak{b}_{\omega_R}$. We conclude that $\mathfrak{b}_{\omega_R} \cong b(\omega_R) = (R : \overline{R})$. Last, if $\mathfrak{b}_{\omega_R} = (R : \overline{R})$, then $\mathfrak{b}_{\omega_R}$ is a regular stable trace ideal by [DMS21, Corollary 3.2], hence we have that $\mathfrak{b}_{\omega_R}^* \cong \mathfrak{b}_{\omega_R} = (R : \overline{R})$ as before. □

Definition 3.2.22. Let $(R, \mathfrak{m}, k)$ be an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field k and canonical ideal ω_R. If any of the equivalent conditions of Theorem 3.2.21, we say that R has the **regular canonical blow-up** (RCB) property (or R is RCB).

Recall that a one-dimensional Cohen-Macaulay local ring with a canonical module $R \subseteq C \subseteq \overline{R}$ such that $C \cong \omega_R$ and module-finite integral closure $\overline{R}$ is **far-flung Gorenstein** if $\operatorname{tr}(\omega_R) = (R : \overline{R})$ (cf. [HKS21, Definition 2.3]). We demonstrate next that a far-flung Gorenstein ring is GCB.

Corollary 3.2.23. *Let R be as in Theorem 3.2.21. If R is far-flung Gorenstein, then R is RCB.*

Proof. Observe that the canonical ideal ω_R of R has a principal reduction $x \in \omega_R$. Consequently, $C = \omega_R/x$ is a canonical module such that $R \subseteq C \subseteq \overline{R}$ and $C \cong \omega_R$. If R is far-flung Gorenstein, then by [HKS21, Definition 2.3], we have that $\operatorname{tr}(\omega_R) = (R : \overline{R})$. Considering that $\mathfrak{b}_{\omega_R}$ is ω_R-Ulrich, it follows by [DMS21, Corollary 3.6 and Proposition 4.19] that $(R : \overline{R}) \subseteq \operatorname{tr}(\mathfrak{b}_{\omega_R}) \subseteq \operatorname{tr}(\omega_R) = (R : \overline{R})$. We conclude that $b(\omega_R) = \operatorname{tr}(\mathfrak{b}_{\omega_R}) = \operatorname{tr}(\omega_R) = (R : \overline{R})$ and $B(\omega_R) = \overline{R}$ by Theorem 3.2.21. □

3.3 The Canonical Blow-Up of a Numerical Semigroup

We turn our attention to the case that $R = K[\![S]\!] = K[\![t^s \mid s \in S]\!]$ is the numerical semigroup ring in indeterminate t associated to the numerical semigroup S and the infinite field K. Observe that R is

a one-dimensional complete Noetherian local domain and hence Cohen-Macaulay. By a result of Nagata in [Nag50], the integral closure $\overline{R}$ of R is module-finite. Consequently, R is an analytically unramified one-dimensional Cohen-Macaulay local ring with infinite residue field K.

Considering the correspondence between the numerical semigroup ring $R = K[\![S]\!]$ and the numerical semigroup S, a natural starting point to begin to understand the properties of $K[\![S]\!]$ is to examine the properties of S. Particularly, if we wish to study the canonical blow-up ring $B(\omega_R)$, then it makes sense to study the corresponding **canonical blow-up** numerical semigroup $B_S(\Omega)$ associated to S and its **relative canonical ideal** Ω as defined in Definition 3.3.7.

We say that a nonempty subset $S \subseteq \mathbb{Z}_{\geq 0}$ is a **numerical semigroup** whenever S is a submonoid of $\mathbb{Z}_{\geq 0}$ such that $\mathbb{Z}_{\geq 0} \setminus S$ is finite. Every numerical semigroup has a unique set of minimal generators $a_1 < \cdots < a_n$ (cf. [GR09, Theorem 2.7]). We will henceforth denote by $S = \langle a_1, \ldots, a_n \rangle$ the numerical semigroup with unique minimal generating set $a_1 < \cdots < a_n$. We refer to the cardinality of the unique minimal generating set of S as the **embedding dimension** $\mu(S)$ of S; the least element of S is its **multiplicity** $e(S)$. Particularly, if $S = \langle a_1, \ldots, a_n \rangle$, then $e(S) = a_1$. By Proposition 2.4.26, the embedding dimension and multiplicity of the numerical semigroup S are equal to the embedding dimension and multiplicity of the numerical semigroup ring $K[\![S]\!]$ for a field K. Consequently, we have that $\mu(S) \leq e(S)$; if equality holds, then S has **maximal embedding dimension**. By an abuse of terminology, we will say in this case that S has **minimal multiplicity**.

Considering that the cardinality of $\mathbb{Z}_{\geq 0} \setminus S$ is finite for any numerical semigroup S, the largest non-negative integer not contained in S is well-defined; it is the **Frobenius number** of S

$$\mathrm{F}(S) = \max\{n \in \mathbb{Z}_{\geq 0} \mid n \notin S\}.$$

Example 3.3.1. Consider the numerical semigroup $S = \langle 4, 11, 13, 18 \rangle$. One can verify that the generating set $\{4, 11, 13, 18\}$ is minimal. We have that $\mu(S) = 4$, $e(S) = 4$, and $\mathrm{F}(S) = 14$.

We say that an integer $n \in \mathbb{Z}_{\geq 0} \setminus S$ is **pseudo-Frobenius** whenever we have that $n + s \in S$ for

all nonzero elements $s \in S$. We define the **pseudo-Frobenius numbers**

$$\mathrm{PF}(S) = \{n \in \mathbb{Z}_{\geq 0} \setminus S \mid n + s \in S \text{ for all nonzero elements } s \in S\}.$$

We refer to $r(S) = |\mathrm{PF}(S)|$ as the **type** of S. Observe that the Frobenius number of S is the largest pseudo-Frobenius number of S. We prescribe a partial order of $\mathbb{Z}$ by declaring that $a \leq_S b$ if and only if $b - a \in S$. We note that the following lemma is well-known (cf. [GR09, Proposition 2.19]).

Proposition 3.3.2. *Let S be a numerical semigroup with the partial order $\leq_S$. We have that*

$$\mathrm{Maximal}_{\leq_S}(\mathbb{Z}_{\geq 0} \setminus S) = \mathrm{PF}(S).$$

Recall that a nonempty set $I \subseteq \mathbb{Z}$ is a (relative) **ideal** of S if $S + I \subseteq I$ and there exists an element $s \in S$ such that $s + I \subseteq S$. Clearly, $\mathfrak{M} = S \setminus \{0\}$ is a proper ideal of S that is maximal with respect to inclusion among all proper ideals of S. Likewise, $\Omega = \{-n \mid n \in \mathbb{Z} \setminus S\}$ is a relative ideal of S. Because of their significance, we distinguish these two ideals by name.

Definition 3.3.3. Let S be a numerical semigroup. We refer to the ideals $\mathfrak{M} = S \setminus \{0\}$ as the **maximal ideal** of S and $\Omega = \{-n \mid n \in \mathbb{Z} \setminus S\}$ as the **relative canonical ideal** of S.

Remark 3.3.4. We note that the unique maximal ideal of the numerical semigroup ring $R = K[\![S]\!]$ corresponding to S is given by $\mathfrak{m} = (t^s \mid s \in \mathfrak{M})$ and the usual canonical module of R is given by $\omega = R[\![t^w \mid w \in \Omega]\!]$, hence there is no coincidence among the terminologies used.

Remark 3.3.5. Often, in the literature of numerical semigroups, the relative canonical ideal of S is defined as $C = \{n \in \mathbb{Z} \mid \mathrm{F}(S) - n \notin S\}$. Observe that C consists of positive integers and contains S. One can verify that $C = \{\mathrm{F}(S) - n \mid n \in \mathbb{Z} \setminus S\} = \mathrm{F}(S) + \Omega$. Later, we will discuss certain properties of S that are defined in terms of its maximal ideal $\mathfrak{M}$ and its relative canonical ideal C.

Remark 3.3.6. Every proper ideal of a numerical semigroup S is finitely generated. Consequently, every relative ideal I of S is finitely generated. Explicitly, there exists an element $s \in S$ such that

$s+I \subseteq S$. Considering that $s+I$ is a proper ideal of S, there exist elements $x_1,\ldots,x_k \in I$ such that $s+I$ is generated by $s+x_1,\ldots,s+x_k$. But this implies that I is generated by $x_1,\ldots,x_k$.

By [Lip71, Proposition 1.1], the blow-up of a stable ideal I of R is given by $B(I) = R[I/x]$ for some non-zero divisor x of I. Considering that R is Noetherian, the ideal I is finitely generated by some elements $x_1 = x, x_2, \ldots, x_k$, and we have that $B(I) = R[x_i/x_1 \mid 1 \leq i \leq k]$. Based on this observation, we make the following analogous definitions for numerical semigroups.

Definition 3.3.7. Let S be a numerical semigroup. Let $I \subseteq \mathbb{Z}$ be a relative ideal of S generated by $x_1 < \cdots < x_k$. We define the **blow-up** of S with respect to I as $B_S(I) = S + \mathbb{Z}_{\geq 0}\langle x_i - x_1 \mid 1 \leq i \leq k\rangle$.

Definition 3.3.8. Let S be a numerical semigroup with relative canonical ideal Ω. We refer to the blow-up $B_S(\Omega)$ of S with respect to Ω as the **canonical blow-up** of S. Further, we say that S has the **Gorenstein canonical blow-up** (GCB) property if the canonical blow-up $B_S(\Omega)$ of S is symmetric.

Our next proposition conveniently describes the canonical blow-up. Before this, we record the following well-known fact for which we could not find a reference.

Lemma 3.3.9. *Let S be a numerical semigroup. We have that $\Omega = \{-x \mid x \in \mathrm{PF}(S)\} + S$.*

Proof. Consider an integer $n \notin S$. If $n < 0$, then $-n = -\mathrm{F}(S) + (\mathrm{F}(S) - n)$ yields an expression of $-n$ as an element of $\{-x \mid x \in \mathrm{PF}(S)\} + S$. On the other hand, suppose that $n > 0$. If $n \in \mathrm{PF}(S)$, then clearly $-n$ belongs to $\{-x \mid x \in \mathrm{PF}(S)\} + S$, so we may assume that $n \notin \mathrm{PF}(S)$. By Proposition 3.3.2, there exists an element $x \in \mathrm{PF}(S)$ such that $x - n \in S$. We conclude that $-n = -x + (x - n)$ yields an expression of $-n$ as an element of $\{-x \mid x \in \mathrm{PF}(S)\} + S$.

Conversely, every element of the form $-x + s$ with $x \in \mathrm{PF}(S)$ and $s \in S$ can be written as $-(x - s)$. Observe that $x - s$ cannot belong to S because x does not belong to S. □

Proposition 3.3.10. *Let S be a numerical semigroup with relative canonical ideal Ω. We have that*

$$B_S(\Omega) = S + \mathbb{Z}_{\geq 0}\langle \mathrm{F}(S) - x \mid x \in \mathrm{PF}(S)\rangle.$$

Proof. Observe that Ω is finitely generated by $\{-x \mid x \in \mathrm{PF}(S)\}$; its least element is $-\mathrm{F}(S)$. By definition, we conclude that $B_S(\Omega) = S + \mathbb{Z}_{\geq 0}\langle \mathrm{F}(S) - x \mid x \in \mathrm{PF}(S)\rangle$. □

Until now, we have made reference to the set of pseudo-Frobenius numbers $\mathrm{PF}(S)$ without any indication of how to obtain $\mathrm{PF}(S)$ in practice. We outline the procedure as follows.

Recall that the **Apéry set** $\mathrm{Ap}(n,S) = \{s \in S \mid s - n \notin S\}$ of S with respect to a nonzero element $n \in S$. We record two well-known propositions that allow us to compute the pseudo-Frobenius numbers of a numerical semigroup; then, we illustrate the process in an example.

Proposition 3.3.11. *[GR09, Lemma 2.4] Let S be a numerical semigroup. Let $w(i)$ denote the least element of S that is congruent to i modulo n. We have that* $\mathrm{Ap}(n,S) = \{w(0), w(1), \ldots, w(n-1)\}$.

Proposition 3.3.12. *[GR09, Proposition 2.20] Let S be a numerical semigroup. If $n \in S \setminus \{0\}$, then* $\mathrm{PF}(S) = \{x - n \mid x \in \mathrm{Ap}(n,S)$ *is maximal with respect to* $\leq_S\}$. *Particularly, we have that*

$$\mathrm{PF}(S) = \{x - e(S) \mid x \in \mathrm{Ap}(e(S),S) \text{ is maximal with respect to } \leq_S\}.$$

Example 3.3.13. Consider the numerical semigroup $S = \langle 4, 11, 13, 18\rangle$ of the Example 3.3.1. We will use the previous proposition show that $\mathrm{F}(S) = 14$. By Proposition 3.3.12, it suffices to begin with $\mathrm{Maximal}_{\leq_S} \mathrm{Ap}(4,S)$. By Proposition 3.3.11, we have that $\mathrm{Ap}(4,S) = \{w(0), w(1), w(2), w(3)\}$, where $w(i)$ denotes the least element of S congruent to i modulo 4. By construction, we have that

$$\mathrm{Ap}(4,S) = \{0, 11, 13, 18\} \text{ and } \mathrm{Maximal}_{\leq_S} \mathrm{Ap}(4,S) = \{11, 13, 18\}.$$

Consequently, we have that $\mathrm{PF}(S) = \{7, 9, 14\}$ so that $\mathrm{F}(S) = 14$ and $B_S(\Omega) = \langle 4, 5, 7\rangle$.

Ultimately, our aim in this section is to understand when the canonical blow-up of a numerical semigroup ring is Gorenstein. Bearing this in mind, we recall that a numerical semigroup S is **symmetric** if $\mathrm{F}(S)$ is odd and for every integer $x \geq 1$, either $x \in S$ or $\mathrm{F}(S) - x \in S$ (cf. [GR09, Proposition 4.4]). One immediate consequence of this definition is that a symmetric numerical semigroup only has one pseudo-Frobenius number. We note that the converse is also true.

Proposition 3.3.14. *[GR09, Corollary 4.11] The following statements are equivalent.*

(1.) *S is a symmetric numerical semigroup.*

(2.) *We have that* $\mathrm{PF}(S) = \{\mathrm{F}(S)\}$.

(3.) *We have that* $r(S) = |\mathrm{PF}(S)| = 1$.

Fröberg demonstrated in [Frö94] that the type of a numerical semigroup S is equal to the Cohen-Macaulay type of the corresponding numerical semigroup ring $K[\![S]\!]$. Earlier, in [Her69, Theorem 3.13 and Corollary 3.2.2], Herzog established that $K[\![S]\!]$ is Gorenstein if and only if S is symmetric. We will often refer to a symmetric numerical semigroup as Gorenstein.

Recall that a numerical semigroup S of embedding dimension two is Gorenstein (cf. [GR09, Example 2.22]). Consequently, any numerical semigroup with 2 as a generator is Gorenstein.

Theorem 3.3.15. *Every numerical semigroup of minimal multiplicity three is GCB. Consequently, every numerical semigroup of multiplicity at most three is GCB.*

Proof. By the exposition preceding the statement of the proposition, it suffices to prove that a numerical semigroup $S = \langle 3, a, b\rangle$ of minimal multiplicity is GCB. By [AG14, Proposition 31], we have that $\mathrm{Ap}(3,S) = \{0,a,b\}$ so that $\mathrm{PF}(S) = \{a-3, b-3\}$. By Proposition 3.3.10, we have that $B_S(\Omega) = \langle 3, a, b-a\rangle$. Observe that b cannot belong to $\langle 3, a\rangle$ by assumption, hence we must have that $b \leq \mathrm{F}(\langle 3,a\rangle) = 2a-3$ so that $b-a \leq a-3$. We claim that $B_S(\Omega) = \langle 3, b-a\rangle$. By hypothesis that S has minimal multiplicity, we must have that $a \equiv 1 \pmod 3$ and $b \equiv 2 \pmod 3$ or vice-versa. Either way, we have that $2a \equiv b \pmod 3$ so that $a \equiv (b-a) \pmod 3$ and $B_S(\Omega) = \langle 3, b-a\rangle$. Our proof is complete, as any numerical semigroup of embedding dimension two is Gorenstein. □

Our next proposition illustrates that the previous proposition fails for larger multiplicity.

Proposition 3.3.16. *The numerical semigroup $S = \langle 4, 11, 13, 18\rangle$ of Examples 3.3.1 and 3.3.13 has minimal multiplicity four but does not have the Gorenstein canonical blow-up property.*

Proof. By Example 3.3.1 and [AG14, Proposition 31], we have that $e(S) = \mu(S) = 4$. By Example 3.3.13, we have that $B_S(\Omega) = \langle 4, 5, 7\rangle$. Observe that $\mathrm{Ap}(4, B_S(\Omega)) = \{0,5,7,10\}$ so that $\mathrm{Maximal}_{\leq_S} \mathrm{Ap}(4, B_S(\Omega)) = \{7, 10\}$. Consequently, $r(B_S(\Omega)) = 2$, so $B_S(\Omega)$ is not Gorenstein. □

Based on the previous two examples, the following question is natural.

Question 3.3.17. Let S be a numerical semigroup. Does it always holds that $r(B_S(\Omega)) \leq r(S)$?

Example 3.3.18. Consider the numerical semigroup $S = \langle 8,9,10,11,13,14,15\rangle$. One can verify that $\mathrm{PF}(S) = \{5,6,7,12\}$ so that $r(S) = 4$. On the other hand, we have that $B_S(\Omega) = \langle 5,6,7,8,9\rangle$ with $\mathrm{PF}(B_S(\Omega)) = \{1,2,3,4\}$, hence we have that $r(B_S(\Omega)) = r(S)$.

Our next proposition exhibits a family of numerical semigroups with $r(S) = r(B_S(\Omega))$.

Proposition 3.3.19. *Let $k \geq 2$ be an integer. Let S be the numerical semigroup generated by the punctured discrete interval $\{2k, 2k+1, \ldots, 4k-1\} \setminus \{3k\}$. The following properties hold.*

(1.) *We have that* $\mathrm{PF}(S) = \{k+1, k+2, \ldots, 2k-1, 3k\}$. *Particularly, we have that* $r(S) = k$.

(2.) *We have that* $B_S(\Omega) = \langle k+1, k+2, \ldots, 2k, 2k+1\rangle$.

(3.) *We have that* $\mathrm{PF}(B_S(\Omega)) = \{1, \ldots, k-1, k\}$. *Particularly, we have that* $r(B_S(\Omega)) = k$.

Proof. (1.) Clearly, for each integer $1 \leq i \leq k-1$ or $k+1 \leq i \leq 2k-1$, we have that $w(i) = 2k+i$, where $w(i)$ denotes the smallest element of S congruent to i modulo $2k$. We claim that $w(k) = 5k$. Certainly, $5k = 2(2k) + k = (2k+1) + (3k-1)$ is an element of S congruent to k modulo $2k$. Considering that the only integers smaller than $5k$ that are congruent to k modulo $2k$ are k and $3k$ and do not belong to S, we conclude that $w(k) = 5k$. By Proposition 3.3.11, we have that

$$\mathrm{Ap}(2k, S) = \{0, 2k+1, 2k+2, \ldots, 3k-1, 3k+1, \ldots, 4k-1, 5k\}.$$

Observe that for each integer $2k+1 \leq i \leq 3k-1$, we have that $2k+1 \leq 5k-i \leq 3k-1$ so that $5k-i$ belongs to S and $i \leq_S 5k$. On the other hand, for all integers $3k+1 \leq i < j \leq 4k-1$, we have that $5k-i \leq 2k-1$ does not belong to S and $1 \leq j-i \leq k-2$ does not belong to S. Consequently, the elements $3k+1, \ldots, 4k-1$, and $5k$ of $\mathrm{Ap}(2k, S)$ are all incomparable with respect to $\leq_S$, and we conclude that $\mathrm{Maximal}_{\leq_S} \mathrm{Ap}(2k, S) = \{3k+1, \ldots, 4k-1, 5k\}$. By Proposition 3.3.12, we find that $\mathrm{PF}(S) = \{k+1, \ldots, 2k-1, 3k\}$, as desired.

(2.) By the previous paragraph, we have that $\mathrm{F}(S) = 3k$. By Proposition 3.3.10, we find that

$$B_S(\Omega) = \mathbb{Z}_{\geq 0}\langle k+1, \ldots, 2k-1, 2k, 2k+1, \ldots, 3k-1, 3k+1, \ldots, 4k-1\rangle.$$

But every integer greater than or equal to $2k+2$ belongs to $\langle k+1, \ldots, 2k, 2k+1\rangle$, hence we conclude that $B_S(\Omega) = \langle k+1, \ldots, 2k, 2k+1\rangle$.

(3.) One can readily verify that $\mathrm{Ap}(k+1, B_S(\Omega)) = \{0, k+2, \ldots, 2k, 2k+1\}$. Further, any pair of nonzero elements from this set are incomparable with respect to $\leq_S$, hence we have that $\mathrm{Maximal}_{\leq_S} \mathrm{Ap}(k+1, B_S(\Omega)) = \{k+2, \ldots, 2k, 2k+1\}$ so that $\mathrm{PF}(B_S(\Omega)) = \{1, \ldots, k-1, k\}$. □

Given any two relative ideals $I, J \subseteq \mathbb{Z}$ of S, recall that $I - J = \{n \in \mathbb{Z} \mid n + J \subseteq I\}$ is a relative ideal of S. Our next two definitions are well-known.

Definition 3.3.20. [HHS19, Lemma 1.1 and Definition 2.2] We say that a numerical semigroup S is **nearly Gorenstein** if it holds that $\mathfrak{M} \subseteq C + (S - C)$.

Definition 3.3.21. [BF97, Proposition 4] We say that a numerical semigroup S is **almost Gorenstein** if it holds that $\mathfrak{M} + C = \mathfrak{M}$.

Every almost Gorenstein numerical semigroup is nearly Gorenstein. Observe that if S is almost Gorenstein, then $\mathfrak{M} + C = \mathfrak{M} \subseteq S$ implies that $\mathfrak{M} \subseteq (S - C) \subseteq C + (S - C)$ so that S is nearly Gorenstein. Generally, the converse does not hold. By the remarks following [MS21, Proposition 1.3], the numerical semigroup $S = \langle 4, 5, 11\rangle$ is nearly Gorenstein but not almost Gorenstein. Explicitly, for this numerical semigroup, we have that $C = S \cup \{1, 6\}$ so that $\mathfrak{M} + C \supsetneq \mathfrak{M}$. Our next proposition illustrates that an almost Gorenstein numerical semigroup is not necessarily GCB.

Proposition 3.3.22. *The numerical semigroup $S = \langle 4, 7, 9\rangle$ is almost Gorenstein (and hence nearly Gorenstein) but does not have the Gorenstein canonical blow-up property.*

Proof. One can verify that $C = S \cup \{5\}$ and $5 + \mathfrak{M} \subseteq \mathfrak{M}$, hence S is almost Gorenstein. On the other hand, $\mathrm{Ap}(4, S) = \{0, 7, 9, 14\}$ so that $\mathrm{Maximal}_{\leq_S} \mathrm{Ap}(4, S) = \{9, 14\}$ and $\mathrm{PF}(S) = \{5, 10\}$. We conclude that $B_S(\Omega) = \langle 4, 5, 7\rangle$, which is not Gorenstein by Proposition 3.3.16. □

We note that $S = \langle 4,7,9\rangle$ has $e(S) = 4 > 3 = \mu(S)$, hence it is not of minimal multiplicity. By Corollary 3.2.19, any almost Gorenstein numerical semigroup of minimal multiplicity is GCB.

3.4 Divisive Numerical Semigroups

We introduce in this section a class of numerical semigroups whose canonical blow-ups are regular. We characterize these numerical semigroups in terms of their pseudo-Frobenius numbers. Before this, we introduce the notion of the difference-Frobenius numbers.

Definition 3.4.1. Let S be a numerical semigroup. We define the **difference-Frobenius numbers**

$$\mathrm{DF}(S) = \{\mathrm{F}(S) - x \mid x \in \mathrm{PF}(S)\}$$

of S. We refer to an element of $\mathrm{DF}(S)$ as **difference-Frobenius**.

Because a numerical semigroup is not uniquely determined by its pseudo-Frobenius numbers, it is not uniquely determined by its difference-Frobenius numbers.

Our next proposition demonstrates an important connection between the difference-Frobenius numbers and the pseudo-Frobenius numbers of a numerical semigroup. Out of desire for future notational convenience, for any finite set $X \subseteq \mathbb{Z}_{\geq 0}$, we adopt the shorthand

$$nX = \underbrace{X + X + \cdots + X}_{n \text{ summands}} = \{x_1 + x_2 + \cdots + x_n \mid x_1, x_2, \ldots, x_n \in X\}.$$

Under this convention, we have that $2X = X + X$. Clearly, if $Y \subseteq X$, then we have that $nY \subseteq nX$.

Proposition 3.4.2. *Let S be a numerical semigroup. The following conditions are equivalent.*

(1.) *We have that* $B_S(\Omega) = \mathbb{Z}_{\geq 0}$.

(2.) *We have that* $1 \in \mathrm{DF}(S)$.

(3.) *We have that* $\mathrm{F}(S) - 1 \in \mathrm{PF}(S)$.

(4.) *We have that* $\mathrm{F}(S) - 1 \notin S$.

(5.) *There exists an integer* $n \geq 1$ *such that* $\{0,1,\ldots,e(S)-1\} \subseteq n\,\mathrm{DF}(S)$.

Proof. By Proposition 3.3.10, we have that $B_S(\Omega) = S + \mathbb{Z}_{\geq 0}\langle d \mid d \in \mathrm{DF}(S)\rangle$, hence conditions (1.) and (2.) are equivalent. Conditions (2.) and (3.) are equivalent by definition. Clearly, condition (3.) implies condition (4.). Conversely, if $\mathrm{F}(S)-1 \notin S$, then $\mathrm{F}(S)-1$ must be pseudo-Frobenius, as $e(S) \geq 2$. Last, if $1 \in \mathrm{DF}(S)$, then $\{0,1,\ldots,e(S)-1\} \subseteq (e(S)-1)\,\mathrm{DF}(S)$. Conversely, if $1 \notin \mathrm{DF}(S)$, then $1 \notin n\,\mathrm{DF}(S)$ for any integer $n \geq 0$. We conclude that (2.) and (5.) are equivalent. □

Definition 3.4.3. We say that a numerical semigroup S is **divisive** if it satisfies any of the equivalent conditions of Proposition 3.4.2.

Corollary 3.4.4. *Every divisive numerical semigroup is GCB.*

Remark 3.4.5. If S is divisive, then $\mathrm{F}(S)-1 \in \mathrm{PF}(S)$ so that S is not Gorenstein. By the exposition preceding Proposition 3.3.15, a numerical semigroup S of embedding dimension 2 is not divisive.

Remark 3.4.6. Let S be a numerical semigroup. By [HKS21, Proposition 6.1], we have that S is far-flung Gorenstein if and only if $\{0,1,\ldots,e(S)-1\} \subseteq 2\,\mathrm{DF}(S)$. Consequently, if S is far-flung Gorenstein, then we must have that $1 \in \mathrm{DF}(S)$, hence S is divisive.

Corollary 3.4.7. *If* S *is a divisive numerical semigroup and* $e(S) = 3$, *then* S *is far-flung Gorenstein.*

Our next objective is to point out further examples of divisive numerical semigroups that are simple to describe. Before this, we record a lemma motivated by [GR99, Corollaries 4 and 5]. We will adopt the notation $m \bmod n$ to denote the remainder of a positive integer m when divided by a positive integer $n < m$. Explicitly, by the Division Algorithm, there exists a positive integer q and a non-negative integer $r < n$ such that $m = qn + r$. We denote $r = m \bmod n$.

Lemma 3.4.8. *Let* m *and* n *be positive integers with* $n < m$. *We have that* $m = \left\lfloor \frac{m}{n} \right\rfloor n + m \bmod n$. *Consequently, if* $n \nmid m$, *then* $\left\lfloor \frac{m}{n} \right\rfloor = \left\lceil \frac{m}{n} \right\rceil - 1$. *If* $n \mid m$, *then* $\left\lfloor \frac{m}{n} \right\rfloor = \left\lceil \frac{m}{n} \right\rceil$.

Proof. By the Division Algorithm, there exists a positive integer q and a non-negative integer $r < n$ such that $m = qn + r$. Observe that

$$\left\lfloor \frac{m}{n} \right\rfloor = \left\lfloor q + \frac{r}{n} \right\rfloor = q + \left\lfloor \frac{r}{n} \right\rfloor = q,$$

where the second equality holds because q is an integer, and the third equality holds because $r < n$. Consequently, we have that

$$m = qn + r = \left\lfloor \frac{m}{n} \right\rfloor n + r = \left\lfloor \frac{m}{n} \right\rfloor n + m \bmod n.$$

If $n \nmid m$, we have that $r > 0$ so that

$$\left\lfloor \frac{m}{n} \right\rfloor = \left\lfloor q + \frac{r}{n} \right\rfloor = q + \left\lfloor \frac{r}{n} \right\rfloor = q = (q+1) - 1 = q + \left\lceil \frac{r}{n} \right\rceil - 1 = \left\lceil q + \frac{r}{n} \right\rceil - 1 = \left\lceil \frac{m}{n} \right\rceil - 1,$$

where the second and sixth equalities hold because q is an integer, and the third and fifth equalities hold because $r < n$ by the Division Algorithm; otherwise, we have that $n \mid m$ so that $r = 0$ and $\frac{m}{n} = q$ is a positive integer, from which the third claim follows. □

Proposition 3.4.9. *Let m and n be integers such that $m > n \geq 2$ and $(m-1) \bmod n \neq 1$. Consider the numerical semigroup generated by the discrete interval $\{m, m+1, m+2, \ldots, m+n\}$, i.e.,*

$$S = \langle m, m+1, m+2, \ldots, m+n \rangle.$$

If either (a.) m is odd or (b.) m is even and $n \geq 3$, then $\mathrm{F}(S) - 1 \notin S$.

Proof. It suffices to show that $\mathrm{F}(S) + m - 1 \in \mathrm{Ap}(m, S)$. For if this is the case, then $\mathrm{F}(S) + m - 1$ is a maximal element of $\mathrm{Ap}(m, S)$ with respect to $\leq_S$ and therefore $\mathrm{F}(S) - 1$ is pseudo-Frobenius. By [GR99, Corollary 4], it suffices to show that $\mathrm{F}(S) + m - 1 = qm + (q-1)n + r$ for some positive integer q and some integer $1 \leq r \leq n$ such that $(q-1)n + r < m$. We proceed by cases.

(i.) If $(m-1) \bmod n = 0$, then $n \mid (m-1)$ so that $\left\lfloor \frac{m-1}{n} \right\rfloor = \left\lceil \frac{m-1}{n} \right\rceil$ by the above lemma. By [GR99, Corollary 5], we have that $\mathrm{F}(S) = \left\lceil \frac{m-1}{n} \right\rceil m - 1$. Observe that

$$\mathrm{F}(S) + m - 1 = \left\lceil \frac{m-1}{n} \right\rceil m + m - 2 = \left\lceil \frac{m-1}{n} \right\rceil m + \left(\left\lfloor \frac{m-1}{n} \right\rfloor - 1 \right) n + (n-1),$$

where we have that $m - 1 = \left\lfloor \frac{m-1}{n} \right\rfloor n$ by the lemma. Consequently, we have written $\mathrm{F}(S) +$

$m-1$ as $qm+(q-1)n+r$ with $q=\left\lfloor \frac{m-1}{n} \right\rfloor = \left\lceil \frac{m-1}{n} \right\rceil$, $r=n-1$, and $(q-1)n+r=m-2$.

(ii.) If $(m-1) \bmod n \geq 2$, then $n \nmid (m-1)$ so that $\left\lfloor \frac{m-1}{n} \right\rfloor = \left\lceil \frac{m-1}{n} \right\rceil - 1$ by the above lemma. Further, we have that $[(m-1) \bmod n] - 1 \geq 1$. We have therefore that

$$\mathrm{F}(S)+m-1 = \left\lceil \frac{m-1}{n} \right\rceil m + m - 2 = \left\lceil \frac{m-1}{n} \right\rceil m + \left\lfloor \frac{m-1}{n} \right\rfloor n + [(m-1) \bmod n] - 1$$

$$= \left\lceil \frac{m-1}{n} \right\rceil m + \left(\left\lceil \frac{m-1}{n} \right\rceil - 1 \right) n + [(m-1) \bmod n] - 1.$$

Consequently, we have written $\mathrm{F}(S)+m-1$ as $qm+(q-1)n+r$ for the integers $q=\left\lceil \frac{m-1}{n} \right\rceil$, $1 \leq r = [(m-1) \bmod n] - 1 \leq n$, and $(q-1)n+r=m-2$.

Either way, we have that $\mathrm{F}(S)+m-1 \in \mathrm{Ap}(m,S)$, and our proof is complete. □

Remark 3.4.10. We cannot relax our assumption that $(m-1) \bmod n \neq 1$. Consider the case that $m=5$ and $n=3$. We have that $m-1=4=3\cdot 1+1$ so that $(m-1) \bmod n = 1$. By [GR99, Corollary 5], we have that $\mathrm{F}(S)+m-1 = \left\lceil \frac{4}{3} \right\rceil 5+5-2=13$ so that $\mathrm{F}(S)-1=8=5+3$ belongs to S. On the other hand, if $m=8$ and $n=3$, then $m-1=7=3\cdot 2+1$ so that $(m-1) \bmod n = 1$. We have that $\mathrm{F}(S)+m-1 = \left\lceil \frac{7}{3} \right\rceil 8+8-2=30$ so that $\mathrm{F}(S)-1=22=2(8+3)$ belongs to S.

We note that if m is even, we cannot relax our assumption that $n \geq 3$. By [GR99, Corollary 9], if $n=2$, then S is a complete intersection, so $\mathrm{F}(S)$ is the only pseudo-Frobenius number.

Proposition 3.4.11. *Let m and n be integers such that $m > n \geq 2$ and $(m-1) \bmod n = 1$. Consider the numerical semigroup $S = \langle m, m+1, m+2, \ldots, m+n \rangle$. We have that* $\mathrm{F}(S)-1 \in S$.

Proof. In case $(m-1) \bmod n = 1$, it follows that $m-1 = \left\lfloor \frac{m-1}{n} \right\rfloor n + 1$ so that

$$\mathrm{F}(S)+m-1 = \left\lceil \frac{m-1}{n} \right\rceil m + \left\lfloor \frac{m-1}{n} \right\rfloor n = (m+n) \left\lfloor \frac{m-1}{n} \right\rfloor + m.$$

We conclude that $\mathrm{F}(S)-1$ is divisible by $m+n$ and must therefore belong to S. □

We summarize the content of Propositions 3.4.9 and 3.4.11 in the following theorem.

Theorem 3.4.12. *Let S be a numerical semigroup generated by an interval, i.e., let*

$$S = \langle m, m+1, m+2, \ldots, m+n \rangle$$

for some integers $m > n \geq 2$. The following statements are equivalent.

(1.) *We have that $(m-1) \bmod n \neq 1$ and either (a.) m is odd or (b.) m is even and $n \geq 3$.*

(2.) *S is divisive, i.e., we have that $\mathrm{F}(S) - 1 \in \mathrm{PF}(S)$.*

Other than numerical semigroups generated by intervals, we will also classify all divisive numerical semigroups of **maximal embedding dimension**. We recall the definition for convenience.

Definition 3.4.13. Let S be a numerical semigroup. We say that S has **maximal embedding dimension** if the embedding dimension of S is equal to the multiplicity of S, i.e., $\mu(S) = e(S)$.

Consequently, S has maximal embedding dimension if and only if there exist minimal generators $a_1 < \cdots < a_{\mu(S)}$ of S such that $\mu(S) = e(S)$. We abbreviate this by e. By [AG14, Proposition 33], we have that $\mathrm{F}(S) = a_e - a_1$, hence S is divisive if and only if $a_e - a_1 - 1 \in \mathrm{PF}(S)$. Our next proposition classifies divisive numerical semigroups of maximal embedding dimension.

Theorem 3.4.14. *Let $S = \langle a_1, \ldots, a_e \rangle$ have maximal embedding dimension e.*

(1.) *If $e = 1$ or $e = 2$, then S is not divisive.*

(2.) *If $e \geq 3$, then S is divisive if and only if $a_{e-1} = a_e - 1$.*

Proof. Of course, if $e = 1$ or $e = 2$, then S is Gorenstein and hence must not be divisive. We may assume therefore that $e \geq 3$. If $a_{e-1} = a_e - 1$, it follows that a_{e-1} and a_e are incomparable with respect to $\leq_S$, hence we have that $a_{e-1} - a_1 = a_e - a_1 - 1 \in \mathrm{PF}(S)$ by [AG14, Proposition 31]. Conversely, we will assume that S is divisive so that $a_e - a_1 - 1 \in \mathrm{PF}(S)$. We conclude that $a_e - 1$ belongs to $\mathrm{Ap}(a_1, S)$. By [AG14, Proposition 31], we conclude that $a_{e-1} = a_e - 1$, as desired. □

3.5 Pinched Discrete Interval Numerical Semigroups

Previously, in Proposition 3.3.19, we illustrated that the numerical semigroup S generated by the punctured discrete interval $\{2k, 2k+1, 2k+2, \ldots, 4k-1\} \setminus \{3k\}$ satisfies $r(S) = r(B_S(\Omega)) = k$. Our focus in this section is to study the numerical semigroups obtained by removing more than one "central" element from the discrete interval $\{n, n+1, \ldots, 2n-1\}$ (cf. Definition 3.5.5). Our next propositions deal with the case in which all but the first and last two generators are deleted.

Proposition 3.5.1. *Let k be a positive integer. Let $n = 4k$. Let $S = \langle n, n+1, 2n-2, 2n-1 \rangle$.*

(1.) *We have that*

$$\begin{aligned}\mathrm{Ap}(n,S) = \{i(n+1) \mid 0 \leq i \leq 2k-1\} \cup \{k(2n-2)\} \\ \cup \{i(2n-2) + j(2n-1) \mid 0 \leq i \leq k-1 \text{ and } 0 \leq j \leq 1\}.\end{aligned}$$

(2.) *We have that*

$$\mathrm{Maximal}_{\leq_S} \mathrm{Ap}(n,S) = \{2kn-2k-1, 2kn-2k, 2kn-2k+1\}.$$

(3.) *We have that* $\mathrm{PF}(S) = \{2kn-6k-1, 2kn-6k, 2kn-6k+1\}$. *Particularly, S is divisive.*

Proof. (1.) By Proposition 3.3.11, it suffices to compute the least element $w(i)$ of S that is congruent to i modulo n for each integer $0 \leq i \leq n-1$. Each element of S is of the form

$$s = \alpha n + \beta(n+1) + \gamma(2n-2) + \delta(2n-1)$$

for some integers $\alpha, \beta, \gamma, \delta \geq 0$, hence the residue of an element of S modulo n is given by $\beta - 2\gamma - \delta$. Given an integer $0 \leq i \leq n-1$, we seek to minimize s subject to the constraint $\beta - 2\gamma - \delta \equiv i \pmod{n}$. Clearly, we can take $\alpha = 0$ because the residue of s modulo n does not depend on α. Observe that for each integer $0 \leq i \leq 2k-1$, there exists an integer $2k+1 \leq j \leq 4k$ such that $n = 4k = i + j$. Consequently, for each integer $0 \leq i \leq 2k-1$, we seek to minimize s subject to the

constraint $\beta - 2\gamma - \delta = i$. Considering that $\gamma \geq 0$ and $\delta \geq 0$, we have that $\beta \geq i$, so we minimize s precisely when $\beta = i$ and $\alpha = \gamma = \delta = 0$. We have therefore illustrated that $w(i) = i(n+1)$ for all integers $0 \leq i \leq 2k-1$. On the other hand, if we have that $2k+1 \leq i \leq 4k-1$, then there exists an integer $0 \leq j \leq 2k-1$ such that $n = 4k = i + j$, and our constraint becomes $2\gamma + \delta - \beta = j$. Like before, we find that $2\gamma + \delta \geq j$ by assumption that $\beta \geq 0$. Given that $j = 2\ell$ is even, we minimize s by taking $\gamma = \ell$ and $\alpha = \beta = \delta = 0$. On the other hand, if $j = 2\ell + 1$ is odd, we minimize s by taking $\gamma = \ell$, $\delta = 1$, and $\alpha = \beta = 0$. We conclude therefore that for each integer $2k+1 \leq i \leq n-1$, we have that $w(i) = \ell(2n-2) + m(2n-1)$ for some integers $0 \leq \ell \leq k-1$ and $0 \leq m \leq 1$. Last, in the case that $i = 2k$, our constraint can be viewed as $\beta - 2\gamma - \delta = 2k$ or $2\gamma + \delta - \beta = 2k$ because $2k$ and $-2k$ are congruent modulo $n = 4k$. By taking $\gamma = k$ and $\alpha = \beta = \delta = 0$, we minimize s.

(2.) Observe that for each pair of integers $0 \leq i < j \leq 2k-1$, we have that $(j-i)(n+1)$ belongs to S, hence any two elements of $\{i(n+1) \mid 0 \leq i \leq 2k-1\}$ are comparable; the largest among them is $(2k-1)(n+1) = 2kn - 2k - 1$. On the other hand, we have that

$$(k-1)(2n-2) + (2n-1) = 2kn - 2k + 1$$

is the largest element of $\{i(2n-2) + j(2n-1) \mid 0 \leq i \leq k-1 \text{ and } 0 \leq j \leq 1\}$. One can readily verify that the distinct elements of this set are comparable: they are of the form $(i-i')(2n-2)$ or $(i-i')(2n-2)+(2n-1)$ for some integers $0 \leq i < i' \leq k-1$. Considering that $k(2n-2) = 2kn - 2k$ belongs to $\mathrm{Ap}(n,S)$, we find that $\mathrm{Maximal}_{\leq_S} \mathrm{Ap}(n,S) = \{2kn-2k-1, 2kn-2k, 2kn-2k+1\}$.

(3.) By Propositions 3.3.12 and Definition 3.4.3, the claims follow at once from (2.) above. □

Proposition 3.5.2. *Let k be a positive integer. Let $n = 4k+2$. Let $S = \langle n, n+1, 2n-2, 2n-1 \rangle$.*

(1.) *We have that*

$$\mathrm{Ap}(n,S) = \{i(n+1) \mid 0 \leq i \leq 2k+1\} \cup \{k(2n-2)\} \cup \{i(2n-2) + j(2n-1) \mid 0 \leq i \leq k-1 \text{ and } 0 \leq j \leq 1\}.$$

(2.) *We have that* $\mathrm{Maximal}_{\leq_S} \mathrm{Ap}(n,S) = \{2kn+n+2k+1\}$.

(3.) *We have that* $\mathrm{PF}(S) = \{2kn+2k+1\}$. *Particularly, S is Gorenstein.*

Proof. (1.) By Proposition 3.3.11, it suffices to compute the least element $w(i)$ of S that is congruent to i modulo n for each integer $0 \leq i \leq n-1$. Each element of S is of the form

$$s = \alpha n + \beta(n+1) + \gamma(2n-2) + \delta(2n-1)$$

for some integers $\alpha, \beta, \gamma, \delta \geq 0$, hence the residue of an element of S modulo n is given by $\beta - 2\gamma - \delta$. Given an integer $0 \leq i \leq n-1$, we seek to minimize s subject to the constraint $\beta - 2\gamma - \delta \equiv i \pmod{n}$. Clearly, we can take $\alpha = 0$ because the residue of s modulo n does not depend on α. Observe that for each integer $0 \leq i \leq 2k$, there exists an integer $2k+2 \leq j \leq 4k$ such that $n = 4k+2 = i+j$. Consequently, for each integer $0 \leq i \leq 2k$, we seek to minimize s subject to the constraint $\beta - 2\gamma - \delta = i$. Considering that $\gamma \geq 0$ and $\delta \geq 0$, we have that $\beta \geq i$, so we minimize s precisely when $\beta = i$ and $\alpha = \gamma = \delta = 0$. We have therefore illustrated that $w(i) = i(n+1)$ for all integers $0 \leq i \leq 2k$. On the other hand, if we have that $2k+3 \leq i \leq 4k-1$, then there exists an integer $0 \leq j \leq 2k-1$ such that $n = 4k+2 = i+j$, and our constraint becomes $2\gamma + \delta - \beta = j$. Like before, we find that $2\gamma + \delta \geq j$ by assumption that $\beta \geq 0$. Given that $j = 2\ell$ is even, we minimize s by taking $\gamma = \ell$ and $\alpha = \beta = \delta = 0$. On the other hand, if $j = 2\ell+1$ is odd, we minimize s by taking $\gamma = \ell$, $\delta = 1$, and $\alpha = \beta = 0$. We conclude therefore that for each integer $2k+2 \leq i \leq n-1$, we have that $w(i) = \ell(2n-2) + m(2n-1)$ for some integers $0 \leq \ell \leq k-1$ and $0 \leq m \leq 1$.

Given that $i = 2k+1$, our constraint becomes $\beta - 2\gamma - \delta = 2k+1$. By taking $\beta = 2k+1$ and $\alpha = \gamma = \delta = 0$, we minimize s. Given that $i = 2k+2$, our constraint becomes $2\gamma + \delta - \beta = 2k$, in which case we minimize s by taking $\gamma = k$ and $\alpha = \beta = \delta = 0$.

(2.) Observe that for each pair of integers $0 \leq i < j \leq 2k+1$, we have that $(j-i)(n+1)$ belongs to S, hence any two elements of $\{i(n+1) \mid 0 \leq i \leq 2k+1\}$ are comparable; the largest among them is $(2k+1)(n+1) = 2kn+2k+n+1$. One can readily verify that the distinct elements of the set $\{i(2n-2) + j(2n-1) \mid 0 \leq i \leq k-1 \text{ and } 0 \leq j \leq 1\}$ are comparable: they are of the

form $(i-i')(2n-2)$ or $(i-i')(2n-2)+(2n-1)$ for some integers $0 \leq i < i' \leq k-1$. Observe that

$$(2k+1)(n+1)-[(k-1)(2n-2)+(2n-1)] = 4k+n = 2n-2$$

belongs to S, hence $(2k+1)(n+1)$ and $(k-1)(2n-2)+(2n-1)$ are comparable. Likewise, we have that $(2k+1)(n+1)-k(2n-2) = 2n-1$ belongs to S, hence $(2k+1)(n+1)$ and $k(2n-2)$ are comparable. We conclude therefore that $\text{Maximal}_{\leq_S} \text{Ap}(n,S) = \{2kn+n+2k+1\}$.

(3.) By Propositions 3.3.12 and Definition 3.4.3, the claims follow at once from (2.) above. □

Proposition 3.5.3. *Let k be a positive integer. Let $n = 4k+3$. Let $S = \langle n, n+1, 2n-2, 2n-1 \rangle$.*

(1.) *We have that*

$$\text{Ap}(n,S) = \{i(n+1) \mid 0 \leq i \leq 2k+1\} \cup \{i(2n-2)+j(2n-1) \mid 0 \leq i \leq k \text{ and } 0 \leq j \leq 1\}.$$

(2.) *We have that* $\text{Maximal}_{\leq_S} \text{Ap}(n,S) = \{(2k+1)(n+1), (2k+1)(n+1)+1\}$.

(3.) *We have that* $\text{PF}(S) = \{2k(n+1)+1, 2k(n+1)+2\}$. *Particularly, S is divisive.*

Proof. (1.) By Proposition 3.3.11, it suffices to compute the least element $w(i)$ of S that is congruent to i modulo n for each integer $0 \leq i \leq n-1$. Each element of S is of the form

$$s = \alpha n + \beta(n+1) + \gamma(2n-2) + \delta(2n-1)$$

for some integers $\alpha, \beta, \gamma, \delta \geq 0$, hence the residue of an element of S modulo n is given by $\beta - 2\gamma - \delta$. Given an integer $0 \leq i \leq n-1$, we seek to minimize s subject to the constraint $\beta - 2\gamma - \delta \equiv i \pmod{n}$. Clearly, we can take $\alpha = 0$ because the residue of s modulo n does not depend on α. Observe that for each integer $0 \leq i \leq 2k+1$, there exists an integer $2k+2 \leq j \leq 4k+3$ such that $n = 4k+3 = i+j$. Consequently, for each integer $0 \leq i \leq 2k+1$, we seek to minimize s subject to the constraint $\beta - 2\gamma - \delta = i$. Considering that $\gamma \geq 0$ and $\delta \geq 0$, we have that $\beta \geq i$, so we minimize s precisely when $\beta = i$ and $\alpha = \gamma = \delta = 0$. We have therefore illustrated that $w(i) = i(n+1)$ for all

integers $0 \leq i \leq 2k+1$. On the other hand, if we have that $2k+2 \leq i \leq 4k+3$, then there exists an integer $0 \leq j \leq 2k+1$ such that $n = 4k+3 = i+j$, and our constraint becomes $2\gamma+\delta-\beta = j$. Like before, we find that $2\gamma+\delta \geq j$ by assumption that $\beta \geq 0$. Given that $j = 2\ell$ is even, we minimize s by taking $\gamma = \ell$ and $\alpha = \beta = \delta = 0$. On the other hand, if $j = 2\ell+1$ is odd, we minimize s by taking $\gamma = \ell$, $\delta = 1$, and $\alpha = \beta = 0$. We conclude therefore that for each integer $2k+2 \leq i \leq n-1$, we have that $w(i) = \ell(2n-2)+m(2n-1)$ for some integers $0 \leq \ell \leq k$ and $0 \leq m \leq 1$.

(2.) Observe that for each pair of integers $0 \leq i < j \leq 2k+1$, we have that $(j-i)(n+1)$ belongs to S, hence any two elements of $\{i(n+1) \mid 0 \leq i \leq 2k+1\}$ are comparable; the largest among them is $(2k+1)(n+1)$. On the other hand, we have that

$$\begin{aligned} k(2n-2)+(2n-1) &= 2kn-2k+2n-1 \\ &= 2kn-2k+2(4k+3)-1 \\ &= 2kn-2k+8k+6-1 \\ &= 2kn+6k+5 \\ &= 2kn+2k+n+1+1 \\ &= (2k+1)(n+1)+1, \end{aligned}$$

so the largest element of $\{i(2n-2)+j(2n-1) \mid 0 \leq i \leq k \text{ and } 0 \leq j \leq 1\}$ is $(2k+1)(n+1)+1$. Further, one can readily verify that the distinct elements of this set are comparable: they are of the form $(i-i')(2n-2)$ or $(i-i')(2n-2)+(2n-1)$ for some integers $0 \leq i < i' \leq k$. Consequently, we conclude that $\text{Maximal}_{\leq_S} \text{Ap}(n,S) = \{(2k+1)(n+1), (2k+1)(n+1)+1\}$.

(3.) By Propositions 3.3.12 and Definition 3.4.3, the claims follow at once from (2.) above. □

Curiously, the numerical semigroups $\langle n, n+1, 2n-2, 2n-1\rangle$ with $n = 4k+1$ for some positive integer k are neither Gorenstein nor divisive, as our next example demonstrates.

Example 3.5.4. Observe that the numerical semigroup $S = \langle 5,6,8,9\rangle$ has $\text{PF}(S) = \{3,4,7\}$, hence it is neither Gorenstein nor divisive. Further, we have that $B_S(\Omega) = \langle 3,4,5\rangle$ is not Gorenstein.

Definition 3.5.5. Let $n \geq 3$ be an integer. Given any integers $1 \leq b \leq n-t \leq n-1$, we define

$$P_n(b,t) = \langle n, n+1, \ldots, n+b-1, 2n-t, 2n-t+1, \ldots, 2n-1 \rangle$$

as the **pinched discrete interval numerical semigroup** with b bottom elements and t top elements.

We have already established some preliminary results for $P_n(2,2)$ by examining the behavior of n modulo 4 in Propositions 3.5.1, 3.5.2, and 3.5.3 and Example 3.5.4. Even more, the numerical semigroups $P_n(1,1)$ have embedding dimension two, hence they are Gorenstein by [GR09, Example 2.22]. Consequently, it suffices to consider the case that either $b \geq 2$ or $t \geq 2$.

We conclude this chapter with a few conjectures toward a general classification of $P_n(b,t)$.

Conjecture 3.5.6. Let n and t be integers such that $1 \leq t \leq n-2$.

(1.) If $n \not\equiv 1 \pmod{t+2}$ and $n \not\equiv 2 \pmod{t+2}$, then $P_n(2,t)$ is divisive.

(2.) If $n \equiv 2 \pmod{t+2}$, then $P_n(2,t)$ is Gorenstein.

(3.) If $n \equiv 1 \pmod{t+2}$, then $P_n(2,t)$ is neither Gorenstein nor divisive.

Conjecture 3.5.7. Let n and b be integers such that $1 \leq b \leq n-2$.

(1.) If $n \not\equiv b+3 \pmod{2b}$ and $n \not\equiv 2 \pmod{2b}$, then $P_n(b,2)$ is divisive.

(2.) If $n \equiv 2 \pmod{2b}$, then $P_n(b,2)$ is Gorenstein.

(3.) If $n \equiv b+3 \pmod{2b}$, then $P_n(b,2)$ is neither Gorenstein nor divisive.

Conjecture 3.5.8. Let n and c be integers such that $2 \leq c \leq n-c$.

(1.) If $n \not\equiv 2c+1 \pmod{3c-2}$ and $n \not\equiv 2 \pmod{3c-2}$, then $P_n(c,c)$ is divisive.

(2.) If $n \equiv 2 \pmod{3c-2}$, then $P_n(c,c)$ is Gorenstein.

(3.) If $n \equiv 2c+1 \pmod{3c-2}$, then $P_n(c,c)$ is neither Gorenstein nor divisive.

Acknowledgements

We extend our humble gratitude to the creators of the [DGM05, GAP System], the NumericalSgps package of which we used extensively for our computations with numerical semigroups. We also thank Mark Denker for his insight regarding some of the computations of Section 3.5.

Chapter 4

Some New Invariants of Noetherian Local Rings

Abstract

We introduce two new invariants of a Noetherian (standard graded) local ring $(R,\mathfrak{m})$ that measure the number of generators of certain kinds of reductions of $\mathfrak{m}$, and we study their properties. Explicitly, we consider the minimum among the number of generators of ideals I such that either $I^2 = \mathfrak{m}^2$ or $I \supseteq \mathfrak{m}^2$ holds. We investigate subsequently the case that R is the quotient of a polynomial ring $k[x_1,\ldots,x_n]$ by an ideal I generated by homogeneous quadratic forms, and we compute these invariants. We devote specific attention to the case that R is the quotient of a polynomial ring $k[x_1,\ldots,x_n]$ by the edge ideal of a finite simple graph G.

4.1 Introduction

Our work began as a simple curiosity: given ideals I and J in a commutative unital ring R such that $I^2 = J^2$, how "close" must I and J be? For simplicity, suppose that J is a prime ideal of R. Localizing at J reduces to the case that (R,J) is a local ring with $I^2 = J^2$. Unless otherwise specified, therefore, we will henceforth assume that $(R,\mathfrak{m})$ is a commutative unital Noetherian local ring with a unique maximal ideal $\mathfrak{m}$. If $R = \bigoplus_{i\geq 0} R_i$ is standard graded, we assume that R_0 is a field, $R = R_0[R_1]$, and $\mathfrak{m} = \bigoplus_{i\geq 1} R_i$ is the homogeneous maximal ideal of R.

Question 4.1.1. Let $(R,\mathfrak{m})$ be a Noetherian (standard graded) local ring. If $I \subsetneq \mathfrak{m}$ is a (homogeneous) ideal of R such that $I^2 = \mathfrak{m}^2$, what can be said of R? What can be said of $\mu(I)$?

Originally, we noticed that if $(R,\mathfrak{m})$ is a regular local ring with an ideal $I \subseteq \mathfrak{m}$, then $I^2 = \mathfrak{m}^2$ only if $I = \mathfrak{m}$, hence we were naturally led to study the invariant

$$\operatorname{cs}(R) = \min\{\mu(I) \mid I \subseteq \mathfrak{m} \text{ is a (homogeneous) ideal of } R \text{ such that } I^2 = \mathfrak{m}^2\}.$$

Generally, it holds that $\dim(R) \leq \operatorname{cs}(R) \leq \mu(\mathfrak{m})$ with $\operatorname{cs}(R) = \mu(\mathfrak{m})$ if and only if for any ideal I of R, the equality $I^2 = \mathfrak{m}^2$ implies that $I = \mathfrak{m}$ (cf. the first and fifth parts of Proposition 4.3.3, respectively). In particular, if R is a regular local ring, then for any ideal I of R, the equality $I^2 = \mathfrak{m}^2$ implies that $I = \mathfrak{m}$; however, there exist non-regular rings for which $\operatorname{cs}(R) = \mu(\mathfrak{m})$. For instance, if R is a hypersurface, then $\operatorname{cs}(R) = \mu(\mathfrak{m})$ (cf. Corollary 4.3.6). On its own, this observation already gives enough reason to study $\operatorname{cs}(R)$ for various kinds of rings.

Likewise, we consider the more restrictive scenario that $\mathfrak{m}^2 = \mathfrak{m}I$ implies that $I = \mathfrak{m}$, i.e., the unique maximal ideal $\mathfrak{m}$ does not admit a proper reduction of reduction number one (cf. [HS06, Definitions 1.2.1 and 8.2.3]). By Proposition 4.3.3(4.), one correct invariant to look at is

$$\operatorname{ms}(R) = \min\{\mu(I) \mid I \subseteq \mathfrak{m} \text{ is a (homogeneous) ideal of } R \text{ such that } \mathfrak{m}^2 \subseteq I\}.$$

Ultimately, it is not obvious and takes some work to establish that $\operatorname{ms}(R)$ relates to the question of $\mathfrak{m}^2 = \mathfrak{m}I$. We illustrate that this connection mainly hinges on the induction performed in the results preceding Proposition 4.2.7 with the end result of Corollary 4.2.8 verifying this motivating claim.

Largely, Section 4.2 is devoted to establishing the result of Corollary 4.2.8; along the way, however, we prove that one can attain the values $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ by ideals generated by elements not in $\mathfrak{m}^2$. We demonstrate subsequently that $\operatorname{ms}(R)$ can be obtained by an ideal generated by general linear elements (cf. Proposition 4.2.9 for the precise statement). We conclude this section by recording several observations about the behavior of $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ with respect to familiar ring operations. Particularly, we show that $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ decrease along surjective ring homomorphisms and that they remain unchanged when passing to the $\mathfrak{m}$-adic completion. Even more, if R is a standard graded algebra over a field k, then the polynomial ring $S = R[X_{t-1}, \ldots, X_n]$ over R in

$n-t$ indeterminates satisfies $\operatorname{ms}(S) = \operatorname{ms}(R) + n - t$ (cf. Proposition 4.2.15 for details).

In Section 4.3, we present some general bounds for $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$. Chiefly, Proposition 4.3.3 gives bounds on these invariants in terms of the (embedding) dimension of R and examines the invariants of $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ when they are equal to $\dim(R)$ and $\mu(\mathfrak{m})$. We discuss also the behavior of $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ when they are "close to" the two boundary values of $\dim(R)$ and $\mu(\mathfrak{m})$, respectively. We provide in Proposition 4.3.10 a useful bound for $\operatorname{ms}(R)$ when $\mu(\mathfrak{m}^2)$ is sufficiently small. We end this section with Proposition 4.3.14 that relates $\operatorname{cs}(R)$ and $\operatorname{ms}(R)$ of two local rings (with the same residue field) to that of their fiber product.

We turn out attention in Section 4.4 to studying the first basic properties of the invariants in the standard graded case. Particularly, we relate $\operatorname{ms}(R)$ to the Weak Lefschetz Property of a standard graded Artinian k-algebra. Even more, for a standard graded algebra $S = k[x_1, \ldots, x_n]/J$, we show in Proposition 4.4.12 that it is enough to study the invariants $\operatorname{cs}(R)$ and $\operatorname{ms}(R)$ in the case that J is generated by quadratic polynomials. We also determine bounds on the invariants for the nth Veronese subring of $k[x,y]$ in Propositions 4.4.15 and 4.4.18 by relating them to cardinality of subsets S of $\{0,1,\ldots,n\}$ such that $S+S = \{s+t \mid s,t \in S\} = \{0,1,\ldots,2n\}$.

Using the result of Proposition 4.4.12, we are motivated in Section 4.5 to devote specific attention to computing the invariants $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ in the case that R is the quotient of a polynomial ring in n indeterminates by a homogeneous ideal I generated by quadratic forms. We establish a connection between the minimum number of generators of I, the number of indeterminates of R, and $\operatorname{cs}(R)$ in Proposition 4.5.1 that provides a useful lower bound on $\operatorname{cs}(R)$; then, we use this technique to investigate $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ in several examples for which either n or $\dim(R/I)$ is small. Particularly, we provide in Remark 4.5.3 a general lower bound for $\operatorname{cs}(R)$.

Last, in Section 4.6, we consider the case that R is the quotient of a polynomial ring by a quadratic squarefree monomial ideal. By the Stanley-Reisner Correspondence, this case is equivalent to the case that R is the edge ring of a finite simple graph G. We relate $\operatorname{cs}(R)$ and $\operatorname{ms}(R)$ to various special properties of finite simple graphs, and we estimate these invariants for many familiar classes of finite simple graphs. We prove in Proposition 4.6.19 that if $\overline{G}$ is chordal, then $\operatorname{ms}(R)$

is equal to the independence number of G. If $\overline{G}$ is not chordal, then the same proposition provides a bound on $\operatorname{ms}(R)$ in terms of the number of vertices and the minimum length of a cycle in $\overline{G}$. Particularly, if the minimum length of a cycle of $\overline{G}$ is four, it turns out that $\operatorname{ms}(R)$ can be quite subtle. We address this case specifically for the path graph in Proposition 4.6.27 and the cycle graph in Proposition 4.6.29. Even though we are not able to give a specific value for $\operatorname{cs}(R)$ or $\operatorname{ms}(R)$ for the cycle graph, we provide [GS, Macaulay2] code in Remark 4.6.32 that we use to conjecture better bounds for these two invariants. By the result of Proposition 4.6.36, it seems that under certain circumstances $\operatorname{ms}(R)$ is related to the number of edges of an edge cover of G in which all of the edges share a common edge or overlap at a vertex. We relate $\operatorname{cs}(R)$ and $\operatorname{ms}(R)$ with the invariants of the graph join of two finite simple graphs in Proposition 4.6.42, and we use this to subsequently provide bounds on $\operatorname{cs}(R)$ for the complete (t-partite) graph and the wheel graph. We conclude this section with Proposition 4.6.50 on the wedge of complete graphs and corollaries thereof.

4.2 Preliminaries and Basic Properties of the Invariants

We will denote by $(R,\mathfrak{m},k)$ a commutative Noetherian (standard graded) local ring with unique (homogeneous) maximal ideal $\mathfrak{m}$ and residue field k. By Nakayama's Lemma, the positive integer $\mu(I) = \dim_k(I/\mathfrak{m}I)$ is the unique minimum number of generators of an ideal I of R. Further, we denote by $\mu_1(I) = \dim_k(I/(I\cap\mathfrak{m}^2))$ denote the number of the generators in a minimal generating set of I that do not lie in $\mathfrak{m}^2$. We say that an element $x \in I$ is **general** if the image of x in $I/\mathfrak{m}I$ lies in a nonempty Zariski open subset of $I/\mathfrak{m}I$. We may assume that the residue field k of R is infinite in order to guarantee the existence of general elements.

Recall that an ideal $J \subseteq I$ is a **reduction** of I if there exists an integer $r \gg 0$ such that $I^{r+1} = I^r J$. We refer to the least integer r such that $I^{r+1} = I^r J$ as the **reduction number** of I with respect to J. Even more, if J is minimal with respect to inclusion among all reductions of I, then J is said to be a **minimal reduction** of I; the absolute reduction number of I is the minimum among all reduction numbers of all minimal reductions of I. By [HS06, Theorem 8.3.5], minimal reductions exist for each ideal of a Noetherian local ring.

Definition 4.2.1. Consider a Noetherian (standard graded) local ring $(R,\mathfrak{m})$. We define

$$\operatorname{cs}(R) = \min\{\mu(I) \mid I \text{ is a (homogeneous) proper ideal of } R \text{ such that } I^2 = \mathfrak{m}^2\} \text{ and}$$
$$\operatorname{ms}(R) = \min\{\mu(I) \mid I \text{ is a (homogeneous) proper ideal of } R \text{ such that } I \supseteq \mathfrak{m}^2\}.$$

We say that an ideal I **witnesses** (or is a **witness of**) $\operatorname{cs}(R)$ or $\operatorname{ms}(R)$ provided that $I^2 = \mathfrak{m}^2$ and $\mu(I) = \operatorname{cs}(R)$ or $I \supseteq \mathfrak{m}^2$ and $\mu(I) = \operatorname{ms}(R)$, respectively. We may also say in this case that $\operatorname{cs}(R)$ or $\operatorname{ms}(R)$ is **witnessed by** I.

Our immediate task is to establish that the invariants $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ can be witnessed by ideals generated by linear forms. Explicitly, if $\operatorname{ms}(R) = n$ or $\operatorname{cs}(R) = n$, we claim that there exist elements $x_1,\ldots,x_n \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $(x_1,\ldots,x_n)R \supseteq \mathfrak{m}^2$ or $(x_1,\ldots,x_n)^2 = \mathfrak{m}^2$, respectively.

Proposition 4.2.2. *We have that $\mu_1(I) \leq \mu(I)$. Equality holds if and only if $I \cap \mathfrak{m}^2 = \mathfrak{m}I$. Consequently, if I witnesses $\operatorname{cs}(R)$, then $\mu(I) = \mu_1(I)$, i.e., $\operatorname{cs}(R)$ is witnessed by linear forms.*

Proof. Consider the short exact sequence $0 \to (I \cap \mathfrak{m}^2)/\mathfrak{m}I \to I/\mathfrak{m}I \to I/(I \cap \mathfrak{m}^2) \to 0$ induced by the inclusion $\mathfrak{m}I \subseteq I \cap \mathfrak{m}^2$. We have that $\mu_1(I) \leq \mu(I)$ by the additivity of length on short exact sequences. Equality holds if and only if $(I \cap \mathfrak{m}^2)/\mathfrak{m}I = 0$ if and only if $I \cap \mathfrak{m}^2 = \mathfrak{m}I$. Last, if I witnesses $\operatorname{cs}(R)$, then $I^2 = \mathfrak{m}^2$ so that $(I \cap \mathfrak{m}^2) = (I \cap I^2) = I^2 = \mathfrak{m}^2 = \mathfrak{m}I$, where the last equality follows from $\mathfrak{m}^2 = I^2 \subseteq \mathfrak{m}I \subseteq \mathfrak{m}^2$. □

Likewise, the claim holds for $\operatorname{ms}(R)$, but the proof requires an induction on $\operatorname{ms}(R)$.

Proposition 4.2.3. *There exists a (homogeneous) ideal I of R that witnesses $\operatorname{ms}(R)$ that satisfies $\mu(I) = \mu_1(I)$. Put another way, $\operatorname{ms}(R)$ is witnessed by (homogeneous) linear forms.*

We will establish Proposition 4.2.3 by first establishing the following lemma and corollary.

Lemma 4.2.4. *Let $(R,\mathfrak{m})$ be a (standard graded) local ring with $\mathfrak{m}^2 \neq 0$. If there exists a (homogeneous) element $x \in \mathfrak{m}$ such that $\mathfrak{m}^2 \subseteq xR$, then there exists a (homogeneous) element $y \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 \subseteq yR$.*

Proof. Consider a (homogeneous) element $x \in \mathfrak{m}$ that satisfies $\mathfrak{m}^2 \subseteq xR$. On the contrary, suppose that for every (homogeneous) element $y \in \mathfrak{m} \setminus \mathfrak{m}^2$, we have that $\mathfrak{m}^2 \not\subseteq yR$. By hypothesis that $\mathfrak{m}^2 \subseteq xR$, we must have that $x \in \mathfrak{m}^2$, from which it follows that $xR \subseteq \mathfrak{m}^2$ and $\mathfrak{m}^2 = xR$. We claim that for any (homogeneous) element $\ell \in \mathfrak{m} \setminus \mathfrak{m}^2$, we have that $x \in \ell\mathfrak{m}$ if and only if $\ell\mathfrak{m}$ contains a minimal generator of $\mathfrak{m}^2 = xR$ if and only if $\ell\mathfrak{m} \cap (\mathfrak{m}^2 \setminus \mathfrak{m}^3) \neq \emptyset$. We verify the first equivalence. If $x \in \ell\mathfrak{m}$, then as x is a minimal generator of $\mathfrak{m}^2$ by hypothesis that $\mathfrak{m}^2 \neq 0$, it is clear that $\ell\mathfrak{m}$ contains a minimal generator of $\mathfrak{m}^2$. Conversely, if $\ell\mathfrak{m}$ contains a minimal generator of $\mathfrak{m}^2$, then there exists an element $z \in \ell\mathfrak{m} \cap (\mathfrak{m}^2 \setminus \mathfrak{m}^3)$ such that $zR = \mathfrak{m}^2 = xR$, from which it follows that $x = zr \in \ell\mathfrak{m}$. By taking the contrapositive of each equivalence, it follows that $\ell\mathfrak{m}$ does not contain a minimal generator of $\mathfrak{m}^2$ if and only if $\ell\mathfrak{m} \cap (\mathfrak{m}^2 \setminus \mathfrak{m}^3) = \emptyset$ if and only if $\ell\mathfrak{m} \subseteq \mathfrak{m}^3$ if and only if $\ell \in (\mathfrak{m}^3 : \mathfrak{m})$. Ultimately, if $\ell \in \mathfrak{m}$ and $\ell \notin (\mathfrak{m}^3 : \mathfrak{m})$ so that $\ell \notin \mathfrak{m}^2$, then $\ell\mathfrak{m}$ must contain a minimal generator of $\mathfrak{m}^2 = xR$.

We claim that $\mathfrak{m} \setminus (\mathfrak{m}^3 : \mathfrak{m}) \neq \emptyset$. On the contrary, if $\mathfrak{m} \setminus (\mathfrak{m}^3 : \mathfrak{m}) = \emptyset$, then we would have that $\mathfrak{m} = (\mathfrak{m}^3 : \mathfrak{m})$ so that $\mathfrak{m}^2 = (\mathfrak{m}^3 : \mathfrak{m})\mathfrak{m} \subseteq \mathfrak{m}^3$ — a contradiction. We conclude that there exists an element $\ell \in \mathfrak{m} \setminus (\mathfrak{m}^3 : \mathfrak{m})$ so that $\ell \in \mathfrak{m} \setminus \mathfrak{m}^2$ and $\mathfrak{m}^2 = xR \subseteq \ell\mathfrak{m}$ — a contradiction. □

Corollary 4.2.5. *Let $(R, \mathfrak{m})$ be a (standard graded) local ring with $\mathfrak{m}^2 \neq 0$. If $x_1, \ldots, x_n \in \mathfrak{m}$ are (homogeneous) elements such that $\mathfrak{m}^2 \subseteq (x_1, \ldots, x_n)R$, then there are (homogeneous) elements $y_1, \ldots, y_n \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 \subseteq (y_1, \ldots, y_n)$.*

Proof. Consider the quotient ring $\bar{R} = R/(x_2, \ldots, x_n)R$. Observe that

$$\bar{\mathfrak{m}}^2 = \left(\frac{\mathfrak{m}}{(x_2, \ldots, x_n)R}\right)^2 = \frac{\mathfrak{m}^2 + (x_2, \ldots, x_n)R}{(x_2, \ldots, x_n)R} \subseteq \frac{(x_1, \ldots, x_n)R}{(x_2, \ldots, x_n)R} = \bar{x}_1\bar{R}.$$

By Lemma 4.2.4, there exists a (homogeneous) element $\bar{y}_1 \in \bar{\mathfrak{m}} \setminus \bar{\mathfrak{m}}^2$ such that $\bar{\mathfrak{m}}^2 \subseteq \bar{y}_1\bar{R}$ so that

$$\frac{\mathfrak{m}^2 + (x_2, \ldots, x_n)R}{(x_2, \ldots, x_n)R} = \bar{\mathfrak{m}}^2 \subseteq \bar{y}_1\bar{R} = \frac{(y_1, x_2, \ldots, x_n)R}{(x_2, \ldots, x_n)R},$$

from which it follows that $\mathfrak{m}^2 + (x_2, \ldots, x_n)R \subseteq (y_1, x_2, \ldots, x_n)R$ and $\mathfrak{m}^2 \subseteq (y_1, x_2, \ldots, x_n)R$. Cer-

tainly, we must have that $y_1 \in \mathfrak{m} \setminus \mathfrak{m}^2$: for if $y_1 \in \mathfrak{m}^2$, then $\bar{y}_1 \in \bar{\mathfrak{m}}^2$ — a contradiction. We have therefore found $y_1 \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 \subseteq (y_1, x_2, \ldots, x_n)$. By repeating this argument with $x_2, \ldots, x_n$, we obtain (homogeneous) elements $y_2, \ldots, y_n \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 \subseteq (y_1, \ldots, y_n)R$. □

Corollary 4.2.6. *Let $(R, \mathfrak{m})$ be a (standard graded) local ring with $\mathfrak{m}^2 \neq 0$. If there exists a (homogeneous) element $x \in \mathfrak{m}$ such that $\mathfrak{m}^2 \subseteq xR$, then there exists a (homogeneous) element $y \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 = y\mathfrak{m}$.*

Proof. By Lemma 4.2.4, there exists a (homogeneous) element $y \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 \subseteq yR$. Consequently, for every (homogeneous) element $z \in \mathfrak{m}^2$, there exists an element $r \in R$ such that $z = yr$. We claim that $r \in \mathfrak{m}$. If $(R, \mathfrak{m})$ is local, the claim holds: if $r \notin \mathfrak{m}$, then r is a unit so that $y = zr^{-1}$ belongs to $\mathfrak{m}^2$ — a contradiction. If $R = \bigoplus_{i \geq 0} R_i$ is graded, then there exist homogeneous elements $r_0, \ldots, r_n$ such that $r = r_0 + \cdots + r_n$ and $z = y(r_0 + \cdots + r_n)$. If z is homogeneous of degree i, then $y(r_0 + \cdots + r_n) = yr_0 + \cdots + yr_n$ lies in R_i, hence we have that $z = yr_j$ for some homogeneous element r_j. Either way, we conclude that r is in $\mathfrak{m}$ so that $\mathfrak{m}^2 = y\mathfrak{m}$. □

Proposition 4.2.7. *Let $(R, \mathfrak{m})$ be a Noetherian (standard graded) local ring with $\mathfrak{m}^2 \neq 0$ and $\operatorname{ms}(R) = n$. There exist (homogeneous) elements $y_1, \ldots, y_n \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 = (y_1, \ldots, y_n)\mathfrak{m}$.*

Proof. It suffices to show that there exist (homogeneous) elements $y_1, \ldots, y_n \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 \subseteq (y_1, \ldots, y_n)\mathfrak{m}$. We proceed by induction on $\operatorname{ms}(R)$. Corollary 4.2.6 establishes the case that $\operatorname{ms}(R) = 1$, so we may assume the claim holds for $1 \leq \operatorname{ms}(R) \leq n-1$. If $\operatorname{ms}(R) = n$, by Corollary 4.2.5, there exist (homogeneous) elements $x_1, \ldots, x_n \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 \subseteq (x_1, \ldots, x_n)R$ and

$$\bar{\mathfrak{m}}^2 = \left(\frac{\mathfrak{m}}{x_n R}\right)^2 = \frac{\mathfrak{m}^2 + x_n R}{x_n R} \subseteq \frac{(x_1, \ldots, x_n)R + x_n R}{x_n R} = (\bar{x}_1, \ldots, \bar{x}_{n-1})\bar{R}.$$

Let $\operatorname{ms}(\bar{R}) = m$. By the above equation, we must have that $m + 1 \leq n$. By induction, there exist

(homogeneous) elements $\bar{y}_1, \ldots, \bar{y}_m \in \bar{\mathfrak{m}} \setminus \bar{\mathfrak{m}}^2$ such that $\bar{\mathfrak{m}}^2 = (\bar{y}_1, \ldots, \bar{y}_m)\bar{\mathfrak{m}}$ so that

$$\begin{aligned}
\frac{\mathfrak{m}^2 + x_n R}{x_n R} = \left(\frac{\mathfrak{m}}{x_n R}\right)^2 = \bar{\mathfrak{m}}^2 &= (\bar{y}_1, \ldots, \bar{y}_m)\bar{\mathfrak{m}} \\
&= \frac{(y_1, \ldots, y_m)R + x_n R}{x_n R} \cdot \frac{\mathfrak{m} + x_n R}{x_n R} \\
&\subseteq \frac{(y_1, \ldots, y_m)\mathfrak{m} + x_n \mathfrak{m} + x_n R}{x_n R} \\
&= \frac{(y_1, \ldots, y_m, x_n)\mathfrak{m} + x_n R}{x_n R},
\end{aligned}$$

hence we have that $\mathfrak{m}^2 \subseteq (y_1, \ldots, y_m, x_n)\mathfrak{m} + x_n R$. We claim that $\mathfrak{m}^2 \subseteq (y_1, \ldots, y_m, x_n)\mathfrak{m}$. Observe that every (homogeneous) element $r \in \mathfrak{m}^2$ has the form $r = a + x_n b$ for some (homogeneous) elements $a \in (y_1, \ldots, y_m, x_n)\mathfrak{m}$ and $b \in R$. Considering that $\bar{y}_i \in \bar{\mathfrak{m}} \setminus \bar{\mathfrak{m}}^2$, it follows that $y_i \in \mathfrak{m} \setminus \mathfrak{m}^2$. On the contrary, if $b \notin \mathfrak{m}$, then b would be a unit by the previous proof so that $x_n = rb^{-1} - ab^{-1}$ belongs to $\mathfrak{m}^2$ — a contradiction. We conclude that $\mathfrak{m}^2 \subseteq (y_1, \ldots, y_m, x_n)\mathfrak{m}$. Conversely, we have that $(y_1, \ldots, y_m, x_n)\mathfrak{m} \subseteq \mathfrak{m}^2$ by hypothesis that $y_1, \ldots, y_m, x_n \in \mathfrak{m} \setminus \mathfrak{m}^2$. Considering that $\operatorname{ms}(R) = n$, we must have that $n \leq m + 1$ so that $n = m + 1$. □

One immediate consequence of Proposition 4.2.7 is the following.

Corollary 4.2.8. *If $(R, \mathfrak{m})$ is a Noetherian (standard graded) local ring with $\mathfrak{m}^2 \neq 0$, then*

$$\operatorname{ms}(R) = \min\{\mu(I) : I \textit{ is a reduction of } \mathfrak{m} \textit{ with reduction number one}\}.$$

Proof. Proposition 4.2.7 illustrates that $\operatorname{ms}(R)$ is witnessed by a reduction of $\mathfrak{m}$ with reduction number one. Conversely, observe that if I is a reduction of $\mathfrak{m}$ with reduction number one, then we have that $\mathfrak{m}^2 = \mathfrak{m}I \subseteq I$, from which it follows that $\mu(I) \geq \operatorname{ms}(R)$, and the claim holds. □

In view of Proposition 4.2.7, the following result demonstrates that $\operatorname{ms}(R)$ is an open condition.

Proposition 4.2.9. *Let $(R,\mathfrak{m},k)$ be a Noetherian local ring with $\operatorname{ms}(R)=n$. The collection*

$$\left\{(x_1+\mathfrak{m}^2,\ldots,x_n+\mathfrak{m}^2)\in\left(\frac{\mathfrak{m}}{\mathfrak{m}^2}\right)^{\oplus n}:x_i\in\mathfrak{m}\setminus\mathfrak{m}^2 \text{ and } \mathfrak{m}^2=(x_1,\ldots,x_n)\mathfrak{m}\right\}$$

is a nonempty Zariski open set, where we identify $\mathfrak{m}/\mathfrak{m}^2$ with $\mathbb{A}^r_k$ via a fixed generating set.

Proof. By Proposition 4.2.7, this collection is nonempty. Observe that $\mathfrak{m}^2=(x_1,\ldots,x_n)\mathfrak{m}$ if and only if the R-linear map $\mathfrak{m}^{\oplus n}\to\mathfrak{m}^2$ sending $(m_1,\ldots,m_n)\mapsto x_1m_1+\cdots+x_nm_n$ is surjective if and only if the k-linear map $(\mathfrak{m}/\mathfrak{m}^2)^{\oplus n}\to\mathfrak{m}^2/\mathfrak{m}^3$ sending $(m_1+\mathfrak{m}^2,\ldots,m_n+\mathfrak{m}^2)\mapsto x_1m_1+\cdots+x_nm_n+\mathfrak{m}^3$ is surjective. Explicitly, the implication of the second equivalence holds by the right exactness of the functor $k\otimes_R-$ (cf. Proposition 2.1.93); the converse of the second equivalence holds by Nakayama's Lemma applied to the cokernel of $\mathfrak{m}^{\oplus n}\to\mathfrak{m}^2$.

Given that $\mu(\mathfrak{m})=r$, fix a generating set $\{y_1,\ldots,y_r\}$ of $\mathfrak{m}$. By setting e_i to be the image $\bar{y}_i$ of y_i in $\mathfrak{m}/\mathfrak{m}^2$, we have that $\{e_1,\ldots,e_r\}$ is an ordered basis of $\mathfrak{m}/\mathfrak{m}^2$. Observe that $\{y_iy_j\mid 1\le i,j\le r\}$ generates $\mathfrak{m}^2$ over R, hence $\{e_ie_j\mid 1\le i,j\le r\}$ generates $\mathfrak{m}^2/\mathfrak{m}^3$ over k. We may therefore obtain a k-vector space basis $\{e_{i_\ell}e_{j_\ell}\mid 1\le\ell\le s\}$, where we denote $\dim_k(\mathfrak{m}^2/\mathfrak{m}^3)=\mu(\mathfrak{m}^2)=s$. Observe that we may write $\bar{x}_i=\sum_j\alpha_{ij}e_j$ for some coefficients $\alpha_{ij}\in k\cong\mathbb{A}^1_k$. We claim that the entries of the matrix of the k-linear map $(\mathfrak{m}/\mathfrak{m}^2)^{\oplus n}\to\mathfrak{m}^2/\mathfrak{m}^3$ are polynomials in the coefficients α_{ij}. Considering that a k-linear map is uniquely determined by how it acts on a basis, it suffices to determine the images of the e_i under $(\mathfrak{m}/\mathfrak{m}^2)^{\oplus n}\to\mathfrak{m}^2/\mathfrak{m}^3$. Observe that the rn basis elements of $(\mathfrak{m}/\mathfrak{m}^2)^{\oplus n}$ are n-tuples f_{ij} whose ith coordinate is $e_j=\bar{y}_j$. Given that x_iy_j is in $\mathfrak{m}^3$, it follows that $x_iy_j+\mathfrak{m}^3=0+\mathfrak{m}^3$ so that f_{ij} is mapped to $0+\mathfrak{m}^3$. By hypothesis that the map is surjective, it follows that at least one basis element f_{ij} is not mapped to $0+\mathfrak{m}^3$, hence we have that

$$f_{ij}\mapsto x_iy_j+\mathfrak{m}^3=(x_i+\mathfrak{m}^2)(y_j+\mathfrak{m}^2)=\bar{x}_i\bar{y}_j=\left(\sum_t\alpha_{it}e_t\right)e_j=\sum_t\alpha_{it}e_te_j.$$

Crucially, any e_te_j that are not basis elements of $\mathfrak{m}^2/\mathfrak{m}^3$ can be written in terms of $e_{i_\ell}e_{j_\ell}$, hence the entries of the matrix corresponding to the k-linear map are polynomials in α_{ij}. Last, the surjectivity of a k-linear map is an open condition: it can be viewed as a non-vanishing condition on some

minors of the corresponding matrix. □

We show next that $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ behave well with respect to (graded) surjections.

Proposition 4.2.10. *Let $(R,\mathfrak{m})$ and $(S,\mathfrak{n})$ be Noetherian (standard graded) local rings. If there exists a surjective (graded) homomorphism $\varphi : R \to S$, then $\operatorname{ms}(R) \geq \operatorname{ms}(S)$ and $\operatorname{cs}(R) \geq \operatorname{cs}(S)$.*

Proof. By hypothesis that φ is a surjective (graded) ring homomorphism, we have that $\varphi(I)$ is a (homogeneous) ideal of S for each (homogeneous) ideal I of R. By hypothesis that $(R,\mathfrak{m})$ and $(S,\mathfrak{n})$ are (standard graded) local rings, every non-unit of S is the image under φ of a non-unit of R, i.e., $\varphi(\mathfrak{m}) = \mathfrak{n}$. If I witnesses $\operatorname{ms}(R)$, then $\mathfrak{n}^2 = \varphi(\mathfrak{m})^2 = \varphi(\mathfrak{m}^2) \subseteq \varphi(I)$. By the Third Isomorphism Theorem, the local rings R and S have the same residue field k, and the k-vector spaces $I/\mathfrak{m}I$ and $\varphi(I)/\varphi(\mathfrak{m}I)$ are isomorphic. We conclude that $\mu(\varphi(I)) = \mu(I) = \operatorname{ms}(R)$, from which it follows that $\operatorname{ms}(S) \leq \mu(I) = \operatorname{ms}(R)$. Likewise, if J witnesses $\operatorname{cs}(R)$, then $\mathfrak{n}^2 = \varphi(\mathfrak{m}^2) = \varphi(J^2) = \varphi(J)^2$ yields that $\operatorname{cs}(S) \leq \mu(J) = \operatorname{cs}(R)$ by a similar rationale as before. □

Our next observation yields nice results on cutting down and adjoining indeterminates.

Proposition 4.2.11. *Let $(R,\mathfrak{m})$ be a Noetherian (standard graded) local ring. Let I be a (homogeneous) proper ideal of R. We have that $\operatorname{ms}(R) \leq \operatorname{ms}(R/I) + \mu(I)$.*

Proof. Let $\operatorname{ms}(R/I) = n$. By Definition 4.2.1, there exist (homogeneous) elements $x_1,\ldots,x_n \in \mathfrak{m}$ such that $(\mathfrak{m}/I)^2 \subseteq (x_1,\ldots,x_n)(R/I)$. Consequently, it follows that

$$\frac{\mathfrak{m}^2+I}{I} = \left(\frac{\mathfrak{m}}{I}\right)^2 \subseteq (x_1,\ldots,x_n)\frac{R}{I} = \frac{(x_1,\ldots,x_n)+I}{I}.$$

We conclude that $\mathfrak{m}^2 \subseteq \mathfrak{m}^2 + I \subseteq (x_1,\ldots,x_n)+I$ so that $\operatorname{ms}(R) \leq n + \mu(I) = \operatorname{ms}(R/I) + \mu(I)$. □

Corollary 4.2.12. *Let $(R,\mathfrak{m})$ be a Noetherian (standard graded) local ring. For any (homogeneous) elements $x_1,\ldots,x_t \in \mathfrak{m}$, we have that*

$$\operatorname{ms}(R) \geq \operatorname{ms}(R/x_1R) \geq \cdots \geq \operatorname{ms}(R/(x_1,\ldots,x_t)) \geq \operatorname{ms}(R) - t.$$

Proof. We obtain the last inequality by Proposition 4.2.11 and the rest by Proposition 4.2.10. □

Corollary 4.2.13. *Let* $(R,\mathfrak{m})$ *be a Noetherian (standard graded) local ring. If* $x_1,\dots,x_{\mathrm{ms}(R)} \in \mathfrak{m}\setminus\mathfrak{m}^2$ *witness* $\mathrm{ms}(R)$, *then* $\mathrm{ms}(R/(x_1,\dots,x_t)) = \mathrm{ms}(R)-t$ *for any integer* $1 \le t \le \mathrm{ms}(R)$.

Proof. By Corollary 4.2.12, it suffices to show that $\mathrm{ms}(R/(x_1,\dots,x_t)) \le \mathrm{ms}(R)-t$. By hypothesis, for any integer $1 \le t \le \mathrm{ms}(R)$, we have that $\mathfrak{m}^2+(x_1,\dots,x_t) \subseteq (x_{t+1},\dots,x_{\mathrm{ms}(R)})+(x_1,\dots,x_t)$ and

$$\bar{\mathfrak{m}}^2 = \frac{\mathfrak{m}^2+(x_1,\dots,x_t)}{(x_1,\dots,x_t)} \subseteq \frac{(x_{t+1},\dots,x_{\mathrm{ms}(R)})+(x_1,\dots,x_t)}{(x_1,\dots,x_t)} = (\bar{x}_{t+1},\dots,\bar{x}_{\mathrm{ms}(R)})\frac{R}{(x_1,\dots,x_t)},$$

where $\bar{x}_i$ is the image of x_i in $R/(x_1,\dots,x_t)$. We conclude that $\mathrm{ms}(R/(x_1,\dots,x_t)) \le \mathrm{ms}(R)-t$. □

Corollary 4.2.14. *Let* $(R,\mathfrak{m})$ *be a Noetherian (standard graded) local ring. For any indeterminates* $X_1,\dots,X_t$, *we have that* $\mathrm{ms}(R) \le \mathrm{ms}(R[X_1]) \le \cdots \le \mathrm{ms}(R[X_1,\dots,X_t]) \le \mathrm{ms}(R)+t$.

Proof. We may identify R and $R[X_1,\dots,X_t]/(X_1,\dots,X_t)$ by the First Isomorphism Theorem. Consequently, the last inequality holds by Proposition 4.2.11 and the others by Proposition 4.2.10. □

Conversely, if $R = k[X_1,\dots,X_t]/I$ for some homogeneous ideal I of $k[X_1,\dots,X_t]$, then for any indeterminates $X_{t+1},\dots,X_n$, the upper bound of Corollary 4.2.14 is sharp.

Proposition 4.2.15. *Let* $R = k[X_1,\dots,X_t]/I$ *for some homogeneous ideal* I *of* $k[X_1,\dots,X_t]$. *Let* $X_{t+1},\dots,X_n$ *be indeterminates. We have that* $\mathrm{ms}(R[X_{t+1},\dots,X_n]) = \mathrm{ms}(R)+n-t$.

Proof. By Corollary 4.2.15, it suffices to show that $\mathrm{ms}(R[X_{t+1},\dots,X_n]) \ge \mathrm{ms}(R)+n-t$. We will prove that there exists a homogeneous ideal J that witnesses $\mathrm{ms}(R[X_{t+1},\dots,X_n])$ and a homogeneous ideal J' of R such that $J = J'+(X_{t+1},\dots,X_n)$ and $J' \supseteq (\bar{X}_1,\dots,\bar{X}_t)^2$; the claim follows.

Let $\mathrm{ms}(R[X_{t+1},\dots,X_n]) = r$. Let $\mathfrak{m} = (X_1,\dots,X_t,X_{t+1},\dots,X_n)$ be the homogeneous maximal ideal of $k[X_1,\dots,X_t,X_{t+1},\dots,X_n]$. Let $\bar{X}_i$ denote the image of X_i in $R[X_{t+1},\dots,X_n]$. By Corollary 4.2.7, there exist homogeneous linear polynomials $g_1,\dots,g_r \in k[X_1,\dots,X_t,X_{t+1},\dots,X_n]$ such that $J = (\bar{g}_1,\dots,\bar{g}_r)$ and $\bar{\mathfrak{m}}^2 = (\bar{g}_1,\dots,\bar{g}_r)\bar{\mathfrak{m}}$. Particularly, for each integer $t+1 \le i \le n$, there exist polynomials $p_1,\dots,p_r \in \mathfrak{m}$ such that $\bar{X}_i^2 = \bar{p}_1\bar{g}_1+\cdots+\bar{p}_r\bar{g}_r$. Consequently, there exists a polynomial $q \in I[X_{t+1},\dots,X_n]$ such that $X_i^2 = p_1g_1+\cdots+p_rg_r+q$. By hypothesis that I belongs to

$k[X_1,\ldots,X_t]$, the polynomial q does not admit any summands that are a scalar multiple of X_i^2. Cancelling these summands, we may write $X_i^2 = (\alpha_1 g_1 + \cdots + \alpha_r g_r)X_i$ for some scalars $\alpha_1,\ldots,\alpha_r$. We conclude that $X_i = \alpha_1 g_1 + \cdots + \alpha_r g_r$, hence X_i belongs to J for each integer $n+1 \leq i \leq t$. Consequently, for each integer $1 \leq i \leq r$, we may write $g_i = h_i + f_i(X_{t+1},\ldots,X_n)$ for some homogeneous polynomials $h_i \in k[X_1,\ldots,X_t]$ and $f_i(X_{t+1},\ldots,X_n) \in k[X_1,\ldots,X_t,X_{t+1},\ldots,X_n]$. By setting $J' = (\bar{h}_1,\ldots,\bar{h}_r)$, we find that $J = J' + (X_{t+1},\ldots,X_n)$ and J' is a homogeneous ideal of R.

Last, we claim that $J' \supseteq (\bar{X}_1,\ldots,\bar{X}_t)^2$. By assumption that J witnesses $\mathrm{ms}(R[X_{t+1},\ldots,X_n])$, for any integers $1 \leq i \leq j \leq t$, the monomial $\bar{X}_i\bar{X}_j$ must belong to J. If $\bar{X}_i\bar{X}_j$ does not vanish, then there exist polynomials $f_1,\ldots,f_{r-n+t} \in J'$, $p_1,\ldots,p_{r-n+t},p_{t+1},\ldots,p_n \in k[X_1,\ldots,X_t,X_{t+1},\ldots,X_n]$, and $q \in I[X_{t+1},\ldots X_n]$ such that $X_iX_j = p_1f_1 + \cdots + p_{r-n+t}f_{r-n+t} + p_{t+1}X_{t+1} + \cdots + p_nX_n + q$. Cancelling any summands from the right-hand side that are not scalar multiples of X_iX_j, we may write $X_iX_j = q_1f_1 + \cdots + q_{r-n+t}f_{r-n+t}$ for some polynomials $q_1,\ldots,q_{r-n+t} \in k[X_1,\ldots,X_t,X_{t+1},\ldots,X_n]$ of degree one. We conclude that X_iX_j belongs to J' for any integers $1 \leq i \leq j \leq t$, from which it follows that $J' \supseteq (\bar{X}_1,\ldots,\bar{X}_t)^2$, as desired. □

Going forward, it will sometimes be useful to treat the local and the standard graded local cases unilaterally. We achieve this as follows. Let $R = \bigoplus_{i\geq 0} R_i$ be a Noetherian standard graded local ring with homogeneous maximal ideal $\mathfrak{m}$. Observe that $R \setminus \mathfrak{m}$ is the multiplicatively closed subset of R consisting of nonzero elements of R whose degree zero homogeneous component is nonzero. Consequently, if R_0 is a field, then the degree zero homogeneous component of any element of $R \setminus \mathfrak{m}$ is a unit. For simplicity, we will often assume that it is. By definition, we have that $\mathfrak{m}^2 R_{\mathfrak{m}} = \{x/s \mid x \in \mathfrak{m}^2 \text{ and } s \in R \setminus \mathfrak{m}\}$, from which one can verify that $\mathfrak{m}^2 R_{\mathfrak{m}} = (\mathfrak{m}R_{\mathfrak{m}})^2$. We begin by establishing that if R_0 is a field, then the square of the homogeneous maximal ideal of R consists precisely of elements of R whose degree zero and degree one components vanish.

Lemma 4.2.16. *Let R be a Noetherian standard graded local ring with homogeneous maximal ideal $\mathfrak{m}$ such that R_0 is a field. We have that $\mathfrak{m}^2 = \bigoplus_{i\geq 2} R_i$.*

Proof. By definition, every element of $\mathfrak{m}^2$ is of the form $x_1y_1 + \cdots + x_ny_n$ for some integer $n \geq$

0 and some elements $x_1,\dots,x_n,y_1,\dots,y_n \in \mathfrak{m}$. By assumption that R_0 is a field, we have that $\mathfrak{m} = \bigoplus_{i\geq 1} R_i$. Consequently, every nonzero element of $\mathfrak{m}^2$ is a sum of homogeneous elements of degree at least two, hence we have that $\mathfrak{m}^2 \subseteq \bigoplus_{i\geq 2} R_i$. Conversely, suppose that x is a homogeneous element of R of degree at least two. By assumption that R is standard graded, we have that $R = R_0[R_1]$, hence there exist integers $n,m_1,\dots,m_n \geq 0$ and elements $\alpha_1,\dots,\alpha_n \in R_0$ and $r_{1,1},\dots,r_{m_1,1},\dots,r_{1,n},\dots,r_{m_n,n} \in R_1$ such that $x = \sum_{i=1}^{n} \alpha_i r_{1,i}\cdots r_{m_i,i}$. By assumption that x is homogeneous of degree at least two, all summands on the right-hand side that lie in degree one must cancel; the rest of the summands lie in $\mathfrak{m}^2$, hence x lies in $\mathfrak{m}^2$. We conclude that $\bigoplus_{i\geq 2} R_i \subseteq \mathfrak{m}^2$. $\square$

We will now demonstrate that $\operatorname{ms}(R) = \operatorname{ms}(R_\mathfrak{m})$ for a Noetherian standard graded local ring with homogeneous maximal ideal $\mathfrak{m}$ such that R_0 is a field. Our next lemma provides a crucial ingredient and illustrates that the generators of any ideal of $R_\mathfrak{m}$ that witnesses $\operatorname{ms}(R_\mathfrak{m})$ can be replaced by the images of homogeneous elements of R of degree one.

Lemma 4.2.17. *Let R be a Noetherian standard graded local ring with homogeneous maximal ideal $\mathfrak{m}$ such that R_0 is a field. If the ideal generated by $\frac{x_1}{1_R},\dots,\frac{x_n}{1_R}$ witnesses $\operatorname{ms}(R_\mathfrak{m})$, then there exist homogeneous elements $y_1,\dots,y_n \in \mathfrak{m}\setminus\mathfrak{m}^2$ such that $\left(\frac{x_1}{1_R},\dots,\frac{x_n}{1_R}\right)R_\mathfrak{m} = \left(\frac{y_1}{1_R},\dots,\frac{y_n}{1_R}\right)R_\mathfrak{m}$.*

Proof. We proceed by induction on $\operatorname{ms}(R_\mathfrak{m}) = n$. By Corollary 4.2.6, if $\mathfrak{m}^2 R_\mathfrak{m} \subseteq \frac{x}{1_R} R_\mathfrak{m}$ for some element $\frac{x}{1_R} \in \mathfrak{m}R_\mathfrak{m}$, then there exists an element $\frac{y}{1_R} \in \mathfrak{m}R_\mathfrak{m}\setminus\mathfrak{m}^2R_\mathfrak{m}$ such that $\mathfrak{m}^2R_\mathfrak{m} = \frac{y}{1_R}\mathfrak{m}R_\mathfrak{m}$. We note that $y \in \mathfrak{m}\setminus\mathfrak{m}^2$, hence if $y = y^0 + \cdots + y^d$ is the unique representation of y in terms of its homogeneous components, then $y^0 = 0_R$ and y^1 is nonzero by Lemma 4.2.16. If $y = y^1$ is homogeneous, then we are done; if y is not homogeneous, then we may define $m = \min\{i \geq 2 \mid y^i \neq 0\}$. We note that y^m belongs to $\mathfrak{m}^2$, hence there exist nonzero elements $r \in \mathfrak{m}$ and $s,t \in R\setminus\mathfrak{m}$ such that $sty^m = rty$. Comparing the homogeneous components of degree m on the left- and right-hand sides and using the fact that $r^0 = 0_R$ and $y^i = 0_R$ for all $2 \leq i \leq m-1$, we find that

$$s^0t^0y^m = r^0t^0y^m + r^{m-1}t^0y^1 + r^0t^{m-1}y^1 = r^{m-1}t^0y^1.$$

Considering that $s,t \in R\setminus\mathfrak{m}$, we must have that s^0 and t^0 are units. We conclude that $y^m =$

$r^{m-1}t^0uy^1$ lies in y^1R, where u is the multiplicative inverse of s^0t^0. By induction on $i \geq m$, we may write $s^0t^0y^i$ as a sum of $r^jt^ky^1$ such that $j+k=i-1$ and $r^0j^0y^i$. Observe that the former lies in y^1R, and the latter is zero. We conclude that all homogeneous components of y of degree at least two lie in y^1R so that $\frac{y}{1_R}R_{\mathfrak{m}} = \frac{y^1}{1_R}R_{\mathfrak{m}}$.

We will assume now that $\mathfrak{m}^2R_{\mathfrak{m}} \subseteq \left(\frac{x_1}{1_R},\ldots,\frac{x_n}{1_R}\right)R_{\mathfrak{m}}$ for some elements $\frac{x_1}{1_R},\ldots,\frac{x_n}{1_R} \in \mathfrak{m}R_{\mathfrak{m}}$. By Proposition 4.2.7, there exist elements $\frac{y_1}{1_R},\ldots,\frac{y_n}{1_R} \in \mathfrak{m}R_{\mathfrak{m}} \setminus \mathfrak{m}^2R_{\mathfrak{m}}$ with $\mathfrak{m}^2R_{\mathfrak{m}} = \left(\frac{y_1}{1_R},\ldots,\frac{y_n}{1_R}\right)\mathfrak{m}R_{\mathfrak{m}}$. We note that $y_1,\ldots,y_n \in \mathfrak{m}\setminus\mathfrak{m}^2$. If $y_n = y_n^1$ is homogeneous, then we may proceed to the next paragraph. If y_n is not homogeneous, then we may define $m = \min\{i \geq 2 \mid y_n^i \neq 0\}$. Considering that y_n^m belongs to $\mathfrak{m}^2$, it follows that

$$\frac{y_n^m}{1_R} = \sum_{i=1}^{n} \frac{r_iy_i}{s_i} = \frac{p_1r_1y_1+\cdots+p_nr_ny_n}{s_1\cdots s_n}$$

for some nonzero elements $r_1,\ldots,r_n \in \mathfrak{m}$, $s_1,\ldots,s_n \in R\setminus\mathfrak{m}$, and $p_i = \prod_{j\neq i}s_j$. Consequently, there exists an element $t \in R\setminus\mathfrak{m}$ such that $s_1\cdots s_nty_n^m = p_1r_1ty_1+\cdots+p_nr_nty_n$. Comparing the homogeneous components of degree m on the left- and right-hand sides and using the fact that $y_n^i = 0_R$ for all $2 \leq i \leq m-1$, we find that

$$s_1^0\cdots s_n^0t^0y_n^m = (p_1r_1ty_1+\cdots+p_{n-1}r_{n-1}ty_{n-1})^m + p_n^0r_n^{m-1}t^0y_n^1,$$

as any term involving r_n^0 vanishes because $r_n^0 = 0_R$. Observe that the element

$$a = p_1r_1ty_1+\cdots+p_{n-1}r_{n-1}ty_{n-1}$$

lies in $(y_1,\ldots,y_{n-1})R$, $b = p_n^0r_n^{m-1}t^0$ lies in R, and $y_n^m = ua^m+buy_n^1$, where u is the multiplicative inverse of $s_1^0\cdots s_n^0t^0$. Consequently, we find that $\frac{y_n^m}{1_R} = \frac{ua^m}{1_R}+\frac{buy_n^1}{1_R}$ lies in $\left(\frac{y_1}{1_R},\ldots,\frac{y_{n-1}}{1_R},\frac{y_n^1}{1_R}\right)R_{\mathfrak{m}}$. By induction on $i \geq m$, we find that the image of all homogeneous components of y_n of degree at least two lie in $\left(\frac{y_1}{1_R},\ldots,\frac{y_n^1}{1_R}\right)R_{\mathfrak{m}}$, from which it follows that $\left(\frac{y_1}{1_R},\ldots,\frac{y_n}{1_R}\right)R_{\mathfrak{m}} = \left(\frac{y_1}{1_R},\ldots,\frac{y_n^1}{1_R}\right)R_{\mathfrak{m}}$.

Observe that $R_{\mathfrak{m}}/(y_n^1/1_R)R_{\mathfrak{m}} \cong (R/y_n^1R)_{\mathfrak{m}}$ is the localization of a Noetherian standard graded

local ring whose degree zero graded piece is a field; moreover, it satisfies $\operatorname{ms}(R_{\mathfrak{m}}/(y_n^1/1_R)R_{\mathfrak{m}}) = n-1$ by Corollary 4.2.13 because $\dfrac{y_n^1}{1_R}$ belongs to a minimal system of generators of an ideal that witnesses $\operatorname{ms}(R_{\mathfrak{m}})$. By induction, there exist homogeneous elements $\bar{z}_1^1,\ldots,\bar{z}_{n-1}^1$ of degree one in R/y_n^1R such that $\bar{\mathfrak{m}}^2 \subseteq \left(\dfrac{\bar{z}_1^1}{1_R},\ldots,\dfrac{\bar{z}_{n-1}^1}{1_R}\right)(R_{\mathfrak{m}}/(y_n^1/1)R_{\mathfrak{m}})$. By the Correspondence Theorem, this yields $\mathfrak{m}^2R_{\mathfrak{m}} \subseteq \left(\dfrac{z_1^1}{1_R},\ldots,\dfrac{z_{n-1}^1}{1_R},\dfrac{y_n^1}{1_R}\right)R_{\mathfrak{m}}$, hence $\left(\dfrac{z_1^1}{1_R},\ldots,\dfrac{z_{n-1}^1}{1_R},\dfrac{y_n^1}{1_R}\right)R_{\mathfrak{m}}$ witnesses $\operatorname{ms}(R_{\mathfrak{m}})$. □

Proposition 4.2.18. *Let R be a Noetherian standard graded local ring with homogeneous maximal ideal $\mathfrak{m}$ such that R_0 is a field. We have that* $\operatorname{ms}(R) = \operatorname{ms}(R_{\mathfrak{m}})$.

Proof. If I witnesses $\operatorname{ms}(R)$, then $\mathfrak{m}^2 \subseteq I$ and $\operatorname{ms}(R) = \mu(I)$. Consequently, we have that $\mathfrak{m}^2R_{\mathfrak{m}} \subseteq IR_{\mathfrak{m}}$, from which it follows that $\operatorname{ms}(R_{\mathfrak{m}}) \leq \mu(IR_{\mathfrak{m}}) \leq \mu(I) = \operatorname{ms}(R)$. Conversely, if $\operatorname{ms}(R_{\mathfrak{m}}) = \ell$, then by Lemma 4.2.17, there exist homogeneous elements $x_1,\ldots,x_\ell \in \mathfrak{m}\setminus\mathfrak{m}^2$ such that $\mathfrak{m}^2R_{\mathfrak{m}} \subseteq (x_1,\ldots,x_\ell)R_{\mathfrak{m}}$. We claim that $\mathfrak{m}^2 \subseteq (x_1,\ldots,x_\ell)R$. It suffices to prove that the homogeneous elements of $\mathfrak{m}^2$ belong to $(x_1,\ldots,x_\ell)R$. If $a \in \mathfrak{m}^2$ is homogeneous, then as in the proof of Lemma 4.2.17, there exist elements $r_1,\ldots,r_\ell \in R$, $s_1,\ldots,s_\ell,t \in R\setminus\mathfrak{m}$, and $p_i = \prod_{j\neq i} s_j$ such that

$$s_1\cdots s_\ell t a = p_1r_1tx_1 + \cdots + p_\ell r_\ell t x_\ell.$$

Observe that $s_1^0\cdots s_\ell^0 t^0 a$ belongs to $(x_1,\ldots,x_\ell)R$ and $s_1^0\cdots s_\ell^0t^0$ is a unit by assumption that R_0 is a field, hence a belongs to $(x_1,\ldots,x_\ell)R$. We conclude that the homogeneous elements of $\mathfrak{m}^2$ belong to $(x_1,\ldots,x_\ell)R$ so that $\mathfrak{m}^2 \subseteq (x_1,\ldots,x_\ell)R$ and $\operatorname{ms}(R) \leq \ell = \operatorname{ms}(R_{\mathfrak{m}})$. □

We wrap up this section by establishing that the invariants $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ do not change with respect to $\mathfrak{m}$-adic completion $\widehat{R}$ of a Noetherian (standard graded) local ring $(R,\mathfrak{m})$. By Proposition 2.1.157, we have that $\widehat{M} \cong M \otimes_R \widehat{R}$ for any finitely generated R-module M. Even more, by Proposition 2.1.158, it follows that $\widehat{R}$ is faithfully flat over R, i.e., we have that $M = 0$ if and only if $\widehat{M} = 0$. Likewise, for any ideals $I_1 \subseteq I_2$, we have that $I_1 = I_2$ if and only if $\widehat{I_1} = \widehat{I_2}$.

Proposition 4.2.19. *Let $(R,\mathfrak{m})$ be a Noetherian (standard graded) local ring with $\mathfrak{m}$-adic completion $\widehat{R}$. We have that* $\operatorname{cs}(R) = \operatorname{cs}(\widehat{R})$ *and* $\operatorname{ms}(R) = \operatorname{ms}(\widehat{R})$.

Proof. For any (homogeneous) ideal I of R, we have that $\mu(I) = \mu(I\widehat{R})$ and $I^2\widehat{R} = (I\widehat{R})^2$ by Corollary 2.1.159. Consequently, if $I^2 = \mathfrak{m}^2$, then the exposition preceding the statement of proposition implies that $(I\widehat{R})^2 = I^2\widehat{R} = \mathfrak{m}^2\widehat{R} = (\mathfrak{m}\widehat{R})^2$. Likewise, if $\mathfrak{m}^2 \subseteq I$, then $(\mathfrak{m}\widehat{R})^2 = \mathfrak{m}^2\widehat{R} \subseteq I\widehat{R}$. We conclude that $\operatorname{cs}(\widehat{R}) \leq \operatorname{cs}(R)$ and $\operatorname{ms}(\widehat{R}) \leq \operatorname{ms}(R)$.

We will establish now that $\operatorname{cs}(R) \leq \operatorname{cs}(\widehat{R})$ and $\operatorname{ms}(R) \leq \operatorname{ms}(\widehat{R})$. Observe that the canonical injection $R \to \widehat{R}$ induces an isomorphism $R/\mathfrak{m}^2 \cong \widehat{R}/(\mathfrak{m}\widehat{R})^2$ by Corollary 2.1.153. By the Fourth Isomorphism Theorem, for any ideal J of $\widehat{R}$ with $J^2 = (\mathfrak{m}\widehat{R})^2 = \mathfrak{m}^2\widehat{R}$, there exists an ideal I of R such that $I \supseteq \mathfrak{m}^2$ and $J = I\widehat{R}$. Considering that $I^2\widehat{R} = (I\widehat{R})^2 = J^2 = \mathfrak{m}^2\widehat{R}$ and $I^2 \subseteq \mathfrak{m}^2$, we conclude that $I^2 = \mathfrak{m}^2$ so that $\operatorname{cs}(R) \leq \operatorname{cs}(\widehat{R})$. Likewise, for any ideal L of $\widehat{R}$ with $L^2 \supseteq (\mathfrak{m}\widehat{R})^2 = \mathfrak{m}^2\widehat{R}$, there exists an ideal K of R such that $K \supseteq \mathfrak{m}^2$ and $L = K\widehat{R}$ so that $\operatorname{ms}(R) \leq \operatorname{ms}(\widehat{R})$. □

4.3 General Bounds on $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$

Primarily, we devote this section to providing bounds for $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$. By the proof of Proposition 4.2.9, we obtain an immediate lower bound for $\operatorname{ms}(R)$.

Corollary 4.3.1. *Let $(R,\mathfrak{m})$ be a Noetherian local ring. We have that*

$$\operatorname{ms}(R) \geq \left\lceil \frac{\mu(\mathfrak{m}^2)}{\mu(\mathfrak{m})} \right\rceil.$$

Even more, if $\operatorname{ms}(R) = 1$, then we have that $\mu(\mathfrak{m}^{n+1}) \leq \mu(\mathfrak{m}^n)$ for all integers $n \geq 1$.

Proof. Let $\operatorname{ms}(R) = r$. By Proposition 4.2.7, there exist elements $y_1, \ldots, y_r \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that $\mathfrak{m}^2 = (y_1, \ldots, y_r)\mathfrak{m}$. Consequently, we have that $\mu(\mathfrak{m}^2) = \mu((y_1, \ldots, y_r)\mathfrak{m}) \leq r\mu(\mathfrak{m})$ or

$$\operatorname{ms}(R) = r \geq \left\lceil \frac{\mu(\mathfrak{m}^2)}{\mu(\mathfrak{m})} \right\rceil.$$

If $\operatorname{ms}(R) = 1$, we have that $\mathfrak{m}^2 = \ell\mathfrak{m}$ for some $\ell \in \mathfrak{m} \setminus \mathfrak{m}^2$ so that $\ell\mathfrak{m}^2 = (\ell\mathfrak{m})\mathfrak{m} = \mathfrak{m}^3$. Continuing in this manner shows that $\ell\mathfrak{m}^n = \mathfrak{m}^{n+1}$ and $\mu(\mathfrak{m}^{n+1}) = \mu(\ell\mathfrak{m}^n) \leq \mu(\mathfrak{m}^n)$ for all integers $n \geq 1$. □

Our next proposition establishes more general bounds for $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$. We illustrate moreover that if R is a Cohen-Macaulay local ring, then $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ are as small as possible if and only if R exhibits "nice" properties. Before this, we need the following lemma.

Lemma 4.3.2. *Let $(R,\mathfrak{m})$ be a Cohen-Macaulay local ring of positive dimension d. If there exist an integer $n \geq 0$ and an $\mathfrak{m}$-primary ideal $(x_1,\ldots,x_d)$ of R such that $(x_1,\ldots,x_d)^{n+1} = \mathfrak{m}(x_1,\ldots,x_d)^n$, then R is regular.*

Proof. If $n = 0$, the assertion is trivial by Definition 2.1.46, so we may assume that $n \geq 1$ and $I = (x_1,\ldots,x_d)$. By hypothesis, the elements $x_1,\ldots,x_d$ form a system of parameters that is an R-regular sequence by Proposition 2.2.25 and our assumption that R is Cohen-Macaulay. Consequently, the map $(R/I)[X_1,\ldots,X_d] \to \bigoplus_{k\geq 0} I^k/I^{k+1}$ that sends X_i to the image of x_i in I/I^2 is an isomorphism by the proof of Proposition 2.1.140. Particularly, I^n/I^{n+1} is isomorphic to the degree n graded piece of $(R/I)[X_1,\ldots,X_d]$, which is isomorphic to $(R/I)^{\oplus\binom{n+d-1}{n}}$. By assumption that $I^{n+1} = \mathfrak{m}I^n$, we have that $I^n/\mathfrak{m}I^n \cong (R/I)^{\oplus\binom{n+d-1}{n}}$ so that $\mu(I^n) = \binom{n+d-1}{n}\ell_R(R/I)$ by taking length on both sides. Considering that $\mu(I^n) \leq \binom{n+\mu(I)-1}{n} \leq \binom{n+d-1}{n}$, we find that $\binom{n+d-1}{n}\ell_R(R/I) \leq \binom{n+d-1}{n}$ and $\ell_R(R/I) \leq 1 = \ell_R(R/\mathfrak{m})$. On the other hand, the inclusion $I \subseteq \mathfrak{m}$ induces a surjection $R/I \to R/\mathfrak{m}$, hence the additivity of length on short exact sequences yields $\ell_R(R/I) \geq \ell_R(R/\mathfrak{m})$. We conclude that $\ell_R(R/I) = \ell_R(R/\mathfrak{m})$ so that $\ell_R(\mathfrak{m}/I) = 0$ and $I = \mathfrak{m}$, i.e., R is regular. □

Proposition 4.3.3. *Let $(R,\mathfrak{m})$ be a Noetherian (standard graded) local ring.*

(1.) *We have that $\dim(R) \leq \operatorname{ms}(R) \leq \operatorname{cs}(R) \leq \mu(\mathfrak{m})$. Particularly, if R is regular, these invariants are all equal.*

(2.) *If R is a Cohen-Macaulay local ring with infinite residue field, then $\operatorname{ms}(R) = \dim(R)$ if and only if R has minimal multiplicity.*

(3.) *If R is Cohen-Macaulay, local, and $\dim(R) > 0$, then $\operatorname{cs}(R) = \dim(R)$ if and only if R is regular.*

(4.) *We have that $\operatorname{ms}(R) = \mu(\mathfrak{m})$ if and only if $\mathfrak{m}I = \mathfrak{m}^2$ implies $I = \mathfrak{m}$ for any ideal I of R.*

(5.) *We have that $\operatorname{cs}(R) = \mu(\mathfrak{m})$ if and only if $I^2 = \mathfrak{m}^2$ implies $I = \mathfrak{m}$ for any ideal I of R.*

Proof. (1.) By definition of $\operatorname{cs}(R)$, we have that $\operatorname{cs}(R) \leq \mu(\mathfrak{m})$. If I witnesses $\operatorname{cs}(R)$, then $I^2 = \mathfrak{m}^2$ so that $\mathfrak{m}^2 \subseteq I$ and $\operatorname{ms}(R) \leq \operatorname{cs}(R)$. If I witnesses $\operatorname{ms}(R)$, then $\mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}$ so that $\sqrt{I} = \mathfrak{m}$ and $\operatorname{ht}(I) = \operatorname{ht}(\mathfrak{m})$. Further, we have that $\operatorname{ht}(I) \leq \mu(I) = \operatorname{ms}(R)$ by Krull's Height Theorem. Combining these two observations gives that $\dim(R) = \operatorname{ht}(\mathfrak{m}) = \operatorname{ht}(I) \leq \operatorname{ms}(R)$. If R is regular, then $\dim(R) = \mu(\mathfrak{m})$ and the invariants are all equal.

(2.) We will assume that the residue field k of R is infinite. By [BH93, Exercise 4.6.14], R has minimal multiplicity if and only if $\mathfrak{m}^2 = (x_1, \ldots, x_n)\mathfrak{m}$ for some R-regular sequence $(x_1, \ldots, x_n)$. If R has minimal multiplicity, therefore, there exists an R-regular sequence $(x_1, \ldots, x_n)$ such that $\mathfrak{m}^2 \subseteq (x_1, \ldots, x_n)$ and $n \leq \dim(R)$. By definition of $\operatorname{ms}(R)$ and (1.), we find that $n \leq \dim(R) \leq \operatorname{ms}(R) \leq n$, from which it follows that $\operatorname{ms}(R) = \dim(R)$. Conversely, we will assume that $\operatorname{ms}(R) = \dim(R)$. By Proposition 4.2.3, there exists an ideal I such that $\mathfrak{m}^2 \subseteq I$ and $\mu(I) = \mu_1(I) = \operatorname{ms}(R) = \dim(R)$. By Proposition 4.2.2, we have that $I \cap \mathfrak{m}^2 = \mathfrak{m}I$ so that $\mathfrak{m}^2 = \mathfrak{m}I$. Considering that $\mu(I) = \operatorname{ms}(R) = \dim(R)$ and $\mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}$, we have that I is a parameter ideal, hence I is generated by a regular sequence by Proposition 2.2.25. Consequently, R has minimal multiplicity.

(3.) If R is regular, the claim holds. Conversely, we will assume that $\operatorname{cs}(R) = \dim(R) = d > 0$. By definition of $\operatorname{cs}(R)$, there exists an ideal I such that $I^2 = \mathfrak{m}^2$ and $\mu(I) = \dim(R)$. Considering that $\mathfrak{m}^2 = I^2 \subseteq \mathfrak{m}I \subseteq \mathfrak{m}^2$, we find that $I^2 = \mathfrak{m}I$, hence I is $\mathfrak{m}$-primary. By Lemma 4.3.2 with $n = 1$, we conclude that R is regular.

(4.) We will assume first that $\mathfrak{m}I = \mathfrak{m}^2$ implies that $I = \mathfrak{m}$ for any (homogeneous) ideal I. If $\operatorname{ms}(R) = n$, there exists a (homogeneous) ideal J with $\mu(J) = n$ and $\mathfrak{m}^2 = \mathfrak{m}J$ by Proposition 4.2.7. By hypothesis, we conclude that $J = \mathfrak{m}$ so that $\operatorname{ms}(R) = \mu(J) = \mu(\mathfrak{m})$. Conversely, assume that $\operatorname{ms}(R) = \mu(\mathfrak{m})$. Given a (homogeneous) ideal I such that $\mathfrak{m}^2 = \mathfrak{m}I$, we have an inclusion of k-vector spaces $I/\mathfrak{m}I = I/\mathfrak{m}^2 \subseteq \mathfrak{m}/\mathfrak{m}^2$ such that $\dim_k(I/\mathfrak{m}I) = \operatorname{ms}(R) = \mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. Consequently, we must have that $I/\mathfrak{m}^2 = \mathfrak{m}/\mathfrak{m}^2$ so that $I = \mathfrak{m}$.

(5.) If $I^2 = \mathfrak{m}^2$ implies that $I = \mathfrak{m}$ for any (homogeneous) ideal I, then the set of (homogeneous) ideals of R whose square is $\mathfrak{m}^2$ is $S = \{\mathfrak{m}\}$. We conclude that $\operatorname{cs}(R) = \min\{\mu(I) \mid I \in S\} = \mu(\mathfrak{m})$.

We will assume therefore that $\operatorname{cs}(R) = \mu(\mathfrak{m})$. Given an ideal I such that $I^2 = \mathfrak{m}^2$, we have that

$$\dim_k(I/\mathfrak{m}^2) = \dim_k(I/\mathfrak{m}I) = \mu(I) \geq \operatorname{cs}(R) = \mu(\mathfrak{m}) = \dim_k(\mathfrak{m}/\mathfrak{m}^2).$$

Considering that $I/\mathfrak{m}^2$ is a k-subspace of $\mathfrak{m}/\mathfrak{m}^2$, we conclude that $I/\mathfrak{m}^2 = \mathfrak{m}/\mathfrak{m}^2$ and $I = \mathfrak{m}$. □

Remark 4.3.4. Based on Proposition 4.3.3(2.), if R is Cohen-Macaulay with infinite residue field and R does not have minimal multiplicity, then $\operatorname{ms}(R) > \dim(R)$. One such family of Cohen-Macaulay local rings is given by $\mathbb{C}[\![x,y,z]\!]/(x^n + y^n + z^n)$ for any integer $n \geq 3$. Generally, for a regular local ring $(S,\mathfrak{n})$ and any nonzero element $s \in \mathfrak{n}$, we have that $e(S/(s)) = \min\{m \mid s \in \mathfrak{m}^m \setminus \mathfrak{m}^{m+1}\}$ so that $\operatorname{ms}(S/(s)) = \dim(S/(s))$ if and only if $e(S/(s)) \leq 2$ if and only if $s \notin \mathfrak{n}^3$ by Corollary 4.3.6. Considering that R is a complete intersection with unique maximal ideal $\mathfrak{m} = (\bar{x},\bar{y},\bar{z})$ and $x^n + y^n + z^n \in (x,y,z)^3$ by assumption that $n \geq 3$, we have that $\operatorname{ms}(R) > \dim(R)$.

Even more, it is possible for $\dim(R) < \operatorname{ms}(R) < \operatorname{cs}(R) < \mu(\mathfrak{m})$ to hold simultaneously. Consider the Artinian complete intersection ring $R = k[x,y,z]/(x^2,y^2,z^2)$ with $\mathfrak{m} = (\bar{x},\bar{y},\bar{z})$ over a field k with $\operatorname{char}(k) \neq 2$. Observe that $I = (\bar{x}+\bar{y}+\bar{z})$ satisfies $\mathfrak{m}^2 \subseteq I$, from which it follows that $\operatorname{ms}(R) = 1$. We demonstrate in Proposition 4.5.4 that $\operatorname{cs}(R) = 2$. Evidently, we have that $\mu(\mathfrak{m}) = 3$.

Last, the Cohen-Macaulay assumption in the third part of Proposition 4.3.3 is necessary. Consider the ring $R = k[x,y]/(x^2,xy)$. Observe that $I = (\bar{y})$ witnesses both $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ since we have that $\bar{\mathfrak{m}}^2 = (\bar{x},\bar{y})^2 = (\bar{y}^2)$, from which it follows that $\dim(R) = \operatorname{ms}(R) = \operatorname{cs}(R) = 1 < 2 = \mu(\mathfrak{m})$ so that R is not regular; however, both $\bar{x}$ and $\bar{y}$ are zero divisors in R, hence we have that $\operatorname{depth}(R) = 0$, i.e., R is not Cohen-Macaulay.

Our next corollary improves upon Corollary 4.3.1 in the case that R is a one-dimensional Cohen-Macaulay local ring with infinite residue field such that $\operatorname{ms}(R) = 1$.

Corollary 4.3.5. *Let $(R,\mathfrak{m})$ be a one-dimensional Cohen-Macaulay local ring with infinite residue field. If $\operatorname{ms}(R) = 1$, we have that $\mu(\mathfrak{m}) = \mu(\mathfrak{m}^{n+1})$ for all integers $n \geq 1$.*

Proof. By Proposition 4.3.3, it follows that R has minimal multiplicity. Consequently, we have that $\mathfrak{m}^2 = x\mathfrak{m}$ for some R-regular element x and $\mathfrak{m}^{n+1} = x^n\mathfrak{m} \cong \mathfrak{m}$ for all integers $n \geq 1$. □

By Proposition 4.3.3, we can explicitly compute $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ if $(R,\mathfrak{m})$ is a **hypersurface**. By definition, this holds if and only if R is Cohen-Macaulay and $\dim(R) \geq \mu(\mathfrak{m}) - 1$.

Corollary 4.3.6. *If $(R,\mathfrak{m})$ is a hypersurface and $\mathfrak{m}^2 \neq 0$, then $\operatorname{cs}(R) = \mu(\mathfrak{m})$. Further, if $e(R) \leq 2$, then we have that $\operatorname{ms}(R) = \dim(R)$; otherwise, we have that $\operatorname{ms}(R) = \mu(\mathfrak{m})$.*

Proof. If R is regular, then we have that $\dim(R) = \operatorname{ms}(R) = \operatorname{cs}(R) = \mu(\mathfrak{m})$, and the claim holds. We may assume therefore that R is not regular. By hypothesis that R is a hypersurface, we have that R is Cohen-Macaulay and $\dim(R) = \mu(\mathfrak{m}) - 1$. If $\dim(R) = 0$, it follows that $\mu(\mathfrak{m}) = 1$ so that $\operatorname{cs}(R) \leq \mu(\mathfrak{m}) = 1$. On the other hand, we have that $\operatorname{cs}(R) \geq 1$ by assumption that $\mathfrak{m}^2 \neq 0$. We will assume therefore that $\dim(R) \geq 1$. By Proposition 4.3.3, we have that $\dim(R) \leq \operatorname{cs}(R) \leq \mu(\mathfrak{m})$ so that $\operatorname{cs}(R) = \mu(\mathfrak{m})$ or $\operatorname{cs}(R) = \mu(\mathfrak{m}) - 1$; however, the latter cannot happen, as it would imply that R is regular by the third part of Proposition 4.3.3 — a contradiction. We conclude that $\operatorname{cs}(R) = \mu(\mathfrak{m})$.

By hypothesis that R is a hypersurface, we have that $\operatorname{ms}(R) = \mu(\mathfrak{m}) - 1$ or $\operatorname{ms}(R) = \mu(\mathfrak{m})$. Considering that R is Cohen-Macaulay, it follows that $\operatorname{ms}(R) = \dim(R)$ if and only if R has minimal multiplicity, i.e., if and only if $e(R) = \mu(\mathfrak{m}) - \dim(R) + 1 \leq 2$. □

Corollary 4.3.7. *Let $(R,\mathfrak{m})$ be a Noetherian (standard graded) local ring. If R is a hypersurface and $\dim(R) > 0$, then $\operatorname{ms}(R) \in \{\mu(\mathfrak{m}) - 1, \mu(\mathfrak{m})\}$; the latter happens if and only if $\mathfrak{m}I = \mathfrak{m}^2$ implies that $I = \mathfrak{m}$ for any ideal I.*

Proof. If R is a hypersurface of positive dimension, then Corollary 4.3.6 implies that $\operatorname{cs}(R) = \mu(\mathfrak{m})$. By Proposition 4.3.3, we have that $\mu(\mathfrak{m}) - 1 \leq \dim(R) \leq \operatorname{ms}(R) \leq \mu(\mathfrak{m})$ so that $\operatorname{ms}(R) = \mu(\mathfrak{m}) - 1$ or $\operatorname{ms}(R) = \mu(\mathfrak{m})$; the latter happens if and only if $\mathfrak{m}I = \mathfrak{m}^2$ implies that $I = \mathfrak{m}$. □

One crucial point in Corollary 4.3.6 is the assumption that R is Cohen-Macaulay. If $\mu(\mathfrak{m}) = \dim(R) + 1$, both $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ take values in $\{\dim(R), \dim(R) + 1\}$; however, it might not be easy to conclude which value each invariant takes if R is not Cohen-Macaulay. Bearing this in mind, it is desirable to seek some additional properties of R along with $\mu(\mathfrak{m}) = \dim(R) + 1$ that guarantee R is Cohen-Macaulay; the following proposition addresses this concern. We note that this is known, but we provide the statement and proof for reference.

Proposition 4.3.8. *Let $(R,\mathfrak{m})$ be a Noetherian local ring with $\mu(\mathfrak{m}) = \dim(R)+1$. If the $\mathfrak{m}$-adic completion $\widehat{R}$ is an integral domain, then R is Cohen-Macaulay. Particularly, if the associated graded ring $\mathrm{gr}_{\mathfrak{m}}(R)$ is an integral domain, then R is Cohen-Macaulay.*

Proof. Observe that $\mu(\widehat{\mathfrak{m}})-1 = \mu(\mathfrak{m})-1 = \dim(R) = \dim(\widehat{R})$ by Corollaries 2.1.159 and 2.1.155. By the Cohen Structure Theorem, we can write $\widehat{R} \cong S/J$ for some ideal J in a regular local ring S such that $\dim(S) = \mu(\mathfrak{m})$. By hypothesis that $\widehat{R}$ is an integral domain, we must have that J is a prime ideal of S with $\mathrm{ht}(J) = \dim(S) - \dim(S/J) = \mu(\mathfrak{m}) - \dim(R) = 1$ by Propositions 2.2.27 and 2.2.20. Considering that S is a UFD by Proposition 2.1.144, we have that J is principal, hence $\widehat{R}$ is Cohen-Macaulay so that R is Cohen-Macaulay by Proposition 2.2.60. Particularly, if $\mathrm{gr}_{\mathfrak{m}}(R)$ is a domain, then $\mathrm{gr}_{\mathfrak{m}}(\widehat{R})$ and $\widehat{R}$ are domains by Propositions 2.1.154 and 2.1.141. □

Remark 4.3.9. It cannot be concluded (even in the equicharacteristic case) that R is Cohen-Macaulay if we only assume that $(R,\mathfrak{m})$ is a domain with $\mu(\mathfrak{m}) = \dim(R)+1$. Counterexamples exist even in dimension two. We will construct an example of such by employing [Lec86, Theorem 1], a discussion of which can be found in [Jon15].

Given a field k, consider the complete Noetherian local ring $S = k[\![x,y,z]\!]/(xy,xz)$ with unique maximal ideal $\mathfrak{n} = (\bar{x},\bar{y},\bar{z})$. Observe that S is reduced but not equidimensional, hence we have that $\mathrm{depth}(S) = 1$. Considering that S contains the field k, the prime ring of S is either $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$, and its action on S is torsion-free. By [Lec86, Theorem 1], it follows that S is the completion of a local domain $(R,\mathfrak{m})$. We have conclude that $\dim(R) = \dim(S) = 2$ and $\mu(\mathfrak{m}) = \mu(\mathfrak{n}) = 3 = \dim(R)+1$. Because $\widehat{R}$ is not Cohen-Macaulay, R is not Cohen-Macaulay. We must therefore assume that R is a hypersurface in Corollary 4.3.6, i.e., R must be Cohen-Macaulay.

If the square of the maximal ideal of a local ring $(R,\mathfrak{m})$ is minimally generated by "few enough" elements, then we obtain an upper bound for $\mathrm{ms}(R)$ as follows.

Proposition 4.3.10. *Let $(R,\mathfrak{m},k)$ be a Noetherian (standard graded) local ring with infinite residue field k with $\mathfrak{m}^2 \neq 0$. If $\mu(\mathfrak{m}^2) < \binom{r+2}{r}$, then $\mathrm{ms}(R) \leq r$. Particularly, if $\mu(\mathfrak{m}^2) \leq 2$, then $\mathrm{ms}(R) = 1$.*

Proof. We obtain this result in the local case as a corollary to the main theorem of [ES76] by taking $I = \mathfrak{m}$ and $n = 2$ (cf. [HS06, Theorem 8.6.8]). If $\mu(\mathfrak{m}^2) < \binom{r+2}{r}$, then by the aforementioned theorem, there exist linear forms $x_1, \ldots, x_r$ such that $\mathfrak{m}^2 = (x_1, \ldots, x_r)\mathfrak{m} \subseteq (x_1, \ldots, x_r)$ so that $\operatorname{ms}(R) \leq r$. If $\mu(\mathfrak{m}^2) \leq 2 < 3 = \binom{1+2}{1}$, we may set $r = 1$ to obtain $\operatorname{ms}(R) \leq 1$. We conclude that $\operatorname{ms}(R) = 1$ by assumption that $\mathfrak{m}^2 \neq 0$.

If R is standard graded local and R_0 is a field, the result holds by Proposition 4.2.18. □

Corollary 4.3.11. *If $(R, \mathfrak{m}, k)$ is a Noetherian (standard graded) local ring with infinite residue field k such that $\mu(\mathfrak{m}^2) < \binom{\mu(\mathfrak{m})+1}{2}$, then $\operatorname{ms}(R) \leq \mu(\mathfrak{m}) - 1$. If $\dim(R) = \mu(\mathfrak{m}) - 1$, equality holds.*

Proof. Using $r = \mu(\mathfrak{m}) - 1$ and the fact that $\binom{\mu(\mathfrak{m})+1}{\mu(\mathfrak{m})-1} = \binom{\mu(\mathfrak{m})+1}{2}$, we obtain the first claim from Proposition 4.3.10; the second claims follows from first part of Proposition 4.3.3. □

We note that it is always true that $\mu(\mathfrak{m}^2) \leq \binom{\mu(\mathfrak{m})+1}{2}$. In fact, for most of the rings that we will consider in this chapter, strict inequality holds because some element of $\mathfrak{m}^2$ vanishes.

Observe that when $\dim(R)$ is small — especially when R is Artinian — it is less restrictive to assume that $\mu(\mathfrak{m}^2)$ is small than to assume that $\mu(\mathfrak{m})$ is small, as $\mu(\mathfrak{m}^2)$ can be small when $\mu(\mathfrak{m})$ is arbitrarily large. Our next two propositions deal with cases when $\mu(\mathfrak{m}^2)$ is small. We remark that Proposition 4.3.10 guaranteed that $\operatorname{ms}(R) = 1$ whenever $\mu(\mathfrak{m}^2) \leq 2$ without any further assumptions on R. Even though we will mainly focus on $\operatorname{cs}(R)$ in the following two propositions, we do make mention of $\operatorname{ms}(R)$ without resorting to Proposition 4.3.10.

Proposition 4.3.12. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring such that $\mathfrak{m}^2 \neq 0$.*

(1.) *If $\operatorname{cs}(R) = 1$, then $\mu(\mathfrak{m}^2) = 1$. If $\dim(R) = 1$, then $e(R) = 1$. If R is Cohen-Macaulay, then R is regular.*

(2.) *Conversely, if $\mu(\mathfrak{m}^2) = 1$, then $\operatorname{ms}(R) = 1$ and $\dim(R) \in \{0, 1\}$. If $\dim(R) = 1$ and R is Cohen-Macaulay, then R is regular and $\operatorname{cs}(R) = 1$. On the other hand, if $\dim(R) = 0$ and 2 is a unit in R, then $\operatorname{cs}(R) = 1$.*

Proof. (1.) Consider a (homogeneous) ideal I that witnesses $\operatorname{cs}(R)$. We have that $\mu(I) = 1$ and $\mu(I^2) = 1$. By definition of $\operatorname{cs}(R)$, we have that $I^2 = \mathfrak{m}^2$ so that $\mu(\mathfrak{m}^2) = \mu(I^2) = 1$, as desired.

Consequently, it follows that $\mu(\mathfrak{m}^{2n}) = 1$ for all integers $n \geq 1$. By Krull's Height Theorem, we have that $\dim(R) = \mathrm{ht}(\mathfrak{m}) = \mathrm{ht}(\mathfrak{m}^2) \leq \mu(\mathfrak{m}^2) = 1$. If $\dim(R) = 1$, we have that $e(R) = \mu(\mathfrak{m}^n)$ for all $n \gg 0$, from which it follows that $e(R) = 1$. Last, if R is Cohen-Macaulay, then R is regular by [Ver18, Theorem 3.2] (Abhyankar's Inequality) since it has multiplicity one.

(2.) Considering that $\mathrm{ms}(R) \leq \mu(\mathfrak{m}^2) = 1$, we find that $\mathrm{ms}(R) = 1$ by assumption that $\mathfrak{m}^2 \neq 0$. By Krull's Height Theorem, we have that $\dim(R) \leq \mu(\mathfrak{m}^2) = 1$, hence $\dim(R) = 0$ or $\dim(R) = 1$.

If $\dim(R) = 1$, then $e(R) = \mu(\mathfrak{m}^n)$ for all $n \gg 0$. Considering that $\mu(\mathfrak{m}^{2n}) = 1$ for all integers $n \geq 1$, we have that $e(R) = 1$. By assumption that R is Cohen-Macaulay, we have that R is regular. By the first part of Proposition 4.3.3, we have that $\mathrm{cs}(R) = \mu(\mathfrak{m}) = \dim(R) = 1$.

Last, suppose that $\dim(R) = 0$, i.e., R is Artinian by Proposition 6.1.2. By assumption that $\mu(\mathfrak{m}^2) = 1$, i.e., that $\mathfrak{m}^2$ is principal, we have that R is stretched in the sense of [Sal80] and [Sal79]. We will adopt the notation of the former so that $\ell_R(R) = e$, $\mu(\mathfrak{m}) = e - h$, and $\dim_k(0 : \mathfrak{m}) = r$. By definition of stretched, we have that $\mathfrak{m}^{h+1} = 0$. By assumption that $\mathfrak{m}^2 \neq 0$, we have that $h \geq 2$. Consider the following cases.

(a.) If $h > 2$, then following the discussion preceding [Sal80, Theorem 1], we have that $\mathfrak{m}^2 = z^2R$ for some element $z \in \mathfrak{m} \setminus \mathfrak{m}^2$. Consequently, we have that $\mathrm{cs}(R) = 1$.

(b.) On the other hand, if $h = 2$, then once again by the exposition preceding [Sal80, Theorem 1], for all indices $i, j \in \{1, \ldots, e - h - r + 1\}$, there exist elements $z_i, z_j \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that either $z_i z_j = 0$ or $\mathfrak{m}^2 = z_i z_j R$. If $z_i^2 = z_i z_i \neq 0$ for some index i, then we must have that $\mathfrak{m}^2 = z_i^2 R$. Otherwise, we have that $z_i^2 = 0$ for all indices i. By the aforementioned discussion in [Sal80], for each index i, there exists an index j such that $z_i z_j \neq 0$, from which it follows that $\mathfrak{m}^2 = z_i z_j R$ so that $(z_i + z_j)^2 = 2 z_i z_j R = z_i z_j R = \mathfrak{m}^2$.

Either way, we have that $\mathrm{cs}(R) = 1$. □

Proposition 4.3.13. *Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring such that $\mu(\mathfrak{m}^2) = 2$. We have that $\dim(R) = 0$ or $\dim(R) = 1$. Even more, the following properties hold.*

(1.) *If $\dim(R) = 0$ and $\mathrm{char}(k) = 0$, then $\mathrm{cs}(R) = 2$.*

(2.) *If* $\dim(R) = 1$, *then* $e(R) \leq 2$. *Further, if* R *is Cohen-Macaulay, then* R *has minimal multiplicity* $e(R) = \mu(\mathfrak{m}) = 2$, $\operatorname{ms}(R) = 1$, *and* $\operatorname{cs}(R) = 2$.

Proof. By Krull's Height Theorem, we have that $\dim(R) = \operatorname{ht}(\mathfrak{m}) = \operatorname{ht}(\mathfrak{m}^2) \leq \mu(\mathfrak{m}^2) = 2$. On the contrary, suppose that $\dim(R) = 2$. By the first corollary of [Sal75], we have that $\mu(\mathfrak{m}^{n+2}) \leq 2$ for all integers $n \geq 0$. Evidently, then, we have that $\mu(\mathfrak{m}^t) \leq 2$ for all $t \gg 0$. We have therefore that $e(R) = \lim_{n\to\infty} \mu(\mathfrak{m}^n)/n = 0$ — a contradiction. We conclude that $\dim(R) = 0$ or $\dim(R) = 1$.

(1.) If $\dim(R) = 0$, then R is Artinian and almost stretched in the sense of [EV08]. By [EV08, Proposition 2.3], we have that $\mathfrak{m}^2 = (x^2, xy)$ for some elements $x, y \in \mathfrak{m} \setminus \mathfrak{m}^2$. Consider the ideal $I = (x, y) \subseteq \mathfrak{m}$. Observe that $\mathfrak{m}^2 = (x^2, xy) \subseteq (x^2, xy, y^2) = I^2$ so that $I^2 = \mathfrak{m}^2$ and $\operatorname{cs}(R) \in \{1, 2\}$. If $\operatorname{cs}(R) = 1$, then by Proposition 4.3.12, we would have that $\mu(\mathfrak{m}^2) = 1$ — a contradiction — so $\operatorname{cs}(R) = 2$.

(2.) If $\dim(R) = 1$, then we have that $e(R) = \mu(\mathfrak{m}^n)$ for all $n \gg 0$. Considering that $\mu(\mathfrak{m}^n) \leq 2$ for all $n \gg 0$ by our exposition in the first paragraph, we have that $e(R) \leq 2$.

Further, if R is Cohen-Macaulay, then we must have that $e(R) = 2$. For if $e(R) = 1$, then it would follow that R is regular so that $\mu(\mathfrak{m}) = \dim(R) = 1$ and thus $\mu(\mathfrak{m}^2) = 1$ — a contradiction. Consequently, we have that $\mu(\mathfrak{m}) = \mu(\mathfrak{m}) - \dim(R) + 1 \leq e(R) = 2$. Considering that $\mu(\mathfrak{m}) \neq 1$, we conclude that $\mu(\mathfrak{m}) = 2 = e(R)$ so that R has minimal multiplicity. By the second part of Proposition 4.3.3, it follows that $\operatorname{ms}(R) = \dim(R) = 1$. By the first part of Proposition 4.3.3, we have that $1 = \dim(R) \leq \operatorname{cs}(R) \leq \mu(\mathfrak{m}) = 2$. If $\operatorname{cs}(R) = 1$, then once again, by Proposition 4.3.12, we would have that $\mu(\mathfrak{m}^2) = 1$ — a contradiction — so we conclude that $\operatorname{cs}(R) = 2$. □

We conclude this section with a proposition concerning the fiber product.

Proposition 4.3.14. *Consider Noetherian local rings* $(S, \mathfrak{m}_S, k)$ *and* $(T, \mathfrak{m}_T, k)$ *of residue field* k. *We have that* $\max\{\operatorname{cs}(S), \operatorname{cs}(T)\} \leq \operatorname{cs}(S \times_k T) \leq \operatorname{cs}(S) + \operatorname{cs}(T)$ *and* $\operatorname{ms}(S \times_k T) = \max\{\operatorname{ms}(S), \operatorname{ms}(T)\}$.

Proof. Consider the canonical surjections $\pi_S : S \to k$ and $\pi_T : T \to k$. We define the **fiber product** of S and T as the subset of $S \times T$ consisting of all pairs (a, b) of $S \times T$ whose images are equal

under the respective canonical surjections, i.e., we have that

$$S \times_k T \stackrel{\text{def}}{=} \{(a,b) \in S \times T \mid \pi_S(a) = \pi_T(b)\}.$$

Observe that $S \times_k T$ is a local subring of $S \times T$ with unique maximal ideal $\mathfrak{m}_S \oplus \mathfrak{m}_T$. We will denote $R = S \times_k T$ when convenient. By definition of R, the maps $p_S : S \times_k T \to S$ and $p_T : S \times_k T \to T$ defined by $p_S(a,b) = a$ and $p_T(a,b) = b$ give rise to the following commutative diagram.

$$\begin{array}{ccc} S \times_k T & \xrightarrow{p_S} & S \\ \downarrow{\scriptstyle p_T} & & \downarrow{\scriptstyle \pi_S} \\ T & \xrightarrow[\pi_T]{} & k \end{array}$$

Considering that π_S and π_T are surjections and $\pi_S \circ p_S$ and $\pi_T \circ p_T$ are surjective by definition of $S \times_k T$, we have that p_S and p_T are surjective. Consequently, it follows that $\operatorname{ms}(S \times_k T) \geq \operatorname{ms}(S)$ and $\operatorname{ms}(S \times_k T) \geq \operatorname{ms}(T)$ by Proposition 4.2.10 so that $\max\{\operatorname{ms}(S), \operatorname{ms}(T)\} \leq \operatorname{ms}(S \times_k T)$. Likewise, the same holds for $\operatorname{cs}(S \times_k T)$.

Given any ideals $I \subseteq \mathfrak{m}_S$ and $J \subseteq \mathfrak{m}_T$ of S and T, respectively, observe that $I \oplus J$ is an ideal of R, as we have that $\pi_S(I) = 0 = \pi_T(J)$. We claim that $\mu(I \oplus J) \leq \mu(I) + \mu(J)$. If $I = (s_1, \ldots, s_m)S$ and $J = (t_1, \ldots, t_n)T$, then for any element $(a,b) \in I \oplus J$, there exist elements $a_1, \ldots, a_m \in S$ and $b_1, \ldots, b_n \in T$ such that

$$(a,b) = \left(\sum_{i=1}^{m} a_i s_i, \sum_{j=1}^{n} b_j t_j \right) = \sum_{i=1}^{m} (a_i s_i, 0) + \sum_{j=1}^{n} (0, b_j t_j).$$

Certainly, we have that $(a_i s_i, 0) = (a_i, 1)(s_i, 0) = (a_i, 0)(s_i, 0)$ as elements of $S \times T$; however, this may not hold in $S \times_k T$ because there is no guarantee that $\pi_S(a_i) \in \{0, 1\}$. Luckily, there is no issue, as we may employ the following trick: for each integer $1 \leq i \leq m$, we have that $\pi_S(a_i)$ belongs to the residue field $k = T/\mathfrak{m}_T$, hence we may find an element $a_i' \in T$ such that $\pi_S(a_i) = \pi_T(a_i')$. Likewise, for each integer $1 \leq j \leq n$, we may find an element $b_j' \in S$ such that $\pi_S(b_j') = \pi_T(b_j)$,

$\pi_T(b_j)$ belongs to $k = S/\mathfrak{m}_S$. We can therefore write

$$(a,b) = \sum_{i=1}^{m}(a_i s_i, 0) + \sum_{j=1}^{n}(0, b_j t_j) = \sum_{i=1}^{m}(a_i, a_i')(s_i, 0) + \sum_{j=1}^{n}(b_j', b_j)(0, t_j),$$

hence (a,b) belongs to the ideal K of R generated by $\{(s_1,0),\ldots,(s_m,0),(0,t_1),\ldots,(0,t_n)\}$. We conclude that $I \oplus J \subseteq K$. Conversely, the generators of K belong to $I \oplus J$. We have therefore shown that $I \oplus J = K$ so that $\mu(I \oplus J) = \mu(K) \leq m+n = \mu(I) + \mu(J)$.

Now, if I witnesses $\operatorname{cs}(S)$ and J witnesses $\operatorname{cs}(T)$, then we have that $\mathfrak{m}_S^2 = I^2$ and $\mathfrak{m}_T^2 = J^2$ so that $(\mathfrak{m}_S \oplus \mathfrak{m}_T)^2 = \mathfrak{m}_S^2 \oplus \mathfrak{m}_T^2 = I^2 \oplus J^2 = (I \oplus J)^2$ and $\operatorname{cs}(S \times_k T) \leq \operatorname{cs}(S) + \operatorname{cs}(T)$.

On the other hand, assume I witnesses $\operatorname{ms}(S)$, J witnesses $\operatorname{ms}(T)$, and $n = \max\{\operatorname{ms}(S), \operatorname{ms}(T)\}$. Denote by $I = (s_1,\ldots,s_n)S$ and $J = (t_1,\ldots,t_n)T$. Considering that $I \subseteq \mathfrak{m}_S$ and $J \subseteq \mathfrak{m}_T$, we have that $s_i \in \mathfrak{m}_S$ and $t_j \in \mathfrak{m}_T$ so that $(s_i, t_j) \in R$ for all integers $1 \leq i, j \leq n$. We claim that $K = ((s_1,t_1),(s_2,t_2),\ldots,(s_n,t_n))R$ contains $\mathfrak{m}_R^2$, hence $\operatorname{ms}(R) \leq n = \max\{\operatorname{ms}(S), \operatorname{ms}(T)\}$. Observe that $\mathfrak{m}_R^2 = \mathfrak{m}_S^2 \oplus \mathfrak{m}_T^2$, so we may consider $(x,y) \in \mathfrak{m}_S^2 \oplus \mathfrak{m}_T^2$. Considering that $\mathfrak{m}_S^2 = \mathfrak{m}_S I$ and $\mathfrak{m}_T^2 = \mathfrak{m}_T J$ by Proposition 4.2.7, we have that $x \in \mathfrak{m}_S I$ and $y \in \mathfrak{m}_T J$. By definition, there exist some elements $x_1,\ldots,x_n \in \mathfrak{m}_S$ and $y_1,\ldots,y_n \in \mathfrak{m}_T$ such that $x = \sum_{i=1}^n s_i x_i$ and $y = \sum_{i=1}^n t_i y_i$. Consequently, the pairs $(x_i, 0)$ and $(0, y_i)$ lie in R and

$$(x,y) = \sum_{i=1}^{n}(x_i, 0)(s_i, t_i) + \sum_{i=1}^{n}(0, y_i)(s_i, t_i)$$

lies in K. We conclude therefore that $\mathfrak{m}_R^2 \subseteq K$, as desired. □

4.4 The Standard Graded Local Case and the Weak Lefschetz Property

We turn our attention to the case that $(R, \mathfrak{m})$ is a standard graded local ring with unique homogeneous maximal ideal $\mathfrak{m}$. Ultimately, we will consider the case that R is the quotient of a polynomial ring over a field by a homogeneous ideal, e.g., a quadratic monomial ideal.

Given an ideal I of a Noetherian local ring $(R, \mathfrak{m})$, recall that the **Rees algebra** of I in R is

defined by $R[It] = \oplus_{n=0}^{\infty} I^n t^n \subseteq R[t]$. We note that $R[It]$ is likewise Noetherian. We define the **special fiber ring** of I in R as $\mathfrak{F}_I(R) = R[It]/\mathfrak{m}R[It]$. Observe that $\mathfrak{F}_{\mathfrak{m}}(R) \cong \operatorname{gr}_{\mathfrak{m}}(R)$.

One naturally wonders how the invariants $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ behave with respect to the associated graded ring of R. Unfortunately, as our next proposition illustrates, it is difficult to say.

Proposition 4.4.1. *Let $(R,\mathfrak{m})$ be a Noetherian local ring. If the associated graded ring $\operatorname{gr}_{\mathfrak{m}}(R)$ is an integral domain and $\operatorname{ms}(R) = 1$, then we have that $\operatorname{ms}(\operatorname{gr}_{\mathfrak{m}}(R)) \leq \operatorname{ms}(R)$.*

Proof. We will henceforth denote $\operatorname{ms}(R) = n$ and the unique homogeneous maximal ideal

$$\widetilde{\mathfrak{m}} = \bigoplus_{i\geq 1} \frac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}}$$

of $\operatorname{gr}_{\mathfrak{m}}(R)$. By the multiplication defined on $\operatorname{gr}_{\mathfrak{m}}(R)$, we have that

$$\widetilde{\mathfrak{m}}^2 = \bigoplus_{i\geq 2} \frac{\mathfrak{m}^i}{\mathfrak{m}^{i+1}}.$$

We denote by r^* the initial form of r in $\operatorname{gr}_{\mathfrak{m}}(R)$, i.e., $r^* = \{r + \mathfrak{m}^n/\mathfrak{m}^{n+1} \mid r \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}\}$.

We will assume that $\operatorname{ms}(R) = 1$. By Proposition 4.2.3, there exists a linear form ℓ such that $\mathfrak{m}^2 \subseteq \ell R \subseteq \mathfrak{m}$. We claim that $\widetilde{\mathfrak{m}}^2 \subseteq \ell^* \operatorname{gr}_{\mathfrak{m}}(R)$. Certainly, it is enough to show the inclusion for all homogeneous elements of $\widetilde{\mathfrak{m}}^2$, hence we may consider some element $r^* \in \widetilde{\mathfrak{m}}^2$ with $r \in \mathfrak{m}^2$. By hypothesis that $\mathfrak{m}^2 \subseteq \ell R$, we have that $r = s\ell$ for some element $s \in R$. By taking initial forms on both sides, we have that $r^* = (s\ell)^* = s^*\ell^*$ is in $\ell^* \operatorname{gr}_{\mathfrak{m}}(R)$ by hypothesis that $\operatorname{gr}_{\mathfrak{m}}(R)$ is a domain. We conclude that $\widetilde{\mathfrak{m}}^2 \subseteq \ell^* \operatorname{gr}_{\mathfrak{m}}(R)$ so that $\operatorname{ms}(\operatorname{gr}_{\mathfrak{m}}(R)) \leq \operatorname{ms}(R)$. □

Observe that $\operatorname{ms}(R) \leq \mu(\mathfrak{m}^2)$ holds in general. On the other hand, if $\operatorname{gr}_{\mathfrak{m}}(R)$ has positive depth, then we have that $\operatorname{cs}(R) \leq \mu(\mathfrak{m}^2)$. Before we establish this, we record the following lemmas.

Lemma 4.4.2. *If $\operatorname{depth} \mathfrak{F}_I(R) \geq 1$, then $\mu(I^k) \leq \mu(I^{k+1})$ for each positive integer k. Further, if equality holds for some positive integer k, it must be the case that $\operatorname{ht}(I) \leq 1$.*

Proof. If $\operatorname{depth} \mathfrak{F}_I(R) \geq 1$, there is a linear form $x \in \mathfrak{F}_I(R)$ that is not a zero divisor on $\mathfrak{F}_I(R)$. Consequently, multiplication by x induces an injective map $I^k/\mathfrak{m}I^k \to I^{k+1}/\mathfrak{m}I^{k+1}$, hence we have

that $\mu(I^k) \leq \mu(I^{k+1})$. If $\mu(I^k) = \mu(I^{k+1})$, then $I^k/\mathfrak{m}I^k \to I^{k+1}/\mathfrak{m}I^{k+1}$ is surjective, from which it follows that $I^{k+1} = xI^k$ and $I^{k+1} \subseteq xR$. We conclude that $\operatorname{ht}(I) = \operatorname{ht}(I^{k+1}) \leq \operatorname{ht}(xR) = 1$. □

Lemma 4.4.3. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Given any element $x \in R$, denote by $\bar{x}$ the image of x in $\operatorname{gr}_{\mathfrak{m}}(R)$. If $\bar{x}$ is not a zero divisor on $\operatorname{gr}_{\mathfrak{m}}(R)$, then x is not a zero divisor on R.*

Proof. We will establish the contrapositive. Consider some nonzero element $y \in R$ such that $xy = 0$. By Krull's Intersection Theorem, it follows that $\bar{y}$ is nonzero in $\operatorname{gr}_{\mathfrak{m}}(R)$; however, we have that $\bar{x}\bar{y} = \overline{xy} = \bar{0}$ in $\operatorname{gr}_{\mathfrak{m}}(R)$, hence $\bar{x}$ is a zero divisor on $\operatorname{gr}_{\mathfrak{m}}(R)$. □

Proposition 4.4.4. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. We have that $\operatorname{ms}(R) \leq \min\{\mu(\mathfrak{m}), \mu(\mathfrak{m}^2)\}$. If we have that $\operatorname{depth}(\operatorname{gr}_{\mathfrak{m}}(R)) \geq 1$, then $\operatorname{cs}(R) \leq \mu(\mathfrak{m}^2)$. If equality holds here, then both R and $\operatorname{gr}_{\mathfrak{m}}(R)$ are one-dimensional Cohen-Macaulay local rings, and R has minimal multiplicity. Even more, if the stronger equality $\operatorname{ms}(R) = \mu(\mathfrak{m}^2)$ holds, then R is regular of dimension one.*

Proof. By definition, we have that $\operatorname{ms}(R) = \min\{\mu(I) \mid I \subseteq \mathfrak{m} \text{ is an ideal of } R \text{ and } \mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}\}$, from which it follows that $\operatorname{ms}(R) \leq \mu(\mathfrak{m})$ and $\operatorname{ms}(R) \leq \mu(\mathfrak{m}^2)$ or $\operatorname{ms}(R) \leq \min\{\mu(\mathfrak{m}), \mu(\mathfrak{m}^2)\}$.

We will assume throughout the rest of the proof that $\operatorname{depth}(\operatorname{gr}_{\mathfrak{m}}(R)) \geq 1$. By Lemma 4.4.2, it follows that $\mu(\mathfrak{m}) \leq \mu(\mathfrak{m}^2)$ so that $\operatorname{cs}(R) \leq \mu(\mathfrak{m}^2)$ by the first part of Proposition 4.3.3.

If $\operatorname{cs}(R) = \mu(\mathfrak{m}^2)$, then $\mu(\mathfrak{m}^2) = \operatorname{cs}(R) \leq \mu(\mathfrak{m})$ by the first part of Proposition 4.3.3, from which it follows that $\mu(\mathfrak{m}) = \mu(\mathfrak{m}^2)$ by the previous paragraph. By Lemma 4.4.2, we conclude that $\dim(R) = \operatorname{ht}(\mathfrak{m}) \leq 1$. Considering that $\dim(R) = \dim(\operatorname{gr}_{\mathfrak{m}}(R)) \geq \operatorname{depth}(\operatorname{gr}_{\mathfrak{m}}(R)) \geq 1$ by assumption, we conclude that $\dim(R) = 1$ so that $\dim(\operatorname{gr}_{\mathfrak{m}}(R)) = 1$ and $\operatorname{depth}(\operatorname{gr}_{\mathfrak{m}}(R)) = 1$, i.e., $\operatorname{gr}_{\mathfrak{m}}(R)$ is Cohen-Macaulay of dimension one; it remains to be seen that $\operatorname{depth}(R) = 1$.

By the proof of Lemma 4.4.2, we have that $\mathfrak{m}^2 = x\mathfrak{m}$ for some element $x \in R$ whose image in $\operatorname{gr}_{\mathfrak{m}}(R)$ is a linear form and hence is neither a unit in $\operatorname{gr}_{\mathfrak{m}}(R)$ nor a zero divisor on $\operatorname{gr}_{\mathfrak{m}}(R)$. By Lemma 4.4.3, we have that x is not a zero divisor on R, and since x is not a unit in R, we have that $\operatorname{depth}(R) \geq 1$. We conclude that $\operatorname{depth}(R) = 1$ so that R is Cohen-Macaulay of dimension one. Observe that this shows that R has minimal multiplicity since $\mathfrak{m}^2 = x\mathfrak{m}$ for some R-regular element x. By the second part of Proposition 4.3.3, we conclude that $\operatorname{ms}(R) = \dim(R)$.

Last, if $\operatorname{ms}(R) = \mu(\mathfrak{m}^2)$, then $\mu(\mathfrak{m}^2) = \operatorname{ms}(R) \leq \operatorname{cs}(R) \leq \mu(\mathfrak{m}^2)$ so that $\operatorname{cs}(R) = \mu(\mathfrak{m}^2)$. By the previous paragraphs, R is Cohen-Macaulay, $\dim(R) = 1$, and $\mu(\mathfrak{m}) = \mu(\mathfrak{m}^2)$ so that $\dim(R) = \operatorname{ms}(R) = \mu(\mathfrak{m}^2) = \mu(\mathfrak{m})$. □

We will assume for the rest of this section that $R = k[x_1, \ldots, x_n]/J$ is a standard graded Artinian k-algebra with unique maximal ideal $\mathfrak{m}$. We will express J explicitly when necessary. Out of desire for notational convenience, we will simply write an element of R as f as opposed to $\bar{f}$. Further, we will denote by $[R]_i$ the ith graded piece of R, i.e., the k-vector subspace generated by the monomials of $k[x_1, \ldots, x_n]/J$ of degree i.

Definition 4.4.5. We say that R enjoys the **Weak Lefschetz Property** (henceforth abbreviated WLP) if for any general linear form ℓ, the multiplication map

$$\cdot\ell : [R]_i \to [R]_{i+1}$$

has maximal rank, i.e., it is either injective or surjective.

If R has Hilbert function $(1, h_1, h_2, \ldots, h_e)$, then [MN13, Lemma 2.9] guarantees that R enjoys the WLP if and only if for any general linear form ℓ and all indices i, we have that

$$h_i(R/(\ell)) = \max\{h_i - h_{i-1}, 0\},$$

where $h_i = \dim_k [R]_i = \mu(\mathfrak{m}^i)$ and $h_i(R/(\ell))$ is the ith entry of the Hilbert function of $R/(\ell)$.

Consider a homogeneous ideal I of R that witnesses $\operatorname{ms}(R)$. By Proposition 4.2.3, I can be generated by linear forms, i.e., there exist $\ell_1, \ldots, \ell_{\operatorname{ms}(R)} \in I \setminus \mathfrak{m}^2$ such that $I = (\ell_1, \ldots, \ell_{\operatorname{ms}(R)})$. We will denote by $R_i = R/(\ell_1, \ldots, \ell_i)$ and by $h_j(i)$ the jth Hilbert coefficient of R_i. We say that R **enjoys the Weak Lefschetz Property at the ith step** if R_i enjoys the WLP, hence R enjoys the WLP at each step $1 \leq i \leq \operatorname{ms}(R)$ whenever R_i enjoys the WLP for each $1 \leq i \leq \operatorname{ms}(R)$.

Proposition 4.4.6. *If R enjoys the WLP at each step, then* $\operatorname{ms}(R) = \min\{i \mid h_2(i) = 0\}$.

Proof. If $h_2(i) = 0$, then $\mathfrak{m}^2 \subseteq (\ell_1, \ldots, \ell_i)$ so that $\operatorname{ms}(R) \leq \min\{i \mid h_2(i) = 0\}$. On the other hand, by Proposition 4.2.3, $\operatorname{ms}(R)$ is the least positive integer i with $\mathfrak{m}^2 \subseteq (\ell_1, \ldots, \ell_i)$, i.e., $h_2(i) = 0$. $\square$

Proposition 4.4.7. *If R enjoys the WLP and $\mu(\mathfrak{m}^2) \leq \mu(\mathfrak{m})$, then $\operatorname{ms}(R) \leq 1$. Conversely, if $\operatorname{ms}(R) \leq 1$, then R enjoys the WLP and $\mu(\mathfrak{m}^{i+1}) \leq \mu(\mathfrak{m}^i)$ for all integers $i \geq 1$.*

Proof. We will assume first that R enjoys the WLP and $\mu(\mathfrak{m}^2) \leq \mu(\mathfrak{m})$. Certainly, if $\mathfrak{m}^2 = 0$, then it follows that $\operatorname{ms}(R) = 0$, as the zero ideal witnesses $\operatorname{ms}(R)$. We may assume therefore that $\mathfrak{m}^2 \neq 0$. By hypothesis that R enjoys the WLP, for any general linear form ℓ, the Hilbert function of $R/(\ell)$ is given by $(1, \mu(\mathfrak{m}) - 1, \max\{\mu(\mathfrak{m}^2) - \mu(\mathfrak{m}), 0\}, \ldots)$. Considering that $\mu(\mathfrak{m}^2) \leq \mu(\mathfrak{m})$, we have that $\mu(\mathfrak{m}^2) - \mu(\mathfrak{m}) \leq 0$ so that the Hilbert function of $R/(\ell)$ is in fact $(1, \mu(\mathfrak{m}) - 1, 0, \ldots)$. We conclude by Proposition 4.4.6 that $\operatorname{ms}(R) = 1$.

Conversely, suppose that $\operatorname{ms}(R) \leq 1$. If $\operatorname{ms}(R) = 0$, then $\mathfrak{m}^i = 0$ for all integers $i \geq 2$, so assume that $\operatorname{ms}(R) = 1$. By Proposition 4.2.3, we have that $\mathfrak{m}^2 \subseteq \ell R \subseteq \mathfrak{m}$ for some general linear form ℓ. Given any minimal generator f of $\mathfrak{m}^2$, there exists an element $g \in \mathfrak{m}$ such that $f = g\ell$. Consequently, the multiplication map $\cdot\ell : [R]_1 \to [R]_2$ is surjective. By [MN13, Proposition 2.6(a)], it follows that the multiplication map $\cdot\ell : [R]_i \to [R]_{i+1}$ is surjective for all integers $i \geq 1$, hence R enjoys the WLP. Further, we have that $\mu(\mathfrak{m}^{i+1}) = \dim_k [R]_{i+1} \leq \dim_k [R]_i = \mu(\mathfrak{m}^i)$ for all $i \geq 1$. $\square$

Proposition 4.4.8. *Let R enjoy the WLP, and suppose that $\mu(\mathfrak{m}^2) > \mu(\mathfrak{m})$.*

(1.) *If $\mu(\mathfrak{m}) = 2$, we have that $\mu(\mathfrak{m}^2) = 3$ and $\operatorname{ms}(R) = 2$.*

(2.) *If $\mu(\mathfrak{m}) \geq 3$ and $\mu(\mathfrak{m}^2) - \mu(\mathfrak{m}) \in \{1, 2\}$, we have that $\operatorname{ms}(R) = 2$.*

Proof. (1.) By our hypotheses that R enjoys the WLP and $\mu(\mathfrak{m}) = 2$, given any general linear form ℓ, the Hilbert function of $R/(\ell)$ is given by $(1, 1, \mu(\mathfrak{m}^2) - 2, \ldots)$. Consequently, the image $\bar{\mathfrak{m}}$ of $\mathfrak{m}$ in $R/(\ell)$ is principal, i.e., we have that $\bar{\mathfrak{m}} = (\bar{f})$ for some element $\bar{f} \in R/(\ell)$. But this implies that $\bar{\mathfrak{m}}^2 = (\bar{f}^2)$ so that $\bar{\mathfrak{m}}^2$ is either principal or the zero ideal, i.e., $\mu(\mathfrak{m}^2) - 2 = 1$ or $\mu(\mathfrak{m}^2) - 2 = 0$. By hypothesis that $\mu(\mathfrak{m}^2) > \mu(\mathfrak{m}) = 2$, the latter cannot happen, hence we conclude that $\mu(\mathfrak{m}^2) = 3$, and the Hilbert function of $R/(\ell)$ is given by $(1, 1, 1, \ldots)$. Observe that $\min\{i \mid h_i(1) \leq i\} = 1$, hence [MZ07, Theorem 5] implies that $R/(\ell)$ enjoys the WLP. Given any linear form ℓ' in R such that $\bar{\ell}'$

is a general linear form in $R/(\ell)$, then, the Hilbert function of $R/(\ell,\ell')$ is given by $(1,0,0,\dots)$. We conclude by Proposition 4.4.6 that $\operatorname{ms}(R)=2$.

(2.) By our hypothesis that R enjoys the WLP and $\mu(\mathfrak{m}^2)-\mu(\mathfrak{m})\in\{1,2\}$, given any general linear form ℓ, the Hilbert function of $R/(\ell)$ is given by either $(1,\mu(\mathfrak{m})-1,1,\dots)$ or $(1,\mu(\mathfrak{m})-1,2,\dots)$. Consequently, we have that $h_2(1)\leq 2$. By hypothesis that $\mu(\mathfrak{m})\geq 3$, we have that $\mu(\mathfrak{m})-1\geq 2$, and we conclude that $\min\{i\mid h_i(1)\leq i\}=2$. By [MZ07, Theorem 5], $R/(\ell)$ enjoys the WLP if and only if $h_0(1)=1=((h_1(1))_{(1)})^{-1}_{-1}$ (cf. [MZ07, Definition-Remark 1]). By definition, the unique 1-binomial expansion of $h_1(1)$ is $\binom{h_1(1)}{1}$, hence we have

$$((h_1(1)_{(1)})^{-1}_{-1}=\left(\binom{h_1(1)}{1}\right)^{-1}_{-1}=\binom{h_1(1)-1}{0}=1=h_0(1),$$

and $R/(\ell)$ enjoys the WLP. Given any linear form ℓ' in R such that $\bar{\ell'}$ is a general linear form in $R/(\ell)$, the Hilbert function of $R/(\ell,\ell')$ is either $(1,\mu(\mathfrak{m})-2,0,\dots)$ or $(1,\mu(\mathfrak{m})-3,0,\dots)$ by assumption that $\mu(\mathfrak{m})\geq 3$. Either way, Proposition 4.4.6 gives that $\operatorname{ms}(R)=2$. □

We turn our attention to the Artinian complete intersection $R=k[x_1,\dots,x_n]/(x_1^2,\dots,x_n^2)$ over a field k of characteristic zero. By [MN13, Theorem 1.1], R enjoys the Weak Lefschetz Property.

Conjecture 4.4.9. If $R=k[x_1,\dots,x_n]/(x_1^2,\dots,x_n^2)$ and $\operatorname{char}(k)=0$, then $R_i=R/(\ell_1,\dots,\ell_i)$ enjoys the Weak Lefschetz Property for any linear forms $\ell_1,\dots,\ell_i$ in R.

Proposition 4.4.10. *If Conjecture 4.4.9 holds, then*

$$\operatorname{ms}(R)=\left\lceil\frac{1}{2}(2n+1-\sqrt{8n+1})\right\rceil.$$

Proof. By [MZ08, Lemma 2.9], we may focus our attention on the coefficients $h_2(i)$. If Conjecture 4.4.9 holds, then R_i enjoys the Weak Lefschetz Property for each integer $1\leq i\leq\operatorname{ms}(R)$. Consequently, we have that $h_0(i)=1$, $h_1(i)=n-i$, and $h_2(i)=h_2(i-1)-h_1(i-1)$ with $h_2(0)=h_2=\binom{n}{2}$

and $h_1(0) = h_1 = n$. One can check that $h_2(i) = \binom{n}{2} - in + \binom{i}{2} = \frac{1}{2}[i^2 - (2n+1)i + n(n-1)]$ and

$$\min\{i \mid h_2(i) = 0\} = \left\lceil \frac{1}{2}(2n+1-\sqrt{8n+1}) \right\rceil.$$

Our proof is complete by Proposition 4.4.6. □

Remark 4.4.11. We note that the integer in Proposition 4.4.10 is precisely the number of non-triangular numbers that do not exceed n, according to the [Inc19, OEIS].

Observe that $\mathrm{gr}_{\mathfrak{m}}(R)$ is a standard graded k-algebra by Proposition 2.1.138, hence we may write $\mathrm{gr}_{\mathfrak{m}}(R)$ as the quotient of the polynomial ring $S = k[x_1, \ldots, x_{\mu(\mathfrak{m})}]$ by a homogeneous ideal I. Let $\bar{x_i}$ denote the image of x_i modulo I. Our next proposition reduces our study to a polynomial ring modulo an ideal generated by quadratic forms.

Proposition 4.4.12. *Let S and I be defined as above. We have that* $\mathrm{cs}(S/I) = \mathrm{cs}(S/I_2)$ *and* $\mathrm{ms}(S/I) = \mathrm{ms}(S/I_2)$, *where I_2 is the ideal generated by the elements of I of degree two.*

Proof. Considering that $I_2 \subseteq I$, it follows that the canonical projection $S/I_2 \to S/I$ is a surjective graded ring homomorphism. Consequently, Proposition 4.2.10 guarantees that $\mathrm{cs}(S/I) \leq \mathrm{cs}(S/I_2)$ and $\mathrm{ms}(S/I) \leq \mathrm{ms}(S/I_2)$. Conversely, we will assume that $\bar{J}$ witnesses $\mathrm{ms}(S/I)$ with $\mu(\bar{J}) = \mathrm{ms}(S/I) = k$. By Proposition 4.2.3, there exist linear forms $\bar{\ell}_1, \ldots, \bar{\ell}_k$ in S/I such that $\bar{J} = (\bar{\ell}_1, \ldots, \bar{\ell}_k)$. Given that $\bar{\mathfrak{m}} = (\bar{x}_1, \ldots, \bar{x}_m)$, we have that

$$\frac{(x_1, \ldots, x_m)^2 + I}{I} = \frac{\mathfrak{m}^2 + I}{I} = \bar{\mathfrak{m}}^2 \subseteq \bar{J} = \frac{J + I}{I} = \frac{(\ell_1, \ldots, \ell_k) + I}{I}$$

so that $(x_1, \ldots, x_m)^2 + I \subseteq (\ell_1, \ldots, \ell_k) + I$. Given any generator $x_i x_j$ of $\mathfrak{m}^2$, write $x_i x_j = a_1\ell_1 + \cdots + a_k\ell_k + s$ for some elements a_e in S and s in I. Express s in terms of its homogeneous components $s = s_0 + s_1 + \cdots + s_d$, where each element s_f is homogeneous of degree f. Comparing degrees shows that $a_1\ell_1 + \cdots + a_k\ell_k + s = b_1\ell_1 + \cdots + b_k\ell_k + s'$ for some elements b_e in S and s' in I such that the $b_e\ell_e$ and s' are homogeneous of degree two. Consequently, $x_i x_j$ is an element of

$(\ell_1,\ldots,\ell_k)+I_2$ so that $(x_1,\ldots,x_m)^2 \subseteq (\ell_1,\ldots,\ell_k)+I_2$ and

$$\frac{\mathfrak{m}^2+I_2}{I_2} = \frac{(x_1,\ldots,x_m)^2+I_2}{I_2} \subseteq \frac{(\ell_1,\ldots,\ell_k)+I_2}{I_2} = \frac{J+I_2}{I_2}.$$

We conclude that $\operatorname{ms}(S/I) \geq \operatorname{ms}(S/I_2)$, from which it follows that $\operatorname{ms}(S/I) = \operatorname{ms}(S/I_2)$. Likewise, if $\bar{J}$ witnesses $\operatorname{cs}(S/I)$ with $\mu(\bar{J}) = \operatorname{cs}(S/I) = k$, by Proposition 4.2.2, there exist linear forms $\bar{\ell}_1,\ldots,\bar{\ell}_k$ such that $\bar{J} = (\bar{\ell}_1,\ldots,\bar{\ell}_k)$. Given that $\bar{\mathfrak{m}} = (\bar{x}_1,\ldots,\bar{x}_m)$, we have

$$\frac{(x_1,\ldots,x_m)^2+I}{I} = \frac{\mathfrak{m}^2+I}{I} = \bar{\mathfrak{m}}^2 = \bar{J}^2 = \frac{J^2+I}{I} = \frac{(\ell_1,\ldots,\ell_k)^2+I}{I}$$

so that $(x_1,\ldots,x_m)^2+I = (\ell_1,\ldots,\ell_k)^2+I$. Given any generator x_ix_j of $\mathfrak{m}^2$, write $x_ix_j = s + \sum_{e,f} a_{ef}\ell_e\ell_f$ for some elements a_{ef} in S and s in J. Once again, comparing the degrees on the left- and right-hand sides gives that $s+\sum_{e,f} a_{ef}\ell_e\ell_f = s' + \sum_{e,f} b_{ef}\ell_e\ell_f$ for some elements b_{ef} in S and s' in I such that $b_{ef}\ell_e\ell_f$ and s' are homogeneous of degree two. Like before, we conclude that $\operatorname{cs}(S/I) \geq \operatorname{cs}(S/I_2)$ so that $\operatorname{cs}(S/I) = \operatorname{cs}(S/I_2)$. □

One natural curiosity that arises when studying $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ for a standard graded k-algebra R is whether these invariants depend on the field k. Our next proposition provides a partial answer and describes the behavior of $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ with respect to field extensions.

Proposition 4.4.13. *Consider an injective field homomorphism $\iota : K \to L$. If I is a monomial ideal of $R = K[x_1,\ldots,x_n]$ and $S = L[x_1,\ldots,x_n]$, then* $\operatorname{cs}(S/I) \leq \operatorname{cs}(R/I)$ *and* $\operatorname{ms}(S/I) \leq \operatorname{ms}(R/I)$.

Proof. We may view any monomial ideal I of R as the monomial ideal of S generated by the same monomials as in R. Every element a of K may be identified with the element $\iota(a)$ of L, hence we may simply write a in place of the element $\iota(a)$ of L. We will denote by $\bar{\mathfrak{m}}$ the image of the homogeneous maximal ideal $\mathfrak{m} = (x_1,\ldots,x_n)$ of R (or S) in the quotient ring R/I (or S/I).

By Proposition 4.2.2, there exist elements $\bar{\ell}_1,\ldots,\bar{\ell}_n$ in $\bar{\mathfrak{m}} \setminus \bar{\mathfrak{m}}^2$ such that $\bar{\mathfrak{m}}^2 = J^2$ for the ideal $J = (\bar{\ell}_1,\ldots,\bar{\ell}_n)R$ and $\operatorname{cs}(R/I) = n$. Consequently, for every pair of integers $1 \leq i \leq j \leq n$, there exist polynomials $f_1,\ldots,f_n$ of R/I such that $\bar{x}_i\bar{x}_j = f_1\bar{\ell}_1 + \cdots + f_n\bar{\ell}_n$. Considering this as an identity

in S/I, we conclude that $J = (\bar{\ell}_1, \ldots, \ell_n)S$ satisfies $\bar{\mathfrak{m}}^2 = J^2$ so that $\operatorname{cs}(S/I) \leq \operatorname{cs}(R/I)$.

By Proposition 4.2.3, the invariant $\operatorname{ms}(R/I)$ is likewise be witnessed by linear forms, hence by a similar argument as above, we conclude that $\operatorname{ms}(S/I) \leq \operatorname{ms}(R/I)$. □

Remark 4.4.14. For any two algebraically closed fields K and L of the same characteristic, either K embeds into L or vice-versa; in this case, the key hypothesis of Proposition 4.4.13 is satisfied.

We conclude this section with a discussion of $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ for two-dimensional Veronese subrings. Let $R = k[x,y]$. Recall that for a positive integer n, the monomial subring

$$R^{(n)} = k[x^i y^{n-i} \mid 0 \leq i \leq n]$$

is called the nth **Veronese** subring of R. Observe that R is integral over $R^{(n)}$, hence we have that $\dim(R)^{(n)} = \dim(R) = 2$ by Proposition 2.1.69. Further, $R^{(n)}$ is a standard graded local ring with homogeneous maximal ideal $\mathfrak{m} = (x^i y^{n-i} \mid 0 \leq i \leq n)$.

Proposition 4.4.15. *Let k be a field, and let $n \geq 1$ be an integer. Let $R^{(n)}$ denote the nth Veronese subring of $R = k[x,y]$, and let $[n] \cup \{0\} = \{0, 1, \ldots, n\}$. We have that $\operatorname{ms}(R^{(n)}) = 2$ and*

$$\operatorname{cs}(R^{(n)}) \leq \min\{|S| : S \subseteq [n] \cup \{0\} \text{ and } S + S = [2n] \cup \{0\}\}.$$

Proof. Observe that $\mathfrak{m}^2 = (x^{i+j} y^{2n-i-j} \mid 1 \leq i \leq j \leq n) = (x^\ell y^{2n-\ell} \mid 0 \leq \ell \leq 2n)$. Clearly, we have that $([n] \cup \{0\}) + \{0,n\} = \{x + y \mid x \in [n] \cup \{0\} \text{ and } y \in \{0,n\}\} = [2n] \cup \{0\}$ so that

$$\mathfrak{m}^2 = (x^\ell y^{2n-\ell} \mid 0 \leq \ell \leq 2n) = (x^{i+j} y^{2n-i-j} \mid i \in [n] \text{ and } j \in \{0,n\}) = \mathfrak{m}(x^n, y^n) \subseteq (x^n, y^n).$$

We conclude that $\operatorname{ms}(R^{(n)}) \leq 2$. Considering that R is integral over $R^{(n)}$, we have that $\operatorname{ms}(R^{(n)}) \geq 2$ by the first part of Proposition 4.3.3, hence equality holds.

On the other hand, if $S \subseteq [n] \cup \{0\}$ satisfies $S + S = [2n] \cup \{0\}$, then $I = (x^i y^{n-i} \mid i \in S)$ satisfies

$$I^2 = (x^{i+j} y^{2n-i-j} \mid i, j \in S) = (x^\ell y^{2n-\ell} \mid \ell \in S + S) = (x^\ell y^{2n-\ell} \mid 0 \leq \ell \leq 2n) = \mathfrak{m}^2,$$

from which it follows that $\mathrm{cs}(R^{(n)}) \leq \mu(I) \leq |S|$. Consequently, we conclude that

$$\mathrm{cs}(R^{(n)}) \leq \min\{|S| : S \subseteq [n] \cup \{0\} \text{ and } S+S = [2n] \cup \{0\}\}. \qquad \square$$

Before we establish our main result on $\mathrm{cs}(R^{(n)})$, we establish two technical lemmas. We gratefully acknowledge Gerry Myerson for his original suggestion in the comments of [Dao19] to consider the set $S(n,d)$ of Lemma 4.4.17.

Lemma 4.4.16. *Given any integers $1 \leq d \leq n-1$, we have that*

$$\left\lfloor \frac{n-d}{d} \right\rfloor d = n - r - d,$$

where r is the least non-negative residue of n modulo d.

Proof. If $n-d < d$, then $\left\lfloor \frac{n-d}{d} \right\rfloor = 0$ and $r = n-d$, so the claim holds. If $n-d \geq d$, then by the Division Algorithm, there exist integers $q \geq 1$ and $0 \leq r \leq d-1$ such that $n = qd+r$. Consequently, we find that

$$\left\lfloor \frac{n-d}{d} \right\rfloor d = \left\lfloor \frac{(q-1)d+r}{d} \right\rfloor d = \left\lfloor q-1+\frac{r}{d} \right\rfloor d = (q-1)d = qd-d = n-r-d. \qquad \square$$

Lemma 4.4.17. *Given any integers $1 \leq d \leq n$, the set*

$$S(n,d) = \{0,1,\ldots,d,n-d,n-d+1,\ldots,n\} \cup \{kd \mid k \geq 1 \text{ is an integer and } d \leq kd \leq n-d\}$$

is contained in $[n] \cup \{0\}$ and satisfies $S(n,d)+S(n,d) = [2n] \cup \{0\}$.

Proof. Let r denote the least non-negative residue of n modulo d. By Lemma 4.4.16, we have that

$$\max\{kd \mid k \geq 1 \text{ is an integer and } d \leq k \leq n-d\} = n-r-d.$$

Considering that $kd+i$ belongs to $S(n,d)+S(n,d)$ each pair of integers $0 \leq i \leq d$ and $k \geq 0$ such

that $0 \leq kd \leq n-d$, the integers $0,1,\ldots,n-r$ belong to $S(n,d)+S(n,d)$. By hypothesis that $S(n,d)$ contains $n-d, n-d+1,\ldots,n$, we conclude that $0,1,\ldots,n$ belong to $S(n,d)+S(n,d)$. Further, $kd+(n-d+i)$ belongs to $S(n,d)+S(n,d)$ for each pair of integers $0 \leq i \leq d$ and $k \geq 1$ such that $d \leq kd \leq n-d$, hence $n+1, n+2,\ldots,2n-d-r$ belong to $S(n,d)+S(n,d)$. Clearly, the integers $2n-2d, 2n-2d+1,\ldots,2n$ belong to $S(n,d)+S(n,d)$, hence $S(n,d)+S(n,d)=[2n]\cup\{0\}$. □

Proposition 4.4.18. *Let n be a positive integer. We have that*

$$\min\{|S| : S \subseteq [n]\cup\{0\} \text{ and } S+S=[2n]\cup\{0\}\} \leq 2\sqrt{2n}+1.$$

Consequently, for the nth Veronese subring $R^{(n)}$ of $R=k[x,y]$, we have that $\operatorname{cs}(R^{(n)}) \leq 2\sqrt{2n}+1$.

Proof. By Lemma 4.4.17, we have that $S(n,d) \subseteq [n]\cup\{0\}$ and $S(n,d)+S(n,d)=[2n]\cup\{0\}$. We claim that $|S(n,d)| \leq 2\sqrt{2n}+1$. One can readily verify that $|S(n,d)| = 2d+\left\lfloor \frac{n}{d} \right\rfloor + 1$. Consequently, we have that $|S(n,d)| \leq 2d+\frac{n}{d}+1 = f_n(d)$ for all integers $d \geq 1$. Considering that $f_n(x)$ attains its minimum $2\sqrt{2n}+1$ at $x=\sqrt{\frac{n}{2}}$, we conclude that $|S(n,d)| \leq 2\sqrt{2n}+1$. □

Corollary 4.4.19. *For any integer $n \geq 2$, we have that*

$$\min\{|S| : S \subseteq [n]\cup\{0\} \text{ and } S+S=[2n]\cup\{0\}\} \geq 2\sqrt{n+\frac{9}{16}}-\frac{1}{2}.$$

Proof. Let $R^{(n)}$ denote the nth Veronese subring of $R=k[x,y]$ with unique homogeneous maximal ideal $\mathfrak{m}=(x^i y^{n-i} \mid 0 \leq i \leq n)$. Observe that $\mu(\mathfrak{m}^2)=2n+1$. By Remark 4.5.3, we find that

$$\operatorname{cs}(R) \geq \sqrt{2(2n+1)+\frac{1}{4}}-\frac{1}{2} = \sqrt{4n+2+\frac{1}{4}}-\frac{1}{2} = 2\sqrt{n+\frac{1}{2}+\frac{1}{16}}-\frac{1}{2} = 2\sqrt{n+\frac{9}{16}}-\frac{1}{2},$$

hence we conclude the desired result by Proposition 4.4.15. □

4.5 Computing $\mathrm{ms}(R)$ and $\mathrm{cs}(R)$ for Quotients by Quadratic Ideals

Let k be a field. We will assume throughout this section that R is a standard graded k-algebra, i.e., R is the quotient of the polynomial ring $S = k[x_1, \ldots, x_n]$ by a homogeneous ideal I. We denote by $\mathfrak{m} = (x_1, \ldots, x_n)$ the homogeneous maximal ideal of S and by $\bar{\mathfrak{m}}$ the image of $\mathfrak{m}$ in R. By Proposition 4.4.12, $\mathrm{ms}(R)$ and $\mathrm{cs}(R)$ depend only on the degree two part of I, hence we may assume that I is a homogeneous quadratic ideal.

Using this as our motivation, we seek to compute $\mathrm{ms}(R)$ and $\mathrm{cs}(R)$ in the case that I possesses certain quadratic generators. We begin by establishing the following lower bound for $\mathrm{cs}(R)$.

Proposition 4.5.1. *Let $R = k[x_1, \ldots, x_n]/I$, where I is minimally generated over $k[x_1, \ldots, x_n]$ by $t > 0$ homogeneous polynomials of degree two. We have that*

$$\binom{n+1}{2} - t \leq \binom{\mathrm{cs}(R)+1}{2}.$$

Particularly, if $t \leq \dfrac{(s+1)(2n-s)}{2}$ for some integer $0 \leq s \leq n-1$, then $\mathrm{cs}(R) \geq n-s-1$. Even more, if $t \leq n-1$, then $\mathrm{cs}(R) = n = \mu(\bar{\mathfrak{m}})$, where $\bar{\mathfrak{m}}$ is the image of $(x_1, \ldots, x_n)$ in R.

Proof. We note that it is straightforward to verify that $\mu(\bar{\mathfrak{m}}^2) = \mu(\mathfrak{m}^2) - \mu(I) = \binom{n+1}{2} - t$. Consider an ideal J of R that witnesses $\mathrm{cs}(R)$. We have that $\mu(J^2) \leq \binom{\mu(J)+1}{2}$ so that

$$\binom{n+1}{2} - t = \mu(\bar{\mathfrak{m}}^2) = \mu(J^2) \leq \binom{\mu(J)+1}{2} = \binom{\mathrm{cs}(R)+1}{2},$$

where the last equality holds because J witnesses $\mathrm{cs}(R)$. If $t \leq \dfrac{(s+1)(2n-s)}{2}$, then

$$\begin{aligned}\binom{n+1}{2} - t \geq \frac{n(n+1) - (s+1)(2n-s)}{2} &= \frac{n^2 + n - 2ns + s^2 - 2n + s}{2} \\ &= \frac{(n-s)^2 - (n-s)}{2} = \binom{n-s}{2}\end{aligned}$$

so that $\binom{\mathrm{cs}(R)+1}{2} \geq \binom{n-s}{2}$ and hence $\mathrm{cs}(R) \geq n-s-1$, as desired.

For the last claim, we will show that if $\operatorname{cs}(R) \neq n$, then $t \geq n$. By the first part of Proposition 4.3.3, we have that $\operatorname{cs}(R) \leq \mu(\bar{\mathfrak{m}}) = n$. Consequently, if $\operatorname{cs}(R) \neq n$, we must have that $\operatorname{cs}(R) \leq n-1$. But then, we have that $\binom{n+1}{2} - t \leq \binom{\operatorname{cs}(R)+1}{2} \leq \binom{n}{2}$ so that $t \geq \binom{n+1}{2} - \binom{n}{2} = n$. □

Remark 4.5.2. For any integer $n \geq 3$, Proposition 4.5.1 provides a class of (standard graded) local rings for which $\operatorname{cs}(R) = \mu(\mathfrak{m})$ other than regular local rings and hypersurface rings.

Remark 4.5.3. Using a similar idea as in the proof of Proposition 4.5.1, one can show that

$$\operatorname{cs}(R) \geq \left\lceil \frac{\sqrt{8\mu(\mathfrak{m}^2)+1}-1}{2} \right\rceil$$

holds for any Noetherian local ring $(R, \mathfrak{m})$. By the third sentence of the proof of Proposition 4.5.1, we have that $\mu(\mathfrak{m}^2) \leq \binom{\operatorname{cs}(R)+1}{2}$ so that $2\mu(\mathfrak{m})^2 \leq \operatorname{cs}(R)[\operatorname{cs}(R)+1]$. Completing the square yields

$$\left(\operatorname{cs}(R) + \frac{1}{2}\right)^2 \geq 2\mu(\mathfrak{m}^2) + \frac{1}{4} = \frac{8\mu(\mathfrak{m})^2+1}{4}.$$

From here, one can easily verify the original displayed inequality.

We turn our attention to the following proposition that we used in Remark 4.3.4.

Proposition 4.5.4. *If* $R = k[x_1, \ldots, x_n]/(x_1^2, \ldots, x_n^2)$ *and* $\operatorname{char}(k) \neq 2$, *then* $\operatorname{cs}(R) = n-1$.

Proof. By applying Proposition 4.5.1 with $s = 0$, we have that $\operatorname{cs}(R) \geq n-1$, so it suffices to exhibit an ideal J of R such that $\mu(J) = n-1$ and $J^2 = \bar{\mathfrak{m}}^2$.

Consider the ideal $J = (\bar{x}_i + \bar{x}_{i+1} \mid 1 \leq i \leq n-1)$. Evidently, we have that $\mu(J) = n-1$. We claim that $\bar{x}_i\bar{x}_j \in J^2$ for any pair of integers $1 \leq i < j \leq n$. Observe that $\bar{x}_i\bar{x}_{i+1} = (\bar{x}_i + \bar{x}_{i+1})^2$ belongs to J^2 for each integer $1 \leq i \leq n-1$, hence $\bar{x}_i\bar{x}_{i+2} = (\bar{x}_i + \bar{x}_{i+1})(\bar{x}_{i+1} + \bar{x}_{i+2}) - x_i\bar{x}_{i+1} - \bar{x}_{i+1}\bar{x}_{i+2}$ belongs to J^2. We obtain $\bar{x}_i\bar{x}_j$ for any pair of integers $1 \leq i < j \leq n$ as follows.

(i.) Compute first the squares $(\bar{x}_i + \bar{x}_{i+1})^2$ of the generators of J for each integer $i \leq j-1$. From this, we obtain generators of J^2 of the form $\bar{x}_i\bar{x}_{i+1}$.

(ii.) Compute next the products $(\bar{x}_i + \bar{x}_{i+1})(\bar{x}_{i+1} + \bar{x}_{i+2})$ for each integer $i \leq j-2$. Using the previous step, we obtain generators of J^2 of the form $\bar{x}_i\bar{x}_{i+2}$.

(iii.) Compute the products $(\bar{x}_i+\bar{x}_{i+1})(\bar{x}_k+\bar{x}_{k+1})$ for each integer $i+2\leq k\leq j-1$. Use the previous steps to cancel any quadratic forms that have already appeared.

Ultimately, we find that $\bar{x}_i\bar{x}_j\in J^2$ for all integers $1\leq i<j\leq n$ so that $\bar{\mathfrak{m}}^2\subseteq J^2$. □

Our next proposition illustrates that when $t=n$, it is possible that $\operatorname{cs}(R)=n-1$ or $\operatorname{cs}(R)=n$, hence the lower bound for $\operatorname{cs}(R)$ provided in Proposition 4.5.1 is sharp in this case.

Proposition 4.5.5. *Let $R=k[x_1,x_2,x_3]/I$, where I is minimally generated by three monomials of degree two and* $\operatorname{char}(k)\neq 2$. *If $I=(x_i^2,x_j^2,x_ix_j)$ for some integers $1\leq i<j\leq 3$, then* $\operatorname{cs}(R)=3$; *otherwise,* $\operatorname{cs}(R)=2$.

Proof. By Proposition 4.5.1, we have that $\operatorname{cs}(R)[\operatorname{cs}(R)+1]\geq 2\left(\binom{3+1}{2}-3\right)=6$, hence we have that $\operatorname{cs}(R)\geq 2$. If $I=(x_i^2,x_j^2,x_ix_j)$, let us assume to the contrary that $\operatorname{cs}(R)=2$, i.e., there exists an ideal J such that $\mu(J)=2$ and $J^2=\bar{\mathfrak{m}}^2$. By Proposition 4.2.2, we may assume that $J=(a\bar{x}_i+b\bar{x}_j+c\bar{x}_k,d\bar{x}_i+e\bar{x}_j+f\bar{x}_k)$ for some elements $a,b,c,d,e,f\in k$. We claim that both c and f must be nonzero. For if not, then without loss of generality, we have that $J=(a\bar{x}_i+b\bar{x}_j,d\bar{x}_i+e\bar{x}_j+f\bar{x}_k)$ so that $J^2=(af\bar{x}_i\bar{x}_k+bf\bar{x}_j\bar{x}_k,2df\bar{x}_i\bar{x}_k+2ef\bar{x}_j\bar{x}_k+\bar{x}_k^2)$. But then, it would be the case that $3=\mu(\bar{\mathfrak{m}}^2)=\mu(J^2)\leq 2$ — a contradiction. Consequently, both c and f are nonzero, hence we may assume without loss of generality that $c=f=1$ and $J=(a\bar{x}_i+b\bar{x}_j+\bar{x}_k,d\bar{x}_i+e\bar{x}_j+\bar{x}_k)$. But then, $(a-d)\bar{x}_i+(b-e)\bar{x}_j$ is a linear combination of the generators of J, hence we may write $J=(a\bar{x}_i+b\bar{x}_j+\bar{x}_k,(a-d)\bar{x}_i+(b-e)\bar{x}_j)$. But this contradicts our previous observation that both generators of J must possess a nonzero multiple of $\bar{x}_k$. We conclude that $\operatorname{cs}(R)=3=\mu(\mathfrak{m})$.

We will assume henceforth that I is not generated by x_i^2, x_j^2, and x_ix_j for any integers $1\leq i<j\leq 3$. Consequently, there are five possibilities for I. Let i, j, and k be distinct indices.

(i.) If I contains three squarefree monomials, we have that $I=(x_1x_2,x_1x_3,x_2x_3)$. Observe that $J=(\bar{x}_1+\bar{x}_2,\bar{x}_1+\bar{x}_3)$ witnesses $\operatorname{cs}(R)$ since $I^2=(\bar{x}_1^2+\bar{x}_2^2,\bar{x}_1^2,\bar{x}_1^2+\bar{x}_3^2)$, from which it follows that $J^2=(\bar{x}_1^2,\bar{x}_2^2,\bar{x}_3^2)=\bar{\mathfrak{m}}^2$ and $\operatorname{cs}(R)=\mu(J)=2$.

(ii.) If I contains two squarefree monomials, then there are two possibilities for J. If $I=(x_i^2,x_ix_j,x_ix_k)$, it suffices to take $J=(\bar{x}_i+\bar{x}_j,\bar{x}_i+\bar{x}_k)$ since it follows that $J^2=(\bar{x}_j^2,\bar{x}_i\bar{x}_j,\bar{x}_k^2)=\bar{\mathfrak{m}}^2$ so that

$\operatorname{cs}(R) = \mu(J) = 2$. On the other hand, it is possible that $I = (x_i^2, x_i x_j, x_j x_k)$. Even in this case, we may take $J = (\bar{x}_i + \bar{x}_j, \bar{x}_i + \bar{x}_k)$ since it holds that $J^2 = (\bar{x}_j^2, \bar{x}_i\bar{x}_k, 2\bar{x}_i\bar{x}_k + \bar{x}_k^2) = (\bar{x}_j^2, \bar{x}_i\bar{x}_k, \bar{x}_k^2) = \bar{\mathfrak{m}}^2$ and $\operatorname{cs}(R) = \mu(J) = 2$.

(iii.) If I contains one squarefree monomial, then by our assumption at the beginning of the above paragraph, we must have that $I = (x_i^2, x_j^2, x_i x_k)$. Observe that $J = (\bar{x}_i + \bar{x}_j, \bar{x}_k)$ witnesses $\operatorname{cs}(R)$ since $J^2 = (\bar{x}_i\bar{x}_j, \bar{x}_j\bar{x}_k, \bar{x}_k^2) = \bar{\mathfrak{m}}^2$ and $\operatorname{cs}(R) = \mu(J) = 2$.

(iv.) If I contains no squarefree monomials, we have that $I = (x_1^2, x_2^2, x_3^2)$. By Proposition 4.5.4, we have that $\operatorname{cs}(R) = 2$. (We constructed J in the proof of Proposition 4.5.4.)

One can readily verify that these are all of the possibilities for I, so we are done. □

For the case of $n = 3$, if $s = 1$, then Proposition 4.5.1 implies that for $t \leq 5$, we have that $1 \leq \operatorname{cs}(R) \leq 3$. Our next proposition illustrates that $\operatorname{cs}(R)$ can lie strictly between these bounds.

Proposition 4.5.6. *Let $R = k[x_1, x_2, x_3]/I$, where I is minimally generated over $k[x_1, x_2, x_3]$ by $t = 4$ monomials of degree two and* $\operatorname{char}(k) \neq 2$. *We have that* $\operatorname{cs}(R) = 2$.

Proof. By Proposition 4.5.1, we have that $\operatorname{cs}(R)[\operatorname{cs}(R) + 1] \geq 2\left(\binom{3+1}{2} - 4\right) = 4$, from which it follows that $\operatorname{cs}(R) \geq 2$. Consider the following cases.

(i.) If $I = (x_1^2, x_2^2, x_3^2, x_i x_j)$ for some integers $1 \leq i < j \leq 3$, then $J = (\bar{x}_i + \bar{x}_k, \bar{x}_j + \bar{x}_k)$ witnesses $\operatorname{cs}(R)$, where k is the index remaining in the set $\{1,2,3\} \setminus \{i, j\}$. We note that $\bar{\mathfrak{m}}^2 = (\bar{x}_i\bar{x}_k, \bar{x}_j\bar{x}_k)$. Further, we have that J^2 is generated by $(\bar{x}_i + \bar{x}_k)^2 = 2\bar{x}_i\bar{x}_k$, $(\bar{x}_i + \bar{x}_k)(\bar{x}_j + \bar{x}_k) = \bar{x}_i\bar{x}_k + \bar{x}_j\bar{x}_k$, and $(\bar{x}_j + \bar{x}_k)^2 = 2\bar{x}_j\bar{x}_k$. By assumption that $\operatorname{char}(k) \neq 2$, it follows that $J^2 = (\bar{x}_i\bar{x}_k, \bar{x}_j\bar{x}_k) = \bar{\mathfrak{m}}^2$ so that $\operatorname{cs}(R) = 2$.

(ii.) If $I = (x_i^2, x_j^2, x_i x_j, x_i x_k)$ for some distinct indices i, j, k, then $J = (\bar{x}_j, \bar{x}_k)$ witnesses $\operatorname{cs}(R)$. We note that $\bar{\mathfrak{m}}^2 = (\bar{x}_k^2, \bar{x}_j\bar{x}_k) = J^2$ so that $\operatorname{cs}(R) = 2$.

(iii.) If $I = (x_i^2, x_j^2, x_i x_k, x_j x_k)$ for some distinct indices i, j, k, then $J = (\bar{x}_i + \bar{x}_j, \bar{x}_k)$ witnesses $\operatorname{cs}(R)$. We note that $\bar{\mathfrak{m}}^2 = (\bar{x}_k^2, \bar{x}_i\bar{x}_j)$. Further, we have that J^2 is generated by $(\bar{x}_i + \bar{x}_j)^2 = \bar{x}_i\bar{x}_j$ and $\bar{x}_k^2$ so that $J^2 = (\bar{x}_k^2, \bar{x}_i\bar{x}_j) = \bar{\mathfrak{m}}^2$ and $\operatorname{cs}(R) = 2$.

(iv.) If $I = (x_i^2, x_i x_j, x_i x_k, x_j x_k)$ for some distinct indices i, j, k, then $J = (\bar{x}_j, \bar{x}_k)$ witnesses $\operatorname{cs}(R)$. We note that $\bar{\mathfrak{m}}^2 = (\bar{x}_j^2, \bar{x}_k^2) = J^2$ so that $\operatorname{cs}(R) = 2$.

One can readily verify that these are all of the possibilities for I, so we are done. □

Proposition 4.5.7. *Let $R = k[x_1, \ldots, x_n]/I$ with $\operatorname{char}(k) \neq 2$, where I is minimally generated by $t = \binom{n+1}{2} - 1$ monomials of degree two. We have that $\operatorname{cs}(R) = 1$.*

Proof. We note that $\mathfrak{m}^2$ is generated by $\binom{n+1}{2}$ distinct monomials of degree two, so I consists of all but one quadratic monomial. Consequently, we have that $\bar{\mathfrak{m}}^2 = \bar{q}R$, where q is the quadratic monomial excluded from I. Observe that $J = (\sum_{i=1}^n \bar{x}_i)$ satisfies $J^2 = \bar{f}R = \mathfrak{m}^2$. We have conclude that $\operatorname{cs}(R) = 1$, as desired. □

Our next aim is to establish similar bounds for $\operatorname{ms}(R)$. We continue to restrict our attention to the case that $R = k[x_1, \ldots, x_n]/I$, where I is minimally generated by $t > 0$ quadratic monomials.

Proposition 4.5.8. *Let $R = k[x_1, \ldots, x_n]/I$, where I is minimally generated by $t > 0$ quadratic monomials.*

(1.) *If $n = 1$, then $\operatorname{ms}(R) = 0$.*

(2.) *If $n = 2$, $\bar{\mathfrak{m}}^2 \neq \bar{0}$, and $\operatorname{char}(k) \neq 2$, then $\operatorname{ms}(R) = 1$.*

Proof. (1.) Clearly, if $n = 1$, then $I = \mathfrak{m}^2$. Consequently, we have that $\bar{\mathfrak{m}}^2 = \bar{0}$ so that $\operatorname{ms}(R) = 0$.

(2.) If $n = 2$, then I must contain (at least) one of the quadratic monomials x_1^2, x_1x_2, or x_2^2. We claim that $J = (\bar{x}_1 + \bar{x}_2)$ satisfies $\bar{\mathfrak{m}}^2 \subseteq \bar{\mathfrak{m}}I$. Observe that $\bar{x}_i(\bar{x}_1 + \bar{x}_2) = \bar{x}_i\bar{x}_1 + \bar{x}_i\bar{x}_2$ and $(\bar{x}_1 + \bar{x}_2)^2 = \bar{x}_1^2 + 2\bar{x}_1\bar{x}_2 + \bar{x}_2^2$. If I contains either of the pure squares $\bar{x}_i^2$, then J must contain the other square $\bar{x}_j^2$ and the mixed term $\bar{x}_1\bar{x}_2$ by hypothesis that $\operatorname{char}(k) \neq 2$, and the aforementioned equations show that $\bar{\mathfrak{m}}^2 \subseteq J$. If I does not contain either of the pure squares, then it must contain $\bar{x}_1\bar{x}_2$, and again, we find that $\bar{\mathfrak{m}}^2 \subseteq J$. □

Proposition 4.5.9. *Let $R = k[x_1, \ldots, x_n]/I$, where I is any non-maximal homogeneous ideal of $k[x_1, \ldots, x_n]$ that contains all quadratic squarefree monomials, i.e., $(x_i x_j \mid 1 \leq i < j \leq n) \subseteq I \subsetneq \mathfrak{m}$. We have that $\operatorname{ms}(R) = 1$.*

Proof. Consider the ideal $J = (\bar{x}_1 + \cdots + \bar{x}_n)$. By assumption that $x_i x_j \in I$ for all $1 \leq i < j \leq n$, we have that

$$\bar{\mathfrak{m}}J = \left(\bar{x}_i \sum_{j=1}^{n} \bar{x}_j \mid 1 \leq i \leq n \right) = \left(\sum_{j=1}^{n} \bar{x}_i \bar{x}_j \mid 1 \leq i \leq n \right) = (\bar{x}_i^2 \mid 1 \leq i \leq n) = \bar{\mathfrak{m}}^2$$

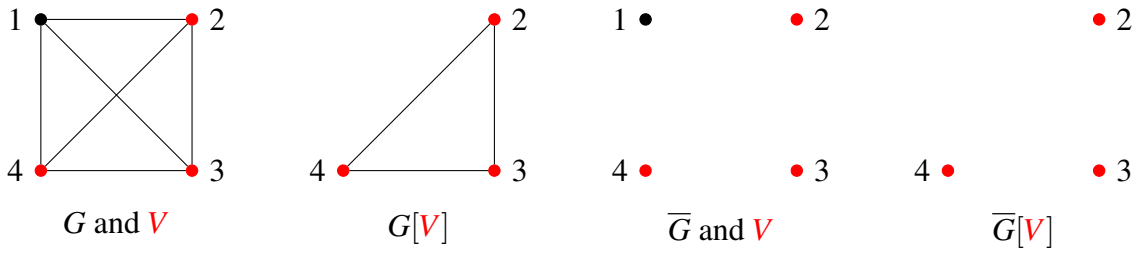
so that $\bar{\mathfrak{m}}^2 = \bar{\mathfrak{m}}J \subseteq J$. Consequently, it follows that $0 \leq \operatorname{ms}(R) \leq 1$. Even more, by hypothesis that I is not the homogeneous maximal ideal, we have that $\bar{\mathfrak{m}}^2 = (\mathfrak{m}^2 + I)/I \neq \bar{0}$, and we conclude that $\operatorname{ms}(R) = 1$. □

Our previous proposition suggests that $\operatorname{ms}(R)$ is controlled primarily by the quadratic squarefree monomials of $k[x_1, \ldots, x_n]$. Consequently, we devote the last section to this case.

4.6 Computing $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ for the Edge Ring of a Finite Simple Graph

Last, we turn our attention to the case that $R = k[x_1, \ldots, x_n]/I$ for some quadratic squarefree monomial ideal I. By the Stanley-Reisner Correspondence, this is equivalent to studying the combinatorial structures of finite simple graphs (cf. [MRS18, Chapter 4]). We denote by G a simple graph on the vertex set $[n] = \{1, 2, \ldots, n\}$ with edges denoted by unordered pairs $\{i, j\}$ for some integers $1 \leq i < j \leq n$. We say that a vertex i is **isolated** if $\{i, j\}$ is not an edge of G for any integer j. If G has no isolated vertices, then G is **connected**.

We say that a subgraph H of G is **induced** if the edge $\{i, j\}$ in G is an edge of H whenever H contains the vertices i and j. Given any nonempty set $V \subseteq [n]$, we will write $G[V]$ for the induced subgraph of G on the vertex set V. We define also the **complement graph** $\overline{G}$ on the vertex set $[n]$ such that $\{i, j\}$ is an edge of $\overline{G}$ if and only if it is not an edge of G. Observe that for any nonempty set $V \subseteq [n]$, the complement of an induced subgraph of G is the induced subgraph of $\overline{G}$ on the same underlying vertex set, i.e., we have that $\overline{G[V]} = \overline{G}[V]$. One can visualize the aforementioned constructions in the following example.



We denote by K_n the complete graph on $[n]$ with edges $\{i,j\}$ for all integers $1 \leq i < j \leq n$, hence K_n has $\binom{n}{2}$ edges. Observe that K_m is an induced subgraph of K_n for each integer $1 \leq m \leq n$.

Our main object of study throughout this section is defined as follows.

Definition 4.6.1. Given a finite simple graph G on the vertex set $[n]$ and any field k, we refer to the quadratic squarefree monomial ideal $I(G) = (x_i x_j \mid \{i,j\} \text{ is an edge of } G)$ of $k[x_1,\ldots,x_n]$ as the **edge ideal** of G, and we call the quotient ring $k(G) = k[x_1,\ldots,x_n]/I(G)$ the **edge ring** of G.

We will continue to study the homogeneous maximal ideal $\mathfrak{m} = (x_1,\ldots,x_n)$ of $k[x_1,\ldots,x_n]$ and its image $\bar{\mathfrak{m}}$ in $k(G)$. Our motivation to consider $\operatorname{ms}(R)$ and $\operatorname{cs}(R)$ from a graphical perspective is rooted in the results of Proposition 4.4.12 and Section 4.5. We begin with the following.

Proposition 4.6.2. *We have that* $\operatorname{ms}(k(K_n)) = 1$ *and* $\operatorname{cs}(k(K_n)) \geq \left\lceil \sqrt{2n+\frac{1}{4}} - \frac{1}{2} \right\rceil$ *for all* $n \geq 1$.

Proof. Observe that K_1 consists of one vertex, hence $k(K_1) = k[x]$ is regular, and the result holds by the first part of Proposition 4.3.3. Otherwise, we have that $n \geq 2$ and $I(K_n) = (x_i x_j \mid 1 \leq i < j \leq n)$. By Proposition 4.5.9, it follows that $\operatorname{ms}(k(K_n)) = 1$. Observe that $\bar{\mathfrak{m}}^2 = (\bar{x}_i^2 \mid 1 \leq i \leq n)$, hence Remark 4.5.3 implies that

$$\operatorname{cs}(k(K_n)) \geq \left\lceil \frac{\sqrt{8\mu(\bar{\mathfrak{m}}^2)+1}-1}{2} \right\rceil = \left\lceil \sqrt{2n+\frac{1}{4}} - \frac{1}{2} \right\rceil. \qquad \square$$

On the other hand, the lower bound for $\operatorname{cs}(k(K_t))$ is sharp whenever $t = \binom{r+1}{2}$ for some integer $r \geq 1$, i.e., t is a triangular number; the idea for the proof is due to Mark Denker.

Proposition 4.6.3. *Let* $t = \binom{r+1}{2}$ *for some integer* $r \geq 1$. *We have that* $\operatorname{cs}(k(K_t)) \leq \sqrt{2t+\frac{1}{4}} - \frac{1}{2} = r$.

Proof. By the Quadratic Formula, the upper bound holds because

$$t = \binom{r+1}{2} \text{ if and only if } r^2 + r - 2t = 0 \text{ if and only if } r = \frac{\sqrt{8t+1}-1}{2} = \sqrt{2t + \frac{1}{4}} - \frac{1}{2}.$$

Given any integer $r \geq 1$, we will construct an ideal J with $\mu(J) = r$ such that $J^2 = (\bar{x}_1^2, \ldots, \bar{x}_t^2)$, where $\bar{x}_i$ denotes the image of x_i modulo $I(K_t)$. We accomplish this via the following steps.

(i.) For each pair of distinct indices $1 \leq i < j \leq r$, choose a distinct monomial generator $m_{i,j}$ of $(\bar{x}_1, \ldots, \bar{x}_t)$. Once all $\binom{r}{2}$ monomials have been chosen as such, there will remain r unused monomial generators.

(ii.) Define homogeneous linear polynomials $f_1, \ldots, f_r$ as $f_i = \sum_{j \neq i} m_{i,j}$. Observe that each of the polynomials $f_1, \ldots, f_r$ is by definition the sum of $r-1$ distinct monomials. Even more, for each pair of distinct indices $1 \leq i < j \leq r$, the polynomials f_i and f_j have only one summand in common — the monomial $m_{i,j}$.

(iii.) For each integer $1 \leq i \leq r$, choose a monomial generator m_i that does not appear as a summand of any of the polynomials $f_1, \ldots, f_r$; then, define the polynomials $g_1, \ldots, g_r$ as $g_i = f_i + m_i$.

(iv.) Ultimately, we obtain r homogeneous linear polynomials $g_1, \ldots, g_r$, each of which is the sum of r distinct linear monomials. Observe that for each integer $1 \leq i \leq t$, we have that g_i^2 is the sum of the squares of all of its monomial summands. By construction, for each monomial summand m of f_i, there exists a distinct polynomial f_j such that m is a summand of f_j and $f_i f_j = m^2$. Consequently, the ideal J^2 contains all of the pure squares $\bar{x}_1, \ldots, \bar{x}_t^2$: they appear either as $m_{i,j}^2 = g_i g_j$ or $m_i^2 = g_i^2 - \sum_{j \neq i} g_i g_j$.

We conclude that the ideal $J = (g_1, \ldots, g_r)$ of $k(K_t)$ satisfies $J^2 = (\bar{x}_1^2, \ldots, \bar{x}_t^2)$ and $\mu(J) \leq r$. □

We illustrate the idea of proof of Proposition 4.6.3 in the following example.

Example 4.6.4. Let $r = 4$. Observe that $\binom{r+1}{2} = 10$, so it suffices to exhibit an ideal J of $\mathrm{cs}(K_{10})$ with $\mu(J) = 4$ and $J^2 = (\bar{x}_1^2, \cdots, \bar{x}_{10}^2)$. By the proof of Proposition 4.6.3, this can be accomplished as follows.

(i.) Choose the monomial generators $m_{i,j}$ for each pair of distinct integers $1 \leq i < j \leq 4$. We will simply take $m_{1,2} = \bar{x}_1$, $m_{1,3} = \bar{x}_2$, $m_{1,4} = \bar{x}_3$, $m_{2,3} = \bar{x}_4$, $m_{2,4} = \bar{x}_5$, and $m_{3,4} = \bar{x}_6$.

(ii.) Define the polynomials $f_i = \sum_{j \neq i} m_{i,j}$ for each integer $1 \leq i \leq r$. By our above choices, they are given by $f_1 = \bar{x}_1 + \bar{x}_2 + \bar{x}_3$, $f_2 = \bar{x}_1 + \bar{x}_4 + \bar{x}_5$, $f_3 = \bar{x}_2 + \bar{x}_4 + \bar{x}_6$, and $f_4 = \bar{x}_3 + \bar{x}_5 + \bar{x}_6$.

(iii.) Choose a monomial generator m_i that does not appear in f_i for each integer $1 \leq i \leq r$; then, add it to f_i, and call the resulting polynomial g_i. We will set $m_i = \bar{x}_{6+i}$ for each integer $1 \leq i \leq r$ so that $g_1 = \bar{x}_1 + \bar{x}_2 + \bar{x}_3 + \bar{x}_7$, $g_2 = \bar{x}_1 + \bar{x}_4 + \bar{x}_5 + \bar{x}_8$, $g_3 = \bar{x}_2 + \bar{x}_4 + \bar{x}_6 + \bar{x}_9$, and $g_4 = \bar{x}_3 + \bar{x}_5 + \bar{x}_6 + \bar{x}_{10}$.

(iv.) Observe that $\bar{x}_1^2 = g_1 g_2$, $\bar{x}_2^2 = g_1 g_3$, $\bar{x}_3^2 = g_1 g_4$, $\bar{x}_4^2 = g_2 g_3$, $\bar{x}_5^2 = g_2 g_4$, and $\bar{x}_6^2 = g_3 g_4$. Once we have these, it follows that $\bar{x}_7^2 = g_1^2 - \sum_{j \neq 1} g_1 g_j$, $\bar{x}_8^2 = g_2^2 - \sum_{j \neq 2} g_2 g_j$, $\bar{x}_9^2 = g_3^2 - \sum_{j \neq 3} g_3 g_j$, and $\bar{x}_{10}^2 = g_4^2 - \sum_{j \neq 4} g_4 g_j$.

By taking $J = (g_1, g_2, g_3, g_4)$, we find that $J^2 = (\bar{x}_1^2, \cdots, \bar{x}_{10}^2)$ and $\mu(J) \leq 4$.

We note that the invariants behave nicely with respect to induced subgraphs.

Proposition 4.6.5. *Given a finite simple graph G on the vertex set $[n]$ with an induced subgraph H on m vertices, we have that* $\operatorname{ms}(k(H)) \leq \operatorname{ms}(k(G))$ *and* $\operatorname{cs}(k(H)) \leq \operatorname{cs}(k(G))$.

Proof. We may assume that $H = G[V]$ is the induced subgraph on the vertex set $V = [m]$. Observe that for any edge $\{i, j\}$ of G such that $m+1 \leq i \leq n$, the monomial $x_i x_j$ of $I(G)$ belongs to the ideal $(x_{m+1}, \ldots, x_n)$ of $k[x_1, \ldots, x_n]$. Consequently, we have that $(x_{m+1}, \ldots, x_n) + I(G) = (x_{m+1}, \ldots, x_n) + I(H)$ so that

$$k(H) = \frac{k[x_1, \ldots, x_m]}{I(H)} \cong \frac{k[x_1, \ldots, x_n]}{(x_{m+1}, \ldots, x_n) + I(H)} = \frac{k[x_1, \ldots, x_n]}{(x_{m+1}, \ldots, x_n) + I(G)} \cong \frac{k(G)}{(\bar{x}_{m+1}, \ldots, \bar{x}_n)}.$$

By Proposition 4.2.10, we conclude that $\operatorname{ms}(k(G)) \geq \operatorname{ms}(k(H))$ and $\operatorname{cs}(k(G)) \geq \operatorname{cs}(k(H))$. □

Using a short technical lemma regarding the ceiling function in conjunction with the propositions established thus far, the lower bound for $\operatorname{cs}(k(K_n))$ is sharp for all integers $n \geq 1$ as follows.

Lemma 4.6.6. *Let $n,r,t \geq 1$ be integers such that $\binom{r}{2} < n \leq \binom{r+1}{2} = t$. If $f(n) = \sqrt{2n+\frac{1}{4}} - \frac{1}{2}$, then $\lceil f(n) \rceil = r$.*

Proof. Observe that f is an increasing function with $f(t) = r$ and $f\left(\binom{r}{2}\right) = r-1$. By hypothesis that $\binom{r}{2} < n \leq \binom{r+1}{2}$, it follows that $r-1 = f\left(\binom{r}{2}\right) < f(n) \leq f\left(\binom{r+1}{2}\right) = f(t) = r$. Consequently, the ceiling function yields $r-1 = \lceil r-1 \rceil < \lceil f(n) \rceil \leq \lceil r \rceil = r$ so that $\lceil f(n) \rceil = r$. □

Observe that t in the hypotheses of Lemma 4.6.6 is the smallest triangular number with $n \leq t$.

Corollary 4.6.7. *If $t = \binom{r+1}{2}$ is the smallest triangular number such that $n \leq t$, then $\operatorname{cs}(k(K_n)) = r$.*

Proof. Observe that K_n is an induced subgraph of K_t for every integer $t \geq n$. By Propositions 4.6.3 and 4.6.5, we have that $\operatorname{cs}(k(K_n)) \leq \operatorname{cs}(k(K_t)) = r$. Consequently, it suffices to show that $\operatorname{cs}(k(K_n)) \geq r$. But this is precisely what Proposition 4.6.2 and Lemma 4.6.6 together imply. □

Even more, $\operatorname{ms}(k(G))$ is monotone decreasing with respect to adding edges between existing vertices of G.

Proposition 4.6.8. *Let G be a finite simple graph that does not contain an edge $\{i,j\}$. Let G' be the finite simple graph obtained from G by adjoining the edge $\{i,j\}$. We have that*

$$\operatorname{ms}(k(G)) - 1 \leq \operatorname{ms}(k(G')) \leq \operatorname{ms}(k(G)).$$

Proof. Observe that $k(G') = k[x_1,\ldots,x_n]/[I(G) + (x_i x_j)] \cong k(G)/(\bar{x}_i \bar{x}_j)$, so the result follows at once by Corollary 4.2.12. □

Conversely, $\operatorname{ms}(k(G))$ is monotone increasing with respect to adding vertices to G.

Proposition 4.6.9. *Let H be a simple graph on the vertex set $[n]$. Let G be the simple graph obtained from H by adding some additional vertices $t+1,\ldots,n$. We have that*

$$\operatorname{ms}(k(G)) = \operatorname{ms}(k(H)) + n - t.$$

Proof. Observe that $k(G) \cong k(H)[X_{t+1}, \ldots, X_n]$, so this follows by Proposition 4.2.15. □

Corollary 4.6.10. *Let G be a finite simple graph on the vertex set $[n]$ with d isolated vertices. Let H be the induced subgraph of G on the non-isolated vertices. We have that* $\operatorname{ms}(k(G)) = \operatorname{ms}(k(H)) + d$.

Our immediate goal is to find bounds for $\operatorname{ms}(k(G))$ and $\operatorname{cs}(k(G))$ for several well-known families of graphs. Before we proceed with this agenda, we recall the following definitions.

Definition 4.6.11. Given a finite simple graph G on the vertex set $[n]$, we say that a set $C \subseteq [n]$ forms a **vertex cover** of G if for every edge $\{i, j\}$ of G, we have that $i \in C$ or $j \in C$. Further, we say that a vertex cover C is a **minimal vertex cover** if $C \setminus \{i\}$ is not a vertex cover of G for any vertex $i \in C$. We denote $\tau(G) = \min\{|C| : C \text{ is a vertex cover of } G\}$.

Definition 4.6.12. Given a finite simple graph G on the vertex set $[n]$, we say that a set $I \subseteq [n]$ forms an **independent vertex set** of G if $\{i, j\}$ is not an edge of G for any vertices $i, j \in I$. Further, we say that an independent vertex set I is a **maximal independent vertex set** if $I \cup \{i\}$ is not an independent vertex set for any vertex $i \notin I$. We denote $\alpha(G) = \max\{|I| : I \text{ is an independent vertex set of } G\}$.

Remark 4.6.13. By [MRS18, Theorem 4.3.6], there exists an irredundant primary decomposition of $I(G)$ in which each ideal is generated by the variables corresponding to the vertices of a distinct minimal vertex cover C. Considering that the height of an ideal in this primary decomposition is $|C|$, by Proposition 4.3.3, we have that $\operatorname{ms}(G) \geq \dim k(G) = n - \operatorname{ht}(I(G)) = n - \tau(G) = \alpha(G)$, where the last equality holds by [Wes00, Lemma 3.1.21].

Corollary 4.6.14. *We have that* $\operatorname{ms}(k(G)) = 1$ *if and only if G is a complete graph.*

Proof. One direction holds by Proposition 4.6.2. Conversely, if G is not complete, then $\{v, w\}$ is not an edge of G for some vertices v and w of G, i.e., it is an independent vertex set. We conclude that $\operatorname{ms}(k(G)) \geq \alpha(G) \geq 2$. □

If k is infinite, we may also obtain bounds for $\operatorname{ms}(k(G))$ based on the number of edges of G.

Proposition 4.6.15. *Let G be a simple graph with n vertices with at least one edge $\{i, j\}$. If the field k is infinite, then* $\operatorname{ms}(k(G)) \leq n-1$. *Even more, if G has at least $n+1$ edges, then* $\operatorname{ms}(k(G)) \leq n-2$.

Proof. Considering that $\{i, j\}$ is an edge, the monomial $\bar{x}_i\bar{x}_j$ vanishes in $k(G)$. Consequently, we have that $\mu(\bar{\mathfrak{m}}^2) < \binom{\mu(\bar{\mathfrak{m}})+1}{2}$. If k is infinite, then $\operatorname{ms}(k(G)) \leq \mu(\bar{\mathfrak{m}}) - 1 = n-1$ by Corollary 4.3.11. Further, if G has at least $n+1$ edges, then $\overline{G}$ has at most $\binom{n}{2} - n - 1$ edges, hence we have that $\mu(\bar{\mathfrak{m}}^2) \leq \binom{n}{2} - 1 < \binom{n}{2}$. □

We will now demonstrate that if the complement graph $\overline{G}$ satisfies a certain property on its induced subgraphs, then $\operatorname{ms}(k(G))$ is precisely the independence number of G. Before we do so, we make the following definitions.

Definition 4.6.16. We say that a finite simple graph G is **chordal** if it has no induced subgraph that is isomorphic to a cycle graph C_i for any integer $i \geq 4$.

We refer to an induced subgraph of G that is isomorphic to a cycle graph C_i with $i \geq 3$ as an **induced cycle of length** i. Consequently, if G has no induced cycles of length $i \geq 4$, it is chordal.

Definition 4.6.17. Given a finite simple graph G such that $\overline{G}$ is not chordal, we define

$$\operatorname{mcn}(G) = \min\{i \geq 4 \mid C_i \text{ is an induced subgraph of } \overline{G}\}.$$

Proposition 4.6.18. *Let G be a simple graph on n vertices. If $\overline{G}$ is not chordal, then $\alpha(G) \leq n - \operatorname{mcn}(G) + 3$.*

Proof. By the exposition preceding Definition 4.6.33, we have that $\alpha(G) = \omega(\overline{G})$, i.e., the maximum size of a clique of $\overline{G}$. Let Q be a clique of $\overline{G}$ of size $\omega(\overline{G})$. Let C be a cycle of $\overline{G}$ of size $\operatorname{mcn}(G) \geq 4$. We claim that no more than three vertices of G lie in both Q and C. On the contrary, if $i \geq 4$ vertices of G lie in both Q and C, then the induced subgraph H of $\overline{G}$ on these i vertices must be K_i because Q is a clique. But this is a contradiction: H is an induced subgraph of the $\operatorname{mcn}(G)$-cycle C, which does not admit K_i as an induced subgraph for $i \geq 4$. We conclude that the number of vertices that Q and C have in common is no more than three, hence we find that $\alpha(G) + \operatorname{mcn}(G) = \omega(\overline{G}) + \operatorname{mcn}(G) = |V(Q)| + |V(C)| = |V(Q) \cup V(C)| + |V(Q) \cap V(C)| \leq n + 3$. □

Proposition 4.6.19. *Let G be a simple graph on the vertex set $[n]$. Let k be an infinite field. If $\overline{G}$ is chordal, then* $\operatorname{ms}(k(G)) = \alpha(G)$. *If $\overline{G}$ is not chordal, then* $\operatorname{ms}(k(G)) \leq n - \operatorname{mcn}(G) + 3$.

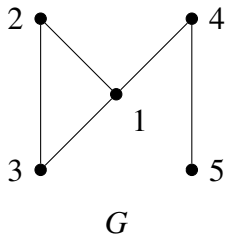
Proof. We will assume first that $\overline{G}$ is chordal. By [Frö90, Theorem 1], the edge ideal $I(G)$ of $k[x_1,\ldots,x_n]$ has a linear resolution. Put another way, the minimal free resolution of $I(G)$ is linear for $k-1$ steps for each integer $k \geq 1$. Particularly, the minimal free resolution $I(G)$ is linear for $\operatorname{ht}(I(G))-1$ steps. By [EHU06, Corollary 5.2], we conclude that $\mathfrak{m}^2 \subseteq I(G)+L$ for any ideal L generated by $n-\operatorname{ht}(I(G))$ linearly independent general linear forms, where $\mathfrak{m}$ denotes the maximal irrelevant ideal of $k[x_1,\ldots,x_n]$. Consequently, we have that $\operatorname{ms}(k(G)) \leq \mu(L) = n - \operatorname{ht}(I(G)) = \alpha(G)$. By Proposition 4.3.3(1.) and Remark 4.6.13, we conclude that $\operatorname{ms}(k(G)) = \alpha(G)$.

We will assume now that $\overline{G}$ is not chordal, i.e., $\overline{G}$ has an induced cycle of length $i \geq 4$. Crucially, observe that $\overline{G}$ has no induced cycles of length $4 \leq i \leq \operatorname{mcn}(G)-1 = (\operatorname{mcn}(G)-3)+2$. By [DHS11, Theorem 2.7], we have that $I(G)$ is $(\operatorname{mcn}(G)-4) = [(\operatorname{mcn}(G)-3)-1]$-steps linear. By Proposition 4.6.18, we have that $\operatorname{mcn}(G)-3 \leq n-\alpha(G) = n - \dim k(G) = \operatorname{ht}(I(G))$, and then, [EHU06, Corollary 5.2] yields $\operatorname{ms}(k(G)) \leq n - \operatorname{mcn}(G) + 3$. □

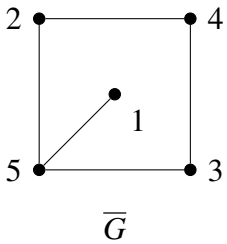
Corollary 4.6.20. *Let G be a finite simple graph with at least two vertices. Let k be an infinite field. If $\overline{G}$ has no induced cycles (i.e., if $\overline{G}$ is a tree), then* $\operatorname{ms}(k(G)) = 2$.

Proof. Observe that $\overline{G}$ is chordal with $\alpha(G) = \omega(\overline{G}) = 2$. □

Remark 4.6.21. For a finite simple graph G whose complement graph $\overline{G}$ is not chordal, it is possible for the upper bound produced in Proposition 4.6.19 to be strict, as the following illustrates.



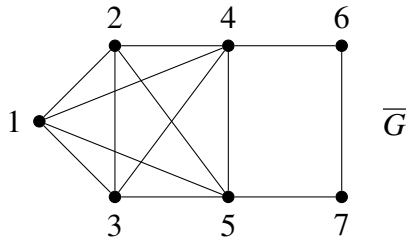
G



$\overline{G}$

Observe that $\operatorname{mcn}(G) = 4$ so that $\operatorname{ms}(k(G)) \leq 4 = n - \operatorname{mcn}(G) + 3$ by Proposition 4.6.19; however, the ideal $J = (x_1+x_2, x_1+x_3, x_4+x_5)$ satisfies $\mathfrak{m}^2 \subseteq I(G)+J$ so that $\operatorname{ms}(k(G)) \leq 3$.

Remark 4.6.22. The converse of the first part of Proposition 4.6.19 does not hold: the finite simple graph G whose complement is pictured below satisfies $\overline{G}$ is not chordal and $\mathrm{ms}(k(G)) = \alpha(G)$.



By Proposition 4.3.10, if k is infinite and $n + \#E(\overline{G}) < \binom{r+2}{r}$, then $\mathrm{ms}(k(G)) \leq r$, where $\#E(\overline{G})$ denotes the number of edges of $\overline{G}$. Observe that $\#E(\overline{G}) = \binom{5}{2} + 3$ so that $n + \#E(\overline{G}) = 20 < \binom{5+2}{2}$ and $\mathrm{ms}(k(G)) \leq 5$. On the other hand, the vertex set $I = \{1,2,3,4,5\}$ of G is independent, hence we have that $5 \leq \alpha(G) \leq \mathrm{ms}(k(G))$. We conclude that $\mathrm{ms}(k(G)) = \alpha(G)$, but $\overline{G}$ is not chordal, as $\overline{G}[\{4,5,6,7\}]$ is isomorphic to the four-cycle C_4.

Generally, this construction yields an infinite family of graphs G_n on $n \geq 7$ vertices with $\mathrm{ms}(k(G_n)) = \alpha(G_n) = n-2$ whose complement graphs $\overline{G_n}$ are not chordal. Explicitly, define $\overline{G_n}$ to be the complete graph K_{n-2} on the vertices $1,2,\ldots,n-2$ adjoined with the edges $\{n-3,n-1\}$, $\{n-2,n\}$, and $\{n-1,n\}$. Observe that

$$n + \#E(\overline{G_n}) = n + \binom{n-2}{2} + 3 = \frac{2n + (n-2)(n-3) + 6}{2} = \frac{n^2 - 3n + 12}{2},$$

from which it follows that

$$\binom{n}{2} - n - \#E(\overline{G_n}) = \frac{n^2 - n}{2} - \frac{n^2 - 3n + 12}{2} = \frac{2n - 12}{2} = n - 6 > 0$$

for all integers $n \geq 7$. By Proposition 4.3.10, we conclude that $\mathrm{ms}(k(G_n)) \leq n-2$. Conversely, the vertex set $I = \{1,2,\ldots,n-2\}$ of G is independent so that $n-2 \leq \alpha(G_n) \leq \mathrm{ms}(k(G_n))$.

We note that this construction also provides a simple graph G on n vertices such that $\mathrm{ms}(k(G)) = \alpha(G)$ and $\alpha(G) < n - \mathrm{mcn}(G) + 3$ whenever k is infinite. By the second part of Proposition 4.6.19, if $\alpha(G) = n - \mathrm{mcn}(G) + 3$, then $\mathrm{ms}(k(G)) = \alpha(G)$; however, for each integer $n \geq 7$,

the complement graph $\overline{G_n}$ is not chordal but it holds that $\operatorname{ms}(k(G_n)) = \alpha(G_n)$, and we have that $\alpha(G_n) = n-2 < n - \operatorname{mcn}(G) + 3$.

Our next proposition partially answers the question posed prior to Definition 4.6.16.

Proposition 4.6.23. *Let G be the graph obtained from the complete graph K_n on $n \geq 3$ vertices by removing $1 \leq \ell \leq \lfloor \frac{n}{2} \rfloor$ pairwise non-adjacent edges. If k is infinite, then we have that* $\operatorname{ms}(k(G)) = 2$.

Proof. Observe that $\overline{G}$ consists of $n-2\ell$ isolated vertices and ℓ pairwise non-adjacent edges. Consequently, $\overline{G}$ is chordal, and we have that $\operatorname{ms}(k(G)) = \alpha(G) = 2$ by Proposition 4.6.19. □

If k is an infinite field, then Proposition 4.6.15 demonstrates that $\operatorname{ms}(k(G)) \leq n-1$. Our next proposition investigates a class of graphs with $\alpha(G) = n-1$.

Proposition 4.6.24. *Let S_n be the star graph on $n \geq 3$ vertices, i.e., the graph with edges $\{1,i\}$ for each integer $2 \leq i \leq n$. We have that* $\operatorname{cs}(k(S_n)) = n$ *and* $\operatorname{ms}(k(S_n)) = n-1$.

Proof. Observe that $I(S_n) = (x_1x_i \mid 2 \leq i \leq n)$ is generated by $t = n-1$ homogeneous polynomials of degree two. By Proposition 4.5.1, we conclude that $\operatorname{cs}(k(S_n)) = n$.

Consider the ideal $J = (\bar{x}_1 + \bar{x}_i \mid 2 \leq i \leq n)$. We find that $\bar{x}_1^2 = \bar{x}_1(\bar{x}_1 + \bar{x}_i)$ and $\bar{x}_i^2 = \bar{x}_i(\bar{x}_1 + \bar{x}_i)$ are in $\bar{\mathfrak{m}}J$ for all integers $2 \leq i \leq n$. Likewise, we have that $\bar{x}_i\bar{x}_j = \bar{x}_j(\bar{x}_1 + \bar{x}_i)$ is in $\bar{\mathfrak{m}}J$ for all integers $2 \leq i < j \leq n$. We conclude that $\bar{\mathfrak{m}}^2 \subseteq \bar{\mathfrak{m}}J$ so that $\operatorname{ms}(k(S_n)) \leq n-1$.

Conversely, the vertices $2, 3, \ldots, n$ are independent, hence we have that $\operatorname{ms}(k(S_n)) \geq n-1$. □

Remark 4.6.25. If k is infinite, then we have that $\operatorname{ms}(k(S_n)) = n-1$ by Proposition 4.6.19: the complement graph $\overline{S_n}$ is the graph union of K_1 and the complete graph K_{n-1}, hence it is chordal with $\alpha(S_n) = n-1$. For a detailed explanation of this argument, see the discussion preceding Proposition 4.6.42.

If $\operatorname{mcn}(G) = 4$ and k is infinite, then $\operatorname{ms}(k(G)) \leq n-4+3 = n-1$; however, this upper bound follows already from Proposition 4.6.15. Consequently, Proposition 4.6.19 does not provide any new information. Going forward, our aim is to understand graphs with $\operatorname{mcn}(G) = 4$. We make use of the following terminology.

Definition 4.6.26. We say that a finite simple graph G is **gap-free** if $\overline{G}$ has no induced cycle of length 4. Put another way, G is gap-free if and only if either $\overline{G}$ is chordal or $\operatorname{mcn}(G) \geq 5$.

Considering that an induced cycle of length 4 in $\overline{G}$ arises from a pair of non-adjacent edges in G that are not connected by a third edge, it follows that many familiar graphs are not gap-free and therefore satisfy $\operatorname{mcn}(G) = 4$. We present non-trivial bounds on $\operatorname{ms}(k(G))$ and $\operatorname{cs}(k(G))$ for these graphs whenever possible.

Proposition 4.6.27. *Let P_n be the path graph on $n \geq 4$ vertices with edges $\{i, i+1\}$ for each integer $1 \leq i \leq n-1$. We have that $\operatorname{cs}(k(P_n)) = n$ and $\lceil \frac{n}{2} \rceil \leq \operatorname{ms}(k(P_n)) \leq n-1$.*

Proof. We note that the edge ideal $I(P_n) = (x_i x_{i+1} \mid 1 \leq i \leq n-1)$ is generated by $t = n-1$ homogeneous polynomials of degree two. By Proposition 4.5.1, we conclude that $\operatorname{cs}(k(P_n)) = n$.

Consider the ideals $J = (\bar{x}_i + \bar{x}_{i+1} \mid 1 \leq i \leq n-1)$ and $\bar{\mathfrak{m}}^2 = (\bar{x}_i^2 \mid 1 \leq i \leq n) + (\bar{x}_i \bar{x}_j \mid 3 \leq i+2 \leq j \leq n)$ of $k(P_n)$. We obtain the pure squares $\bar{x}_i^2$ of $\bar{\mathfrak{m}}^2$ in $\bar{\mathfrak{m}}J$ by taking the products $\bar{x}_i(\bar{x}_i + \bar{x}_{i+1})$. Further, the mixed terms $\bar{x}_i \bar{x}_j$ with $3 \leq i+2 \leq j \leq n$ can be obtained as follows.

(i.) Using the fact that $\bar{x}_i \bar{x}_{i+1}$ vanishes in $k(P_n)$, we have that $\bar{x}_i(\bar{x}_{i+1} + \bar{x}_{i+2}) = \bar{x}_i \bar{x}_{i+2}$.

(ii.) Using the previous step, it follows that $\bar{x}_i \bar{x}_{i+3} = \bar{x}_i(\bar{x}_{i+2} + \bar{x}_{i+3}) - \bar{x}_i \bar{x}_{i+2}$ is in $\bar{\mathfrak{m}}J$.

(iii.) Continue in this manner to obtain $\bar{x}_i \bar{x}_k$ for all integers $i+2 \leq k \leq j$.

We conclude that $\bar{\mathfrak{m}}^2 \subseteq \bar{\mathfrak{m}}J$, from which it follows that $\operatorname{ms}(k(P_n)) \leq n-1$.

On the other hand, we have that $\alpha(P_n) = \lceil \frac{n}{2} \rceil$ so that $\operatorname{ms}(k(P_n)) \geq \lceil \frac{n}{2} \rceil$ by Remark 4.6.13. Explicitly, the collection of $\lceil \frac{n}{2} \rceil$ odd vertices of P_n is a maximum independent vertex set. □

Remark 4.6.28. We have that $\operatorname{ms}(k(P_4)) = 2$, as the ideal $J = (\bar{x}_1 + \bar{x}_2, \bar{x}_3 + \bar{x}_4)$ of $k(P_4)$ contains $\bar{\mathfrak{m}}^2$. On the other hand, the path graph P_n is not gap-free for any integer $n \geq 5$. If k is infinite, we may conclude that $\operatorname{ms}(k(P_n)) \leq n-1$ by Proposition 4.6.15.

Proposition 4.6.29. *Let C_n be the cycle graph on $n \geq 3$ vertices, i.e., the path graph P_n together with the edge $\{1, n\}$. We have that $n-1 \leq \operatorname{cs}(k(C_n)) \leq n$ and $\lfloor \frac{n}{2} \rfloor \leq \operatorname{ms}(k(C_n)) \leq n-1$. If $n \geq 3$ is odd, then $\operatorname{cs}(k(C_n)) = n-1$. If $n = 3$, then $\operatorname{ms}(k(C_n)) = \lfloor \frac{n}{2} \rfloor$. For $n \leq 7$, we have that $\operatorname{ms}(k(C_n)) \leq \lceil \frac{n}{2} \rceil$. Equality holds for $n = 4$ and $n = 6$.*

Proof. Observe that $I(C_n) = (x_i x_{i+1} \mid 1 \leq i \leq n-1) + (x_1 x_n)$ is generated by $t = n$ quadratic monomials. By Proposition 4.5.1 with $s = 0$ and Proposition 4.3.3, we have $n-1 \leq \operatorname{cs}(k(C_n)) \leq n$.

Clearly, the cycle graph C_3 and the complete graph K_3 are isomorphic, hence we have that $\operatorname{ms}(k(C_3)) = 1 = \left\lfloor \frac{3}{2} \right\rfloor$ by Proposition 4.6.2. Generally, we find that $\operatorname{ms}(k(C_n)) \geq \alpha(C_n) = \left\lfloor \frac{n}{2} \right\rfloor$ by Remark 4.6.13, as the $\left\lfloor \frac{n}{2} \right\rfloor$ even vertices of C_n form a maximum independent vertex set.

Consequently, it remains to prove the last two statements. We will exhibit for each integer $4 \leq n \leq 7$ an ideal J of $k(C_n)$ such that $\mu(J) = \left\lceil \frac{n}{2} \right\rceil$ and $\bar{\mathfrak{m}}^2$ is contained in $\bar{\mathfrak{m}}J$.

For $n = 4$, we have $I(C_n) = (x_1x_2, x_2x_3, x_3x_4, x_1x_4)$ and $\bar{\mathfrak{m}}^2 = (\bar{x}_1^2, \bar{x}_2^2, \bar{x}_3^2, \bar{x}_4^2) + (\bar{x}_1\bar{x}_3, \bar{x}_2\bar{x}_4)$. Consider the ideal $J = (\bar{x}_1 + \bar{x}_2, \bar{x}_3 + \bar{x}_4)$ of $k(C_n)$. We obtain the pure squares $\bar{x}_i^2$ of $\bar{\mathfrak{m}}^2$ in $\bar{\mathfrak{m}}J$ by taking the products $\bar{x}_i(\bar{x}_i + \bar{x}_{i+1})$ and $\bar{x}_{i+1}(\bar{x}_i + \bar{x}_{i+1})$ for $i = 1$ and $i = 3$. We obtain the terms $\bar{x}_1\bar{x}_3$ and $\bar{x}_2\bar{x}_4$ by taking $\bar{x}_1(\bar{x}_3 + \bar{x}_4)$ and $\bar{x}_2(\bar{x}_3 + \bar{x}_4)$. We conclude that $\operatorname{ms}(k(C_4)) = 2 = \left\lceil \frac{4}{2} \right\rceil$.

For $n = 5$, we have $I(C_n) = (x_1x_2, x_2x_3, x_3x_4, x_4x_5, x_1x_5)$ and

$$\bar{\mathfrak{m}}^2 = (\bar{x}_1^2, \bar{x}_2^2, \bar{x}_3^2, \bar{x}_4^2, \bar{x}_5^2) + (\bar{x}_1\bar{x}_3, \bar{x}_1\bar{x}_4, \bar{x}_2\bar{x}_4, \bar{x}_2\bar{x}_5, \bar{x}_3\bar{x}_5).$$

Consider the ideal $J = (\bar{x}_1 + \bar{x}_2, \bar{x}_3 + \bar{x}_4, \bar{x}_4 + \bar{x}_5)$ of $k(C_n)$. We obtain the pure squares $\bar{x}_i^2$ of $\bar{\mathfrak{m}}^2$ in the same fashion as in the previous paragraph. Further, we obtain the mixed terms by taking $\bar{x}_3(\bar{x}_1 + \bar{x}_2)$, $\bar{x}_1(\bar{x}_4 + \bar{x}_5)$, $\bar{x}_2(\bar{x}_3 + \bar{x}_4)$, $\bar{x}_2(\bar{x}_4 + \bar{x}_5) - \bar{x}_2\bar{x}_4$, and $\bar{x}_3(\bar{x}_4 + \bar{x}_5)$, respectively.

For $n = 6$, we have $I(C_n) = (x_i x_{i+1} \mid 1 \leq i \leq 5) + (x_1x_6)$ and

$$\bar{\mathfrak{m}}^2 = (\bar{x}_i^2 \mid 1 \leq i \leq 6) + (\bar{x}_i\bar{x}_j \mid 3 \leq i+2 \leq j \leq 6 \text{ and } j \leq i+4).$$

Consider the ideal $J = (\bar{x}_1 + \bar{x}_2, \bar{x}_3 + \bar{x}_4, \bar{x}_5 + \bar{x}_6)$ of $k(C_n)$. We obtain the pure squares $\bar{x}_i^2$ of $\bar{\mathfrak{m}}^2$ as in the previous two paragraphs; then, we obtain the mixed terms sequentially by first gathering all of the $\bar{x}_i\bar{x}_j$ such that $j = i+2$. Explicitly, we have that $\bar{x}_3(\bar{x}_1 + \bar{x}_2) = \bar{x}_1\bar{x}_3$, $\bar{x}_2(\bar{x}_3 + \bar{x}_4) = \bar{x}_2\bar{x}_4$, $\bar{x}_5(\bar{x}_3 + \bar{x}_4) = \bar{x}_3\bar{x}_5$, and $\bar{x}_6(\bar{x}_4 + \bar{x}_5) = \bar{x}_4\bar{x}_6$ in $k(C_n)$. We use these to gather all of the $\bar{x}_i\bar{x}_j$ such that $j = i+3$. We have that $\bar{x}_1(\bar{x}_3 + \bar{x}_4) - \bar{x}_1\bar{x}_3 = \bar{x}_1\bar{x}_4$, $\bar{x}_2(\bar{x}_4 + \bar{x}_5) - \bar{x}_2\bar{x}_4 = \bar{x}_2\bar{x}_5$, and $\bar{x}_3(\bar{x}_5 + \bar{x}_6) - \bar{x}_3\bar{x}_5 = \bar{x}_3\bar{x}_6$. Last, we gather the terms $\bar{x}_i\bar{x}_j$ such that $j + i = 4$. We have that $\bar{x}_1(\bar{x}_5 + \bar{x}_6) = \bar{x}_1\bar{x}_5$ and

$\bar{x}_6(\bar{x}_1+\bar{x}_2)=\bar{x}_2\bar{x}_6$ in $k(C_n)$. We conclude that $\bar{\mathfrak{m}}^2 \subseteq \bar{\mathfrak{m}}J$ so that $\operatorname{ms}(k(C_6)) \leq 3$. Considering that $\alpha(C_6)=\lceil \frac{6}{2} \rceil = 3$, we have that $\operatorname{ms}(k(C_6)) = \lceil \frac{6}{2} \rceil$.

For $n=7$, we have $I(C_n)=(x_ix_{i+1} \mid 1 \leq i \leq 6)+(x_1x_7)$ and

$$\bar{\mathfrak{m}}^2=(\bar{x}_i^2 \mid 1 \leq i \leq 7)+(\bar{x}_i\bar{x}_j \mid 3 \leq i+2 \leq j \leq 7 \text{ and } j \leq i+5).$$

Consider the ideal $J=(\bar{x}_1+\bar{x}_2,\bar{x}_3+\bar{x}_4,\bar{x}_5+\bar{x}_6,\bar{x}_6+\bar{x}_7)$ of $k(C_n)$. We obtain the pure squares $\bar{x}_i^2$ of $\bar{\mathfrak{m}}^2$ as in the previous three paragraphs and the mixed terms as in the previous paragraph.

Finally, if $n=2m+1$ for some integer $m \geq 1$, then the ideal $J=(\bar{x}_1+\bar{x}_i \mid 2 \leq i \leq 2m+1)$ of $k(C_n)$ satisfies $\bar{\mathfrak{m}}^2=J^2$. Observe that $I(C_n)=(x_ix_{i+1} \mid 1 \leq i \leq 2m)+(x_1x_{2m+1})$ and

$$\bar{\mathfrak{m}}^2=(\bar{x}_i^2 \mid 1 \leq i \leq 2m+1)+(\bar{x}_i\bar{x}_j \mid 3 \leq i+2 \leq j \leq 2m+1).$$

We obtain the pure squares $\bar{x}_i^2$ of $\bar{\mathfrak{m}}^2$ for each integer $1 \leq i \leq 2m+1$ by taking

$$\bar{x}_1^2=\sum_{j=2}^{2m}(-1)^j(\bar{x}_1+\bar{x}_j)(\bar{x}_1+\bar{x}_{j+1}) \text{ and}$$
$$\bar{x}_i^2=(\bar{x}_1+\bar{x}_i)^2+\sum_{j=2}^{i-1}(-1)^{i+j}(\bar{x}_1+\bar{x}_j)(\bar{x}_1+\bar{x}_{j+1})+\sum_{j=i}^{2m}(-1)^{i+j+1}(\bar{x}_1+\bar{x}_j)(\bar{x}_1+\bar{x}_{j+1}).$$

Considering that the pure squares of $\bar{\mathfrak{m}}^2$ belong to J^2, we obtain the mixed terms as follows.

(i.) We have that $\bar{x}_1\bar{x}_3=(\bar{x}_1+\bar{x}_2)(\bar{x}_1+\bar{x}_3)-\bar{x}_1^2$.

(ii.) We have that $\bar{x}_1\bar{x}_4=(\bar{x}_1+\bar{x}_3)(\bar{x}_1+\bar{x}_4)-\bar{x}_1^2-\bar{x}_1\bar{x}_3$.

(iii.) Continuing in this manner, we obtain all mixed terms $\bar{x}_1\bar{x}_j$ with $2 \leq j \leq 2m+1$.

(iv.) We obtain the remaining mixed terms $\bar{x}_i\bar{x}_j$ for some integers $4 \leq i+2 \leq j \leq 2m+1$ by observing that $\bar{x}_i\bar{x}_j=(\bar{x}_1+\bar{x}_i)(\bar{x}_1+\bar{x}_j)-\bar{x}_1^2-\bar{x}_1\bar{x}_i-\bar{x}_1\bar{x}_j$.

We conclude that $\operatorname{cs}(k(C_n))=\operatorname{cs}(k(C_{2m+1}))=2m=n-1$. □

Corollary 4.6.30. *We have that* $\operatorname{ms}(k(P_5))=3$ *and* $3 \leq \operatorname{ms}(k(P_6)) \leq 4$.

Proof. Observe that P_n is isomorphic to the induced subgraph $C_{n+1}[\{1,2,\ldots,n\}]$. By Propositions

4.6.5, 4.6.27, and 4.6.29, we conclude that $\lceil \frac{n}{2} \rceil \leq \operatorname{ms}(k(P_n)) \leq \operatorname{ms}(k(C_{n+1})) \leq \lceil \frac{n+1}{2} \rceil$ for each integer $n \leq 6$. □

Remark 4.6.31. Unfortunately, the technique of the proof of Proposition 4.6.29 fails to produce an ideal that witnesses $\operatorname{ms}(k(C_n))$ for $n \geq 8$. Consider the cycle graph C_8 with edge ideal $I(C_8) = (x_i x_{i+1} \mid 1 \leq i \leq 7) + (x_1 x_8)$. Using the same approach as in the proof, the ideal $J = (\bar{x}_1 + \bar{x}_2, \bar{x}_3 + \bar{x}_4, \bar{x}_5 + \bar{x}_6, \bar{x}_7 + \bar{x}_8)$ of $k(C_8)$ is a prospective witness of $\operatorname{ms}(k(C_8))$; however, one can show that the element $\bar{x}_1 \bar{x}_5$ of $\bar{\mathfrak{m}}^2$ is not contained in J.

Remark 4.6.32. We believe that $\operatorname{ms}(k(C_n)) \leq \lceil \frac{n}{2} \rceil$ does not hold for all integers $n \geq 8$ whenever k has characteristic zero. Using the following code in Macaulay2, one can generate any number of random ideals in $\mathbb{Q}(C_8)$ and subsequently test whether such an ideal witnesses $\operatorname{ms}(\mathbb{Q}(C_8))$.

```
loadPackage "EdgeIdeals";
loadPackage "RandomIdeals";

setRandomSeed(currentTime())

-- Declare the file to which a witness ideal will be written.
file = "msWitnessIdealsC_n";

-- Declare the number of variables for the cycle.
n = 8

-- Establish the polynomial ring and its homogeneous maximal ideal.
R = QQ[x_1 .. x_n];
m = ideal(vars R);

-- Declare the number of random ideals to test.
```

```
numRuns = 1000000;

-- Define the graph G and the edge ideal of G in R.
G = cycle R;
I = edgeIdeal G;

-- Specify the generators. The first entry is the degree of a monomial.
B = basis(1, R);

-- Create a list whose length is the total number of possible generators.
-- The integers in the list prescribe how Macaulay2 will randomly choose a
-- monomial of this degree (randomly means that 0 is a possible coefficient,
-- so the 0 polynomial could appear). E.g., in the following list, Macaulay2
-- will randomly choose four degree one terms.
L = {1,1,1,1};

-- This begins the loop. First, we generate a random ideal J; then, we test
-- if m^2 is a subset of I + J. If it is, then J is written to the file, and
-- a new line is created. The loop ends after numRuns iterations.
for iter from 1 to numRuns do (
  J = randomIdeal(L, B);
  if isSubset(m^2, I + J) then {
    file << J << endl;
  };);

file << close;
```

Consistently, for one million random ideals, we could not find an ideal J of $k(C_8)$ with $\mu(J) = 4$

and $\bar{\mathfrak{m}}^2 \subseteq J$. Certainly, further testing is required to determine if this is the case for larger values.

On the other hand, consider the linear forms y_i of $k(C_n)$ defined by

$$y_i = \begin{cases} \bar{x}_i + \bar{x}_{n-2} + \bar{x}_{n-1} + \bar{x}_n & \text{if } i \equiv 0 \pmod 4, \\ \bar{x}_i - \bar{x}_{n-2} - \bar{x}_{n-1} - \bar{x}_n & \text{if } i \equiv 1 \pmod 4, \\ \bar{x}_i - \bar{x}_{n-2} - \bar{x}_{n-1} + \bar{x}_n & \text{if } i \equiv 2 \pmod 4, \text{ and} \\ \bar{x}_i - \bar{x}_{n-2} + \bar{x}_{n-1} + \bar{x}_n & \text{if } i \equiv 3 \pmod 4. \end{cases}$$

We have found that for all integers $8 \leq n \leq 40$, the ideal $J = (y_i \mid 1 \leq i \leq n-3)$ satisfies $\bar{\mathfrak{m}}^2 \subseteq J$ in $k(C_n)$. Consequently, we have that $\operatorname{ms}(k(C_n)) \leq n-3$ for all integers $8 \leq n \leq 40$.

Even more, the proof of Proposition 4.6.29 does not settle the case of $\operatorname{cs}(k(C_n))$ when n is even. Using the following code in Macaulay2, we have not found an ideal J of $\mathbb{Q}(C_{2n})$ with $\mu(J) = 2n-1$ such that $\bar{\mathfrak{m}}^2 = J^2$, hence we believe that $\operatorname{cs}(k(C_{2n})) = 2n$ if k has characteristic zero.

```
loadPackage "EdgeIdeals";
loadPackage "RandomIdeals";

setRandomSeed(currentTime())

-- Declare the file to which a witness ideal will be written.
file = "csWitnessIdealsC_2n";

-- Declare the largest value of n to test.
n = 20

-- Declare the number of random ideals to test in each iteration.
numRuns = 10000;
```

```
-- Run a loop.
for i from 2 to n do (
  n = 2*i;
  R = QQ[x_1 .. x_n];
  m = ideal(vars R);
  G = cycle R;
  I = edgeIdeal G;
  B = basis(1, R);
  -- Define the witness ideal J.
  L = {};
  for j from 1 to n - 1 do (
    L = append(L, 1));
  for iter from 1 to numRuns do (
    J = randomIdeal(L, B);
    if isSubset(m^2, I + J^2) then {
        file << i << endl;
  };););

file << close;
```

Our next proposition aims for a partial explanation of the difficulty of computing $\mathrm{ms}(k(C_n))$ for n sufficiently large. Before we are able to state it, we must recall the following terminology. Let G be a simple graph on the vertex set $[n] = \{1, 2, \ldots, n\}$. We say that a nonempty set $Q \subseteq [n]$ forms a **clique** in G whenever $\{i, j\}$ is an edge of G for any vertices $i, j \in Q$. Consequently, Q is a clique of G if and only if the induced subgraph of $G[Q]$ is isomorphic to the complete graph $K_{|Q|}$. Likewise, a nonempty set $\mathscr{Q} \subseteq [n]$ is a **coclique** if the vertices of $\mathscr{Q}$ form a clique of $\overline{G}$. Consequently, $\mathscr{Q}$ is a coclique of G if and only if the induced subgraph $\overline{G}[\mathscr{Q}]$ is isomorphic to the complete graph $K_{|\mathscr{Q}|}$ if and only if the induced subgraph $G[\mathscr{Q}]$ is isomorphic to the empty graph $\overline{K_{|\mathscr{Q}|}}$ if and only if $\mathscr{Q}$ is

an independent vertex set of G. Consequently, we have that

$$\alpha(G) = \max\{|\mathscr{Q}| : \mathscr{Q} \text{ is a coclique of } G\} = \max\{|\mathscr{Q}| : \mathscr{Q} \text{ is a clique of } \overline{G}\} = \omega(\overline{G}),$$

where $\omega(G)$ denotes the **clique number** of G. Crucially, any edge of G is trivially a clique.

One other important invariant of the graph G is its **vertex clique cover number**, i.e., the minimum number of cliques in G needed to cover all of the vertices of G

$$\theta(G) = \min\left\{\ell \mid Q_1, \ldots, Q_\ell \text{ are cliques of } G \text{ and } [n] = \bigcup_{i=1}^{\ell} Q_i\right\}.$$

For instance, we have that $\theta(P_n) = \theta(C_n) = \left\lceil \frac{n}{2} \right\rceil$. For if $n = 2\ell$, then a minimum clique covering is achieved by the edges $\{1,2\},\{3,4\},\ldots,\{2\ell-1,2\ell\}$; on the other hand, if $n = 2\ell+1$, then a minimum clique covering is achieved by the edges $\{1,2\},\{3,4\},\ldots,\{2\ell-1,2\ell\},\{2\ell+1\}$.

Definition 4.6.33. Let G be a simple graph with vertices $[n]$ and vertex clique cover $[n] = \bigcup_{i=1}^{\ell} Q_i$. We say that two cliques Q_i and Q_j are **clique-adjacent** if one of the following conditions holds.

(a.) There exist vertices $v \in Q_i$ and $w \in Q_j$ such that $\{v,w\}$ is an edge of G.

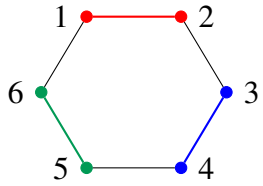
(b.) There exists a vertex $v \in Q_i \cap Q_j$, i.e., the cliques Q_i and Q_j "overlap" at a vertex.

Further, if each pair Q_i and Q_j of cliques are clique-adjacent, we say that $\{Q_i\}_{i=1}^{\ell}$ is K_ℓ-**connected**. We say that G is K_ℓ-connected if it admits a vertex clique cover $\{Q_i\}_{i=1}^{\ell}$ that is K_ℓ-connected.

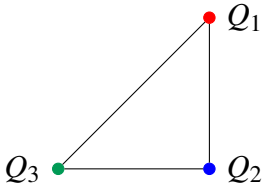
Definition 4.6.34. Let G be a simple graph with vertices $[n]$ and a clique covering $[n] = \bigcup_{i=1}^{\ell} Q_i$. We define the **clique graph** $\mathscr{C}(G,X)$ of G induced by the vertex clique cover $X = \{Q_i\}_{i=1}^{\ell}$ to be the simple graph whose vertices are the cliques $Q_1,\ldots,Q_\ell$ together with the edges $\{Q_i,Q_j\}$ for all integers $1 \leq i < j \leq \ell$ such that Q_i and Q_j are clique-adjacent (as defined in Definition 4.6.33).

Example 4.6.35. Observe that $Q_1 = \{1,2\}$, $Q_2 = \{3,4\}$, and $Q_3 = \{5,6\}$ is a minimum clique covering of the cycle graph C_6. Because the edges $\{2,3\}$, $\{4,5\}$, and $\{1,6\}$ belong to C_6, the clique Q_1 is clique-adjacent to both Q_2 and Q_3, and the clique Q_2 is clique-adjacent to Q_3. Consequently, the clique graph $\mathscr{C}(C_6,X)$ of C_6 induced by the clique covering $X = \{Q_1,Q_2,Q_3\}$ has

vertices Q_1, Q_2, and Q_3 and edges $\{Q_1, Q_2\}, \{Q_1, Q_3\}$, and $\{Q_2, Q_3\}$. Put another way, we have that $\mathscr{C}(C_6, X) \cong K_3$, i.e., C_6 is K_3-connected.



C_6



$\mathscr{C}(C_6, X)$

Crucially, the cycle graph C_n on $n \leq 6$ vertices is $K_{\lceil n/2 \rceil}$-connected; however, for any integer $n \geq 7$, we have that $\mathscr{C}(C_n, X) \cong C_{\lceil n/2 \rceil}$, where X is the clique covering from the paragraph preceding Definition 4.6.33. Because X is a minimum clique covering of C_n, it follows that C_n is not K_ℓ-connected for any integer $\ell \geq 1$.

Every connected graph has a trivial vertex clique covering by all of its edges. We refer to a vertex clique cover of G by edges as an **edge cover** of G. Consequently, the clique cover X of the paragraph preceding Definition 4.6.33 is an edge cover of C_n. Generalizing the idea of the proof of Proposition 4.6.29 yields the following observation.

Proposition 4.6.36. *If a finite simple graph G admits an edge cover $X = \{E_i\}_{i=1}^{\ell}$ such that the edges of X are all clique-adjacent (i.e., X is K_ℓ-connected), then we have that* $\mathrm{ms}(k(G)) \leq \ell$.

Proof. Observe that $\bar{\mathfrak{m}}^2 = (\bar{x}_i^2 \mid 1 \leq i \leq n) + (\bar{x}_e \bar{x}_f \mid \{e, f\} \text{ is not an edge of } G)$. We claim that the ideal $J = \sum_{i=1}^{\ell} (\bar{x}_r + \bar{x}_s \mid E_i = \{r, s\})$ satisfies $J \supseteq \bar{\mathfrak{m}}^2$. By hypothesis that X is an edge cover of G, for each integer $1 \leq i \leq n$, there exists an integer j such that $\{i, j\}$ belongs to X. Consequently, the terms $\bar{x}_i^2 = \bar{x}_i(\bar{x}_i + \bar{x}_j)$ of $\bar{\mathfrak{m}}^2$ belong to $\bar{\mathfrak{m}}J$. We obtain all of the mixed terms $\bar{x}_e \bar{x}_f$ such that $\{e, f\}$ is not an edge of G as follows.

(i.) By hypothesis that the edges of X are clique-adjacent, any two edges $\{e, e'\}$ and $\{f, f'\}$ of X are either connected by an edge $\{e, f'\}$, $\{e', f\}$, or $\{e', f'\}$, or they "overlap" so that $e' = f'$.

(ii.) If $\{e, f'\}$ is an edge, then $\bar{x}_e \bar{x}_f = \bar{x}_e(\bar{x}_f + \bar{x}_{f'})$ belongs to $\bar{\mathfrak{m}}J$; a similar argument shows that $\bar{x}_e \bar{x}_f$ belongs to $\bar{\mathfrak{m}}J$ if $\{e', f\}$ is an edge. If $\{e', f'\}$ is an edge, then $\bar{x}_e \bar{x}_{f'} = \bar{x}_{f'}(\bar{x}_e + \bar{x}_{e'})$ belongs to $\bar{\mathfrak{m}}J$ so that $\bar{x}_e \bar{x}_f = \bar{x}_e(\bar{x}_f + \bar{x}_{f'}) - \bar{x}_e \bar{x}_{f'}$ belongs to $\bar{\mathfrak{m}}J$. If $e' = f'$, then $\bar{x}_e \bar{x}_f = \bar{x}_e(\bar{x}_f + \bar{x}_{e'}) =$

$\bar{x}_e(\bar{x}_f + \bar{x}_{f'})$ belongs to $\bar{\mathfrak{m}}J$. Observe that in any case, we conclude that $\bar{x}_e\bar{x}_f$ belongs to $\bar{\mathfrak{m}}J$ (and so must belong to J).

We conclude that $\bar{\mathfrak{m}}^2 \subseteq \bar{\mathfrak{m}}J \subseteq J$ so that $\operatorname{ms}(k(G)) \leq \mu(J) = \ell$, as desired. □

Remark 4.6.37. Recall that the **diameter** of a finite simple graph is the maximum distance of a shortest path connecting any two vertices. By the proof of Proposition 4.6.36, any finite simple graph satisfying the hypotheses of the proposition must have diameter at most three. Explicitly, the maximum occurs precisely when there exist vertices e and f such that $\{e, f\}$ is not an edge and the edges $\{e, e'\}$ and $\{f, f'\}$ do not overlap.

Observe that in a finite simple graph of diameter two, any two vertices e and f are connected by a path of length at most two, hence either $\{e, f\}$ is an edge or $\{e, e'\}$ and $\{e', f\}$ are distinct edges. Consequently, it is natural to wonder if G has diameter two, then must any $\lceil \frac{n}{2} \rceil$ edges of G constitute an edge cover of G such that the hypotheses of Proposition 4.6.36 hold? For if this were the case, then we would have that $\operatorname{ms}(k(G)) \leq \lceil \frac{n}{2} \rceil$.

Unfortunately, the answer is no. Even more, it is not the case that in a finite simple graph of diameter two, every pair of edges in an edge cover must be clique-adjacent. Consider the Wagner graph M_8 pictured below.

Upon inspection, we find that M_8 has diameter two. Further, the colored edges of both figures give a minimum clique covering (by maximal cliques); however, the pair of red and blue edges in the left-hand graph are not clique-adjacent. On the other hand, if we "amend" the left-hand edge cover to obtain the figure on the right, we have found a minimum clique covering of M_8 (by maximal cliques) that is clique-adjacent.

Crucially, every finite simple graph H is an induced subgraph of a finite simple graph G of diameter two. Explicitly, for any vertex v that is not in $V(H)$, we may define $G = H * K_1$, where K_1

is the complete graph on the vertex v, i.e., it is simply the isolated vertex v (cf. the second paragraph following Corollary 4.6.41 for a definition of the graph operation $*$). Observe that $H \cong G[V(H)]$. Further, by Proposition 4.6.42, we have that $\mathrm{ms}(G) = \mathrm{ms}(H)$, hence it suffices to understand this invariant for finite simple graphs of diameter two.

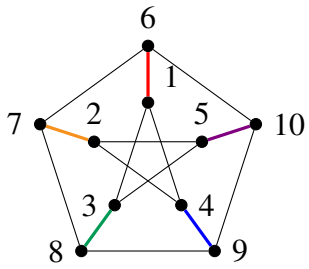
Bearing all of these observations in mind, we ask the following question.

Question 4.6.38. If G is a finite simple graph of diameter two, must it admit an edge cover that is K_ℓ-connected? In particular, can any edge cover of G be "amended" to an edge cover that is K_ℓ-connected?

Often, conjectures in graph theory are given a litmus test against the Petersen graph P, as it is renowned among graph theorists for its consistent ability to produce counterexamples to many expected properties of graphs. Crucially, the Petersen graph is a simple connected graph of diameter two with 10 vertices and 15 edges. Even more, we have that $\alpha(P) = 4$ (cf. [Wes00, p. 1.1.12]). Our next proposition confirms that the Petersen graph does not contradict our findings thus far, hence in particular, Question 4.6.38 remains open.

Proposition 4.6.39. *If P is the Petersen graph, then* $8 \leq \mathrm{cs}(k(P)) \leq 10$ *and* $4 \leq \mathrm{ms}(k(P)) \leq 5$.

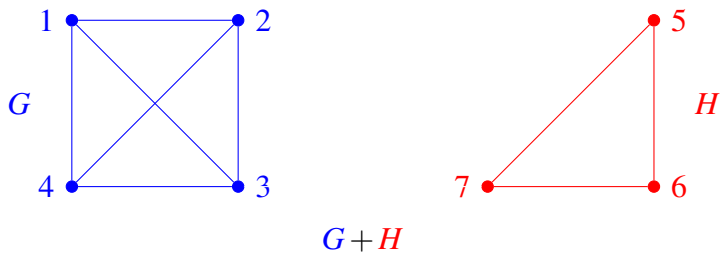
Proof. By the preceding commentary and Remark 4.6.13, we have that $\mathrm{ms}(k(P)) \geq \alpha(P) \geq 4$. Conversely, we may realize the Petersen graph in the plane as a five-cycle connected to a pentagram by some "spokes" (cf. [Gra10]).



One can readily verify that the colored edges pictured above induce a K_5-connected edge cover of P: indeed, the red edge shares a "common edge" with each of the other colored edges, hence it is clique-adjacent to each of the colored edges; the rest are clique-adjacent by symmetry. We

conclude that $4 \leq \mathrm{ms}(P) \leq 5 = \lceil \frac{9}{2} \rceil$. Last, we have that $|E(P)| = 15 < 19$ so that $8 \leq \mathrm{cs}(k(P)) \leq 10$ by Propositions 4.3.3 and 4.5.1 with $s = 1$. □

Consider two finite simple graphs G and H on the disjoint vertex sets $V(G)$ and $V(H)$ with respective edge sets $E(G)$ and $E(H)$. We recall that the **graph union** of G and H is the graph $G+H$ on the vertex set $V(G) \cup V(H)$ and edge set $E(G) \cup E(H)$. We illustrate this below for the blue graph G and the red graph H.



Observe that G and H are both induced subgraphs of $G+H$. Further, there are no edges between G and H in $G+H$, hence every independent vertex set of $G+H$ is the disjoint union of some independent vertex set of G and some independent vertex set of H. Consequently, we obtain the following bounds.

Proposition 4.6.40. *We have that* $\mathrm{ms}(k(G+H)) \geq \max\{\mathrm{ms}(k(G)), \mathrm{ms}(k(H)), \alpha(G)+\alpha(H)\}$ *and* $\mathrm{cs}(k(G+H)) \geq \max\{\mathrm{cs}(k(G)), \mathrm{cs}(k(H))\}$ *for any finite simple graphs* G *and* H.

Proof. By Proposition 4.6.5, Remark 4.6.13, and the exposition preceding the statement of this proposition, we have that $\mathrm{ms}(k(G+H)) \geq k(G)$, $\mathrm{ms}(k(G+H)) \geq k(H)$, and $\mathrm{ms}(k(G+H)) \geq \alpha(G+H) = \alpha(G)+\alpha(H)$, so the lower bound for $\mathrm{ms}(k(G+H))$ holds. Likewise, the lower bound for $\mathrm{cs}(k(G+H))$ holds by Proposition 4.6.5. □

Corollary 4.6.41. *We have that* $\mathrm{ms}(k(K_n + K_1)) = 2$ *for all integers* $n \geq 1$.

Proof. By Proposition 4.6.40, it follows that $\mathrm{ms}(k(K_n+K_1)) \geq \alpha(K_n)+\alpha(K_1) = 2$. Conversely, we have that $\mathrm{ms}(k(K_n+K_1)) \leq 1+\mathrm{ms}(k(K_n)) = 2$ by Propositions 4.6.2 and 4.6.10. □

Generally, the invariants $\operatorname{ms}(k(G+H))$ and $\operatorname{cs}(k(G+H))$ are difficult to understand because there are no relations between the vertices of G and the vertices of H. Explicitly, we have that $k(G+H) \cong k(G) \otimes_k k(H)$ (cf. Question 4.7.1). Even still, the Macaulay2 code provided below is a good starting point to study these rings.

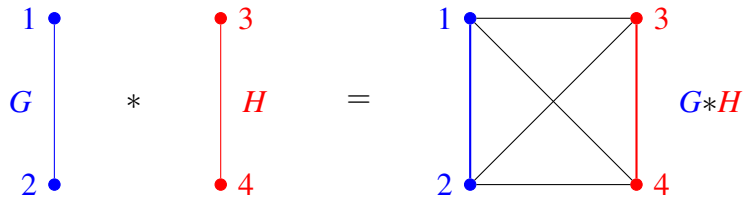
```
-- This script takes a quintuple (int_1, int_2, graph_1, graph_2,
-- numLinearForms) and defines the edge ring of the disjoint union G + H on
-- int_1 + int_2 vertices. It defines also a list L with numLinearForms
-- copies of 1 from which a random ideal K can be created. The inputs
-- graph_1 and graph_2 are graphs from the EdgeIdeals package, e.g., the
-- cycle graph (cycle), the anticycle graph (antiCycle), the complete
-- graph (completeGraph), and the complete multipartite graph
-- (completeMultiPartite).

loadPackage "EdgeIdeals";
loadPackage "RandomIdeals";

setRandomSeed(currentTime())

-- Declare the file to which a witness ideal will be written.
file = "msWitnessIdealsDisjointUnion";

-- Declare the number of variables of the first graph.
int_1 = read "How many vertices does your first graph have? ";
n_1 = value int_1;

-- Establish the polynomial ring for the first graph.
R = QQ[x_1 .. x_(n_1)];
```

```
-- Define the graph G and the edge ideal of G in R.
graph_1 = read "What type of graph would you like to consider? ";
graph_1 = value graph_1;
G = graph_1 R;
I = edgeIdeal G;

-- Declare the number of variables of the second graph.
int_2 = read "How many vertices does your second graph have? ";
n_2 = value int_2;

-- Establish the polynomial ring for the second graph.
S = QQ[x_(n_1 + 1) .. x_(n_1 + n_2)];

-- Define the graph H and the edge ideal of H in S.
graph_2 = read "What type of graph would you like to consider? ";
graph_2 = value graph_2;
H = graph_2 S;
J = edgeIdeal H;

-- Define the ambient polynomial ring and its homogeneous maximal ideal.
T = QQ[x_1 .. x_(n_1 + n_2)];
m = ideal(vars T);

-- Identify I and J as ideals of T.
f_1 = map(T, R);
I = f_1(I);
```

```
f_2 = map(T, S);
J = f_2(J);

-- Specify the generators. The first entry is the minimum degree of a
-- monomial.
B = basis(1, T);

-- Create a list whose length is the total number of possible generators.
-- The integers in the list prescribe how Macaulay2 will randomly choose a
-- monomial of this degree (randomly means that 0 is a possible coefficient,
-- so the 0 polynomial could appear).
numLinearForms = read "How many linear forms would you like to consider? ";
len = value numLinearForms;
L = {};
for i from 1 to len do (
  L = append(L, 1));

-- This begins the loop. First, we generate a random ideal K; then, we test
-- if m^2 is a subset of I + J + K. If it is, then K is written to the file,
-- and a new line is created. The loop ends after numRuns iterations.
numTests = read "How many random ideals would you like to test? ";
numRuns = value numTests;
for iter from 1 to numRuns do (
  K = randomIdeal(L, B);
  if isSubset(m^2, I + J + K) then {
    file << K << endl;
  };);
```

```
file << close;
```

We define the **graph join** $G*H$ of G and H as the graph union $G+H$ together with all edges joining a vertex of G with a vertex of H. For example, the graph join of two paths on $n=2$ vertices is the complete graph K_4.



Observe that $G=(G*H)[V(G)]$ and $H=(G*H)[V(H)]$ are induced subgraphs of $G*H$.

Even more, the complement graph of the graph join $G*H$ is the graph union of the complements of G and H, i.e., we have that $\overline{G*H}=\overline{G}+\overline{H}$. Explicitly, the pair $\{i,j\}$ is an edge of $G*H$ if and only if (a.) $\{i,j\}$ is an edge of G or (b.) $\{i,j\}$ is an edge of H or (c.) $i\in V(G)$ and $j\in V(H)$ or vice-versa, hence $\{i,j\}$ is an edge of $\overline{G*H}$ if and only if $\{i,j\}$ is neither an edge of G nor an edge of H nor an edge connecting some vertex of G to some vertex of H if and only if $\{i,j\}$ is an edge of $\overline{G}$ or $\overline{H}$, i.e., $\{i,j\}$ is an edge of $\overline{G}+\overline{H}$. Consequently, the graph invariants of $G*H$ can be described in terms of those of $\overline{G}+\overline{H}$.

Let m and n be positive integers. Let G and H be simple graphs on the respective vertex sets $V(G)=[m]$ and $V(H)=\{m+1,m+2,\ldots,m+n\}$. We have the edge ideals $I(G)$ and $I(H)$, edge rings $k(G)=k[x_1,\ldots,x_m]/I(G)$ and $k(H)=k[x_{m+1},\ldots,x_{m+n}]/I(H)$, and their respective irrelevant maximal ideals $\mathfrak{m}_G=(x_1,\ldots,x_m)$ and $\mathfrak{m}_H=(x_{m+1},\ldots,x_{m+n})$. By definition of $G*H$, observe that $V(G*H)=V(G)\cup V(H)$ and

$$E(G*H)=E(G)\cup\{\{i,j\}\mid 1\leq i\leq m \text{ and } m+1\leq j\leq n\}\cup E(H).$$

Consequently, the edge ideal of $G*H$ is given by

$$I(G*H)=I(G)+(x_ix_j\mid 1\leq i\leq m \text{ and } m+1\leq j\leq n)+I(H)=I(G)+\mathfrak{m}_G\mathfrak{m}_H+I(H).$$

Using this notation, we make the following observation.

Proposition 4.6.42. *Let G and H be simple graphs on the vertex sets $V(G)$ and $V(H)$ as above. We have that* $\operatorname{ms}(k(G*H)) = \max\{\operatorname{ms}(k(G)), \operatorname{ms}(k(H))\}$ *and*

$$\max\{\operatorname{cs}(k(G)), \operatorname{cs}(k(H))\} \leq \operatorname{cs}(k(G*H)) \leq \operatorname{cs}(k(G)) + \operatorname{cs}(k(H)).$$

Proof. Let $R = k[x_1, \ldots, x_m, x_{m+1}, \ldots, x_n]$. Observe that the edge ideals $I(G)$ and $I(H)$ and the maximal ideals $\mathfrak{m}_G = (x_1, \ldots, x_m)$ and $\mathfrak{m}_H = (x_{m+1}, \ldots, x_n)$ lie in R; they satisfy $I(G) + \mathfrak{m}_G\mathfrak{m}_H + I(H) = (I(G) + \mathfrak{m}_H) \cap (I(H) + \mathfrak{m}_G)$ by [Gel21, Proposition 2.21]. Observe that $k(G) \cong R/(I(G) + \mathfrak{m}_H)$ and $k(H) \cong R/(I(H) + \mathfrak{m}_G)$. We will henceforth identify $k(G)$ and $k(H)$ with their quotients of R. By the analog of [Rot09, Proposition 5.11] in the category of commutative rings, the fiber product of $k(G)$ and $k(H)$ with respect to k is the subring

$$k(G) \times_k k(H) \stackrel{\text{def}}{=} \{(f + I(G) + \mathfrak{m}_H, g + I(H) + \mathfrak{m}_G) \mid f + \mathfrak{m}_G + \mathfrak{m}_H = g + \mathfrak{m}_G + \mathfrak{m}_H\} \subseteq k(G) \times k(H)$$

together with the restriction of the first-coordinate projection map $\pi_1 : k(G) \times_k k(H) \to k(G)$ and the restriction of the second-coordinate projection map $\pi_2 : k(G) \times_k k(H) \to k(H)$. Observe that the triple $(R, \pi_{k(G)}, \pi_{k(H)})$ with the ring homomorphisms defined by $\pi_{k(G)}(f) = f + I(G) + \mathfrak{m}_H$ and $\pi_{k(H)}(f) = f + I(H) + \mathfrak{m}_G$ satisfies the identity $\pi_G \circ \pi_{k(G)} = \pi_H \circ \pi_{k(H)}$ for the canonical surjections $\pi_G : k(G) \to k$ and $\pi_H : k(H) \to k$, hence the analog of [Rot09, Proposition 5.11] in the category of commutative rings yields a unique ring homomorphism $\theta : R \to k(G) \times_k k(H)$ defined by $\theta(f) = (f + I(G) + \mathfrak{m}_H, f + I(H) + \mathfrak{m}_G)$ with $\ker\theta = (I(G) + \mathfrak{m}_H) \cap (I(H) + \mathfrak{m}_G)$. By [Gel21, Proposition 2.1], we find that θ is surjective with $\ker\theta = I(G) + \mathfrak{m}_G\mathfrak{m}_H + I(H) = I(G*H)$, hence it induces a ring isomorphism $\bar{\theta} : k(G*H) \to k(G) \times_k k(H)$ by the First Isomorphism Theorem.

We claim that for any element $(g + I(G) + \mathfrak{m}_H, h + I(H) + \mathfrak{m}_G)$ of the fiber product $k(G) \times_k k(H)$ such that $g, h \in R$ are homogeneous polynomials of same degree, there exists a homogeneous polynomial $f \in R$ such that $\theta(f) = (g + I(G) + \mathfrak{m}_H, h + I(H) + \mathfrak{m}_G)$. Indeed, for any homogeneous polynomials $g, h \in R$ of positive degree, we may write $g = g_{G\setminus H} + g_{H\setminus G} + g_{G\cap H}$ and

$h = h_{G\setminus H} + h_{H\setminus G} + h_{G\cap H}$ for some polynomials $g_{G\setminus H}, h_{G\setminus H} \in \mathfrak{m}_G \setminus \mathfrak{m}_H$, $g_{H\setminus G}, h_{H\setminus G} \in \mathfrak{m}_H \setminus \mathfrak{m}_G$, and $g_{G\cap H}, h_{H\cap G} \in \mathfrak{m}_G \cap \mathfrak{m}_H$. Consequently, the polynomial $f = g_{G\setminus H} + h_{H\setminus G}$ satisfies $\theta(f) = (g + I(G) + \mathfrak{m}_H, h + I(H) + \mathfrak{m}_G)$. Even more, if g and h have the same degree, then f is homogeneous.

Let $a = \max\{\mathrm{ms}(k(G)), \mathrm{ms}(k(H))\}$. By Proposition 4.2.7, there exist homogeneous linear forms $s_1, \ldots, s_a$ in the variables $x_1, \ldots, x_m$ whose images in $k(G)$ satisfy $\mathfrak{m}_G^2 = (s_1, \ldots, s_a)\mathfrak{m}_G$. Likewise, there exist homogeneous linear forms $t_1, \ldots, t_a$ in the variables $x_{m+1}, \ldots, x_{m+n}$ whose images in $k(H)$ satisfy $\mathfrak{m}_H^2 = (t_1, \ldots, t_a)\mathfrak{m}_H$. By the surjectivity of θ, there exist polynomials $f_i \in R$ such that $\theta(f_i) = (s_i + I(G) + \mathfrak{m}_H, t_i + I(H) + \mathfrak{m}_G)$ for each integer $1 \leq i \leq a$. Crucially, the elements s_i and t_i are homogeneous linear forms, so we may assume that the polynomials f_i are homogeneous by the construction of the previous paragraph. By the proof of Proposition 4.3.14, we have that $\mathfrak{m}^2_{k(G)\times_k k(H)} \subseteq ((s_1, t_1), \ldots, (s_a, t_a))$. Going modulo $I(G*H) = I(G) + \mathfrak{m}_G\mathfrak{m}_H + I(H)$, we find that $\mathfrak{m}^2_{k(G*H)} \subseteq (\bar{f}_1, \ldots, \bar{f}_a)$. Because the polynomials f_i are homogeneous, we conclude that $\mathrm{ms}(k(G*H)) \leq a$. Last, $\mathrm{ms}(k(G*H)) \geq a$ holds by Proposition 4.2.10 since there are surjections $k(G*H) \to k(G)$ and $k(G*H) \to k(H)$.

Likewise, the $\mathrm{cs}(k(G*H))$ bounds follow by the proof of Proposition 4.3.14 and the second paragraph here. □

Combining Propositions 4.6.19 and 4.6.42 yields two immediate corollaries.

Corollary 4.6.43. *Let G and H be graphs on disjoint vertex sets $V(G)$ and $V(H)$ such that $\overline{G}$ and $\overline{H}$ are chordal. If k is an infinite field, then* $\mathrm{ms}(k(G*H)) = \max\{\alpha(G), \alpha(H)\}$.

Corollary 4.6.44. *Let m and n be positive integers. Let G be the graph obtained from the complete graph K_m by removing $1 \leq i \leq \left\lfloor \frac{m}{2} \right\rfloor$ non-adjacent edges. Let H be the graph obtained from K_n by removing $1 \leq j \leq \left\lfloor \frac{n}{2} \right\rfloor$ non-adjacent edges. If k is infinite, then* $\mathrm{ms}(k(G*H)) = 2$.

Proof. Observe that $\overline{G}$ consists of $m - 2i$ isolated vertices and i non-adjacent edges. Likewise, $\overline{H}$ consists of $n - 2j$ isolated vertices and j non-adjacent edges. Consequently, $\overline{G}$ and $\overline{H}$ are chordal so that $\mathrm{ms}(k(G*H)) = \max\{\alpha(G), \alpha(H)\} = 2$ by Proposition 4.6.23 and Corollary 4.6.43. □

For any positive integers $n_1, \ldots, n_t$, the graph $K_{n_1,n_2,\ldots,n_t} = \overline{K_{n_1}} * \overline{K_{n_2}} * \cdots * \overline{K_{n_t}}$ is called the **complete t-partite graph** on $n_1, \ldots, n_t$. Considering that $k(\overline{K}_n) = k[x_1, \ldots, x_n]$ is regular, it follows by Proposition 4.3.3 that $\operatorname{ms}(k(\overline{K}_n)) = n$, hence we obtain the following.

Corollary 4.6.45. *We have that* $\operatorname{ms}(K_{n_1,n_2,\ldots,n_t}) = \max\{n_1, n_2, \ldots, n_t\}$.

Proof. Observe that $\operatorname{ms}(k(K_{n_1,\ldots,n_t})) = \max\{\operatorname{ms}(k(\overline{K_{n_1}})), \ldots, \operatorname{ms}(k(\overline{K_{n_t}}))\}$ by Proposition 4.6.42. By the observation preceding the statement of the corollary, the latter value is $\max\{n_1, \ldots, n_t\}$. □

Given a finite simple graph G on n vertices, one naturally wonders if $\operatorname{ms}(k(G)) + \operatorname{ms}(k(\overline{G})) = n$. Our next proposition illustrates that this is not the case.

Proposition 4.6.46. *We have that* $\operatorname{ms}(k(S_n)) + \operatorname{ms}(k(\overline{S_n})) = n + 1$.

Proof. Observe that $S_n = \overline{K_{n-1}} * K_1$, hence $\overline{S_n} = K_{n-1} + K_1$ so that $\operatorname{ms}(k(\overline{S_n})) = 2$ by Corollary 4.6.41. We conclude the result, as $\operatorname{ms}(k(S_n)) = n - 1$ by Proposition 4.6.24. □

We provide bounds on our invariants for the wheel graph on $n \geq 4$ vertices. We will see that in turn, the following proposition yields a slightly improved upper bound on the cycle graph.

Proposition 4.6.47. *Let W_n be the wheel graph on $n \geq 4$ vertices, i.e., the graph join of the complete graph K_1 and the cycle graph C_{n-1}. The following inequalities hold.*

$$n - 2 \leq \operatorname{cs}(k(W_n)) \leq \begin{cases} n-1 & \text{if } n \text{ is even and} \\ n & \text{if } n \text{ is odd} \end{cases}$$

$$\left\lfloor \frac{n-1}{2} \right\rfloor \leq \operatorname{ms}(k(W_n)) \leq \begin{cases} \left\lceil \frac{n-1}{2} \right\rceil & \text{if } n \leq 7 \text{ and} \\ n-3 & \text{if } n \geq 8. \end{cases}$$

If $n = 4, 5$, or 7, then $\operatorname{ms}(k(W_n))$ achieves its lower bound.

Proof. Observe that $W_n = K_1 * C_{n-1}$, hence Proposition 4.6.42 implies that

$$\max\{\mathrm{cs}(k(K_1)), \mathrm{cs}(k(C_{n-1}))\} \leq \mathrm{cs}(k(W_n)) \leq \mathrm{cs}(k(K_1)) + \mathrm{cs}(k(C_{n-1})) = \mathrm{cs}(k(C_{n-1})) + 1$$

and $\mathrm{ms}(k(W_n)) = \max\{\mathrm{ms}(k(K_1)), \mathrm{ms}(k(C_{n-1}))\} = \mathrm{ms}(k(C_{n-1}))$. By Proposition 4.6.29, the stated lower bounds for $\mathrm{cs}(k(W_n))$ and $\mathrm{ms}(k(W_n))$ hold. If n is even, then $n-1$ is odd so that $\mathrm{cs}(C_{n-1}) = n-2$; otherwise, we have that $\mathrm{cs}(k(C_{n-1})) \leq n-1$, hence the upper bound for $\mathrm{cs}(k(W_n))$ holds. Likewise, if $n \leq 7$, then the upper bound for $\mathrm{ms}(k(W_n))$ holds by Proposition 4.6.29. Last, we have that $\mathrm{ms}(k(W_4)) = \mathrm{ms}(k(C_3)) = 1$; $\mathrm{ms}(k(W_5)) = \mathrm{ms}(k(C_4)) = 2$; and $\mathrm{ms}(k(W_7)) = \mathrm{ms}(k(C_6)) = 3$ by Proposition 4.6.29.

For $n \geq 8$, we construct an edge cover $\{E_i\}_{i=1}^{n-3}$ that is K_{n-3}-connected. First, we cover two clique-adjacent "perimeter" edges of W_n; then, we cover the remaining $n-5$ "perimeter" vertices and the "hub" with the $n-5$ edges connecting the "hub" to each of these "perimeter" vertices. Ultimately, we obtain an edge cover with $n-3 = 2+(n-5)$ edges. It is K_{n-3}-connected because the two "perimeter" edges are clique-adjacent, and both of these edges are clique-adjacent to an edge connecting the "hub" and a "perimeter" vertex because the "hub" is adjacent to all "perimeter" vertices. By Proposition 4.6.36, we conclude that $\mathrm{ms}(k(W_n)) \leq n-3$. □

Corollary 4.6.48. *We have that* $\mathrm{ms}(k(C_n)) \leq n-2$ *for all integers* $n \geq 8$.

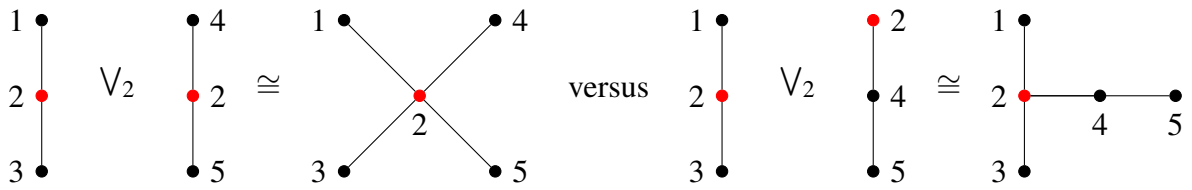
Proof. By Proposition 4.6.47, we have that $\mathrm{ms}(k(C_n)) = \mathrm{ms}(k(W_{n+1})) \leq n-2$ for all $n \geq 8$. □

We conclude with a discussion of another familiar graphical construction.

Definition 4.6.49. Consider any finite simple graphs G and H with respective vertex sets $V(G)$ and $V(H)$ such that $V(G) \cap V(H) = \{v\}$ and respective edge sets $E(G)$ and $E(H)$. We define the **wedge graph** $G \vee_v H$ with respect to v as the graph with vertices $V(G) \cup V(H)$ and edges $E(G) \cup E(H)$. Put another way, $G \vee_v H$ is obtained by "gluing" G and H together at their common vertex v.

Generally, the vertex v determines the corresponding wedge graph $G \vee_v H$. Explicitly, for any labelling of the vertices of G, the wedge graph $G \vee_v H$ depends upon the labeling of the vertices of

H. Below is a diagram of two non-isomorphic graphs that are obtained by wedging two copies of P_3 with different labelings.



On the other hand, for the complete graph K_n, the wedge vertex is irrelevant, as every labeling of the vertices of K_n induces a graph automorphism of K_n. Because the diameter of K_n is one, the wedge graphs $K_m \vee K_n$ form a family of graphs of diameter two. By the discussion of Remark 4.6.37, graphs of diameter two are of particular interest because they are highly connected yet ostensibly exhibit subtle behavior with respect to the invariants.

Our first result on the wedge of complete graphs gives non-trivial bounds on $\operatorname{ms}(K_m \vee K_n)$.

Proposition 4.6.50. *We have that* $2 \leq \operatorname{ms}(k(K_m \vee K_n)) \leq \min\{m,n\}$.

Proof. We will assume that $m < n$ so that $\min\{m,n\} = m$ and $\max\{m,n\} = n$. Further, we will assume that K_m is the complete graph on the vertices $[m] = \{1,2,\ldots,m\}$ and K_n is the complete graph on the vertices $\{m, m+1, \ldots, m+n-1\}$. By definition, the graph $K_m \vee K_n$ is obtained by gluing K_m and K_n along the common vertex m of K_m and K_n, hence we have that

$$I(K_m \vee K_n) = (x_i x_j \mid 1 \leq i < j \leq m \text{ or } m \leq i < j \leq m+n-1) \text{ and}$$
$$\bar{\mathfrak{m}}^2 = (\bar{x}_i^2 \mid 1 \leq i \leq m+n-1) + (\bar{x}_i \bar{x}_j \mid 1 \leq i \leq m-1 \text{ and } m+1 \leq j \leq m+n-1).$$

Consider the ideal $J = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{m-1}, \bar{x}_m + \bar{x}_{m+1} + \cdots + \bar{x}_{m+n-1})$. We obtain the pure squares $\bar{x}_i^2$ for each integer $m \leq i \leq m+n-1$ by taking $\bar{x}_i(\bar{x}_m + \bar{x}_{m+1} + \cdots + \bar{x}_{m+n-1})$, and the remaining pure squares $\bar{x}_i^2$ for each integer $1 \leq i \leq m-1$ are clearly contained in $\bar{\mathfrak{m}}J$. We obtain the mixed terms $\bar{x}_i \bar{x}_j$ such that $1 \leq i \leq m-1$ and $m+1 \leq j \leq m+n-1$ in the following manner.

(i.) Observe that $\bar{x}_i(\bar{x}_m + \bar{x}_{m+1} + \cdots + \bar{x}_{m+n-1})$ contains $\bar{x}_i \bar{x}_j$ as a summand.

(ii.) Given any integer $\ell \in \{m, m+1, \ldots, m+n-1\} \setminus \{j\}$, observe that the monomial $\bar{x}_i\bar{x}_\ell$ is an element of $\bar{\mathfrak{m}}J$ by hypothesis that $1 \leq i \leq m-1$.

(iii.) Consequently, we have that $\bar{x}_i\bar{x}_j = \bar{x}_i(\bar{x}_m + \bar{x}_{m+1} + \bar{x}_{m+n-1}) - \sum_{\ell \in S} \bar{x}_i\bar{x}_\ell$ is an element of $\bar{\mathfrak{m}}J$, where S is the set $\{m, m+1, \ldots, m+n-1\} \setminus \{j\}$.

We conclude that $\operatorname{ms}(k(K_m \vee K_n)) \leq \min\{m, n\}$. On the other hand, we have that $\alpha(K_m \vee K_n) = 2$ so that $\operatorname{ms}(k(K_m \vee K_n)) \geq 2$. Every vertex $1 \leq i \leq m-1$ is incident to all vertices $1 \leq i < j \leq m$, hence the set $\{i, j\}$ with $m+1 \leq j \leq m+n-1$ is a maximum independent vertex set. □

Remark 4.6.51. We note that the proof of Proposition 4.6.50 comes from the following observation. Let G be a simple graph on n vertices. Relabelling G, if necessary, if the vertices $\{1, 2, \ldots, m\}$ form an independent vertex set in $\overline{G}$ and the induced subgraph on $\{m+1, m+2, \ldots, n\}$ is connected in $\overline{G}$, then the ideal $\bar{\mathfrak{m}}^2$ of $k(G)$ is contained in $J = (\bar{x}_1 + \cdots + \bar{x}_m, \bar{x}_{m+1}, \ldots, \bar{x}_n)$. Indeed, if the vertices $\{1, 2, \ldots, m\}$ are independent in $\overline{G}$, then the graph G must contain all the edges $\{i, j\}$ such that $1 \leq i < j \leq i$. Consequently, the pure squares $\bar{x}_i^2$ such that $1 \leq i \leq m+1$ belong to the ideal $\bar{\mathfrak{m}}J$, as they can be written as $\bar{x}_i^2 = \bar{x}_i(\bar{x}_1 + \cdots + \bar{x}_m)$. Clearly, the pure squares $\bar{x}_{m+1}^2, \ldots, \bar{x}_n^2$ all belong to $\bar{\mathfrak{m}}J$. Further, the mixed terms $\bar{x}_i\bar{x}_j$ such that $m+1 \leq i < j \leq n$ belong to the ideal $\bar{\mathfrak{m}}J$, as the monomials $\bar{x}_{m+1}, \ldots, \bar{x}_n$ all belong to J by construction.

Corollary 4.6.52. *Let T_n be the kite graph on $n \geq 5$ vertices, i.e., the wedge graph of the complete graphs K_{n-2} and K_2. We have that* $\operatorname{ms}(k(T_n)) = 2$.

Remark 4.6.53. The kite graph of Corollary 4.6.52 is also called the **lollipop graph** $L_{n-2,1}$.

Our next goal is to extend Corollary 4.6.52 to the wedge graph of K_m and n copies of K_2.

Definition 4.6.54. Let m and n be positive integers. We define the **jellyfish graph** $J_{m,n}$ with body of size m and n tentacles as the simple graph $J_{m,n} = K_m \vee (\vee_{i=1}^n K_2)$ on $m+n$ vertices with an edge $\{i, j\}$ whenever $1 \leq i < j \leq m$ or $i = 1$ and $m+1 \leq j \leq m+n$.

Proposition 4.6.55. *Let m and n be positive integers. We have that $\overline{J_{m,n}} \cong (\overline{K_{m-1}} * K_n) + K_1$. Particularly, the complement graph $\overline{J_{m,n}}$ is chordal with $\omega(\overline{J_{m,n}}) = n+1$.*

Proof. Observe that $\{i, j\}$ is an edge of $\overline{J_{m,n}}$ if and only if $2 \leq i \leq m$ and $m+1 \leq j \leq m+n$ or $m+1 \leq i < j \leq m+n$. Consequently, the vertex $i = 1$ of $\overline{J_{m,n}}$ forms a copy of K_1; the vertices $2 \leq i \leq m$ of $\overline{J_{m,n}}$ form a copy of $\overline{K_{m-1}}$; the vertices $m+1 \leq i \leq m+n$ of $\overline{J_{m,n}}$ form a clique K_n; and each vertex of $\overline{K_{m-1}}$ is adjacent to a vertex of K_n. We conclude that $\overline{J_{m,n}} \cong (\overline{K_{m-1}} * K_n) + K_1$. Considering that this is a union of chordal graphs, it follows that $\overline{J_{m,n}}$ is chordal. Further, observe that $\omega(\overline{J_{m,n}}) = \omega(\overline{K_{m-1}} * K_n) = \alpha(K_{m-1} + \overline{K_n}) = n+1$. □

Proposition 4.6.56. *Let m and n be positive integers. We have that* $\operatorname{ms}(J_{m,n}) = n+1$.

Proof. By Proposition 4.6.55, we have that $\overline{J_{m,n}}$ is chordal with $\omega(\overline{J_{m,n}}) = n+1$. Consequently, it follows that $\operatorname{ms}(J_{m,n}) = \alpha(J_{m,n}) = \omega(\overline{J_{m,n}}) = n+1$ by Proposition 4.6.19. □

4.7 Further Directions

One lingering question concerns the tensor product of standard graded algebras over a field k. Consider the k-algebras $R = k[x_1, \ldots, x_m]/I$ for some homogeneous quadratic ideal I of $k[x_1, \ldots, x_m]$ and $S = k[y_1, \ldots, y_n]/J$ for some homogeneous quadratic ideal J of $k[y_1, \ldots, y_n]$. Observe that $I + J$ is an ideal of $k[x_1, \ldots, x_m, y_1, \ldots y_n]$ and

$$R \otimes_k S \cong \frac{k[x_1, \ldots, x_m, y_1, \ldots, y_n]}{I+J}.$$

We note that the quadratic squarefree monomials $\bar{x}_i \bar{y}_j$ of $R \otimes_k S$ do not vanish.

Question 4.7.1. Let R and S be defined as above. What are $\operatorname{ms}(R \otimes_k S)$ and $\operatorname{cs}(R \otimes_k S)$?

Earlier, in Section 4.6, we saw that even if I and J are quadratic squarefree monomial ideals, the above question is quite subtle. We provided some Macaulay2 code toward verifying this observation in the paragraph after Corollary 4.6.41.

One other interesting graphical invariant related to Section 4.6 can be defined as follows. Let $\mathbf{X} = (X_1, \ldots, X_m)$ be an m-dimensional random vector with multivariate normal (or Gaussian) distribution $X \sim \mathcal{N}_m(\boldsymbol{\mu}, \boldsymbol{\Sigma})$, where $\boldsymbol{\Sigma}$ is an $m \times m$ positive-semidefinite matrix known as the *covariance*

matrix. Consider the finite simple graph G on the vertices $[m]$ with an edge $\{i,j\}$ if and only if the random variables X_i and X_j are conditionally dependent given all of the other random variables (cf. [Uhl17, Corollary 2.2]). By the paragraph following [GS18, Problem 1.2], we may define the *maximum likelihood threshold* $\operatorname{mlt}(G) = \min\{\#\text{i.i.d. samples} \mid \mathbf{\Sigma} \text{ exists with probability one}\}$.

Proposition 4.7.2. *Let G be the finite simple graph corresponding to an m-dimensional Gaussian random vector. Let $I(G)$ be the edge ideal in $\mathbb{R}[x_1,\ldots,x_m]$. We have that $\operatorname{ms}(\mathbb{R}(G)) = \operatorname{mlt}(\overline{G})$ if*

(1.) *$\overline{G}$ is chordal;*

(2.) *$\overline{G}$ is complete;*

(3.) *G is complete; or*

(4.) *$\overline{G}$ has no induced cycles (i.e., $\overline{G}$ is a tree).*

Proof. By [GS18, Proposition 1.3] and Proposition 4.6.19, if $\overline{G}$ is chordal, then $\operatorname{mlt}(\overline{G}) = \omega(\overline{G}) = \alpha(G) = \operatorname{ms}(\mathbb{R}(G))$. If $\overline{G}$ is complete, then G has no edges, hence $\mathbb{R}(G) = \mathbb{R}[x_1,\ldots,x_m]$ is a regular standard graded local ring, from which it follows that $\operatorname{ms}(\mathbb{R}(G)) = m$ by Propositions 4.2.18 and 4.3.3. Conversely, if G is complete, then $\operatorname{ms}(\mathbb{R}(G)) = 1$ by Proposition 4.6.2. Last, if $\overline{G}$ has no cycles, then $\operatorname{ms}(\mathbb{R}(G)) = 2$ by Corollary 4.6.20. By the paragraph preceding [GS18, Proposition 1.3], we have that $\operatorname{ms}(\mathbb{R}(G)) = \operatorname{mlt}(\overline{G})$ in each of these cases. □

Question 4.7.3. Let G be the finite simple graph corresponding to an m-dimensional Gaussian random vector. Let $I(G)$ be the edge ideal in $\mathbb{R}[x_1,\ldots,x_m]$. Does it hold that $\operatorname{ms}(\mathbb{R}(G)) = \operatorname{mlt}(\overline{G})$?

Acknowledgements

We express our gratitude to Hailong Dao for suggesting this problem to us and for many productive conversations regarding this work. We appreciate the useful comments of Grigoriy Blekherman toward a possible connection with the maximum likelihood threshold of a graph. We thank the creators of the Macaulay2 computer algebra software and especially those who contributed to the `EdgeIdeals` and `RandomIdeals` packages.

Chapter 5

On a Generalization of Two-Dimensional Veronese Subrings

Abstract

If a is a positive integer and k is a field, then the ath Veronese subring of the two-dimensional polynomial ring $k[x,y]$ is the monomial subring $k[x,y]^{(a)} = k[x^i y^{a-i} \mid 1 \leq i \leq a]$. We demonstrate that for any nonempty subset $A \subseteq [a] = \{0,1,\ldots,a\}$, the properties of the monomial subring $k[x,y]^{(A)}$ are intimately intertwined with the properties of the r-fold sumsets of A.

5.1 Introduction

We say that a nonempty subset S of non-negative integers is **Sidon** if for every pair of non-negative integers $i \leq j$, the sum $s_i + s_j$ of the elements $s_i, s_j \in S$ is unique. Put another way, there do not exist distinct pairs of integers $i \leq j$ and $i' \leq j'$ such that $s_i + s_j = s_{i'} + s_{j'}$ for some elements $s_i, s_j, s_{i'}, s_{j'} \in S$. Originally introduced by Simon Sidon in his study of Fourier series, Sidon sets culled significant interest in the field of additive number theory after a result of Erdös and Turán showed that for every real number $x > 0$, the number of elements of a Sidon set that do not exceed x is at most $\sqrt[4]{x} + O(\sqrt[4]{x})$ (cf. [ET41]). Even now, it remains an open problem to determine the maximum number of elements not exceeding a given real number $x > 0$ that a Sidon set can contain.

Essentially, the question of Sidon is to determine how "dense" a Sidon set can be if its largest element does not exceed some real number $x > 0$. Conversely, given a positive integer a, one can ask the question of how "sparse" a set can be such that the n-fold sum of its elements achieves a maximum value of a. Colloquially, this question is known as the **Postage Stamp Problem**, as it can be interpreted accordingly: let n and t be positive integers. Given that an envelope affords

enough space for n stamps and there are t distinct denominations of stamps available to us, what is the maximum cost of postage a such that any letter of cost $0, 1, \ldots, a$ can be mailed?

Let X be a nonempty subset of non-negative integers. We define the n-fold sum of X as

$$nX = \underbrace{X + \cdots + X}_{n \text{ summands}} = \{x_1 + \cdots + x_n \mid x_1, \ldots, x_n \in X\},$$

and we denote $[a] = \{0, 1, \ldots, a\}$. Considered among the first to state the Postage Stamp Problem, Rohrbach defined the invariants $a(n,X) = \max\{a : [a] \subseteq nX\}$ and $a(n,t) = \max\{a(n,X) : |X| = t\}$ in his seminal 1937 paper (cf. [Roh37]). Even though it is relatively simple to state, it has been shown that the computational complexity of the Postage Stamp Problem is exponential in both n and t, and there remain many open questions that relate to $a(n,t)$ (cf. [AB80]).

Consider a nonempty set $A \subseteq [a]$. We say that A is a **complete double** of $[a]$ if $2A = [2a]$ (cf. [Dao19]). Clearly, the set $[a]$ is a complete double of itself, hence one might naturally seek the least cardinality of A such that it is a complete double of $[a]$, i.e., $\mu(a) = \min\{|A| : 2A = [2a]\}$. Based on a MathOverflow discussion in [Dao19], we establish preliminary bounds for $\mu(a)$ in Proposition 5.2.6 — all though, the discussion of Remark 5.2.8 illustrates that the current bound is not sharp.

Generalizing the notion of a complete double of $[a]$, we define the **regularity** of a set $A \subseteq [a]$ as $\operatorname{reg}(A) = \inf\{r \mid rA = [ra]\}$. One can readily verify that A is a complete double of $[a]$ if $\operatorname{reg}(A) = 2$. We prove that $\operatorname{reg}(A)$ is finite only if $\{0, 1, a-1, a\}$ is a subset of A in Proposition 5.2.2; then, we demonstrate that this necessary condition is in fact sufficient by Propositions 5.2.14 and 5.2.15. Combined, these three propositions imply that if $\operatorname{reg}(A)$ is finite, then $\operatorname{reg}(A) \leq a - 2$.

Given any set $A \subseteq [a]$ that contains 0 and a and any field k, we define the monomial subring $k[x,y]^{(A)} = k[x^i y^{a-i} \mid i \in A] \subseteq k[x,y]$; we refer to $k[x,y]^{(A)}$ as the ath **pseudo-Veronese** subring of $k[x,y]$. We establish in Proposition 5.3.4 that if A contains 1 and $a-1$, then the Hilbert-Samuel multiplicity of $k[x,y]^{(A)}$ is simply a. Under these same conditions, Proposition 5.3.5 illustrates moreover that the homogeneous maximal ideal $\mathfrak{m} = (x^i y^{a-i} \mid i \in A)$ of $k[x,y]^{(A)}$ and the homogeneous maximal ideal $\mathfrak{a} = (x^i y^{a-i} \mid 0 \leq i \leq a)$ of $k[x,y]^{(a)}$ possess the same radical. We demonstrate

in Proposition 5.3.9 that $k[x,y]^{(A)}$ is Cohen-Macaulay if and only if $A = [a]$. Last, we conclude the third section by establishing that the Castelnuovo-Mumford regularity of $k[x,y]^{(A)}$ and the regularity of A coincide (cf. Proposition 5.3.12), hence there is no coincidence in this naming convention.

5.2 Complete Doubles and the Regularity of a Set

We will henceforth assume that a is a positive integer, and we denote by $[a] = \{0, 1, \ldots, a\}$ the set of non-negative integers that do not exceed a. Given a nonempty subset X of non-negative integers (or more generally, any nonempty subset of a nonempty semigroup), the set of sums of pairs of elements of X is written $X + X = \{x + y \mid x, y \in X\}$. We will henceforth adopt the shorthand

$$nX = \underbrace{X + \cdots + X}_{n \text{ summands}} = \{x_1 + \cdots + x_n \mid x_1, \ldots, x_n \in X\}.$$

Using this convention, it is straightforward to verify that

$$n[a] = \{a_1 + \cdots + a_n \mid 0 \leq a_1, \ldots, a_n \leq a\} = [na].$$

Further, for any nonempty set $Y \subseteq X$, we have that $nY \subseteq nX$ for all integers $n \geq 1$. Often, we will write $\#X$ to denote the cardinality of X. For instance, we have that $\#[a] = a + 1$.

Definition 5.2.1. We say that a nonempty set $A \subseteq [a]$ is a **complete double** of $[a]$ if $2A = [2a]$.

We note that the terminology "complete double" was introduced by Hailong Dao in [Dao19]. Our first result gives a necessary condition for a set $A \subseteq [a]$ to be a complete double of $[a]$.

Proposition 5.2.2. *We have that $rA = [ra]$ for some integer $r \geq 1$ only if $A \supseteq \{0, 1, a-1, a\}$. Put another way, if $\{0, 1, a-1, a\}$ is not contained in A, then A is not a complete double of $[a]$.*

Proof. Certainly, if $0 \notin A$ or $a \notin A$, then $0 \notin rA$ and $ra \notin rA$ for any integer $r \geq 1$ because 0 is uniquely represented in rA as the r-fold sum $0 = 0 + \cdots + 0$ and similarly for ra. On the other hand, if $0 \in A$ but $1 \notin A$, then $1 \notin rA$ for any integer $r \geq 1$ because 1 is uniquely represented in

rA as the sum of 1 and $r-1$ copies of 0. Last, assume that $0,1,a \in A$ but that $a-1 \notin A$. Let $m = \max\{x \in A \mid x < a-1\}$. Observe that for any integer $r \geq 1$, the largest element of $rA \setminus \{ra\}$ is $(r-1)a+m = ra-a+m < ra-1$. We conclude that $ra-1 \notin rA$ for any integer $r \geq 1$. □

Consequently, Proposition 5.2.2 gives a necessary condition for a nonempty set $A \subseteq [a]$ to be a complete double of $[a]$. Before we establish a sufficient condition, we need two technical lemmas.

Lemma 5.2.3. *Given any integers $1 \leq d \leq a-1$, we have that*

$$\left\lfloor \frac{a-d}{d} \right\rfloor d = a-r-d,$$

where r denotes the least non-negative residue of a modulo d.

Proof. Observe that if $a-d < d$, then $\left\lfloor \frac{a-d}{d} \right\rfloor = 0$ and $r = a-d$ so that $a-r-d = 0$, and the claim holds. Consequently, we may assume that $a-d \geq d$. By the Division Algorithm, we may write $a = qd+r$ for some integer $q \geq 1$ and some integer $0 \leq r \leq d-1$. Consequently, we find that

$$\left\lfloor \frac{a-d}{d} \right\rfloor d = \left\lfloor \frac{(q-1)d+r}{d} \right\rfloor d = \left\lfloor q-1+\frac{r}{d} \right\rfloor d = (q-1)d = qd-d = a-r-d. \qquad \square$$

We gratefully acknowledge Gerry Myerson for his suggestion of the following lemma.

Lemma 5.2.4. *Given any integers $a \geq 1$ and $1 \leq d \leq a$, the set*

$$C(a,d) = \{0,1,\ldots,d,a-d,a-d+1,\ldots,a\} \cup \{td \mid t \geq 1 \text{ is an integer and } d \leq td \leq a-d\}$$

satisfies $2C(a,d) = [2a]$. Put another way, $C(a,d)$ is a complete double of $[a]$.

Proof. Let r be the least non-negative residue of a modulo d. By Lemma 5.2.3, we have that

$$\max\{td \mid t \geq 1 \text{ is an integer and } d \leq t \leq n-d\} = n-r-d.$$

Considering that $td+i$ belongs to $C(a,d)+C(a,d)$ each pair of integers $0 \leq i \leq d$ and $t \geq 0$ such that $0 \leq td \leq n-d$, the integers $0,1,\ldots,n-r$ belong to $C(a,d)+C(a,d)$. By hypothesis that

$C(a,d)$ contains $n-d, n-d+1, \ldots, n$, we conclude that $0, 1, \ldots, n$ belong to $C(a,d)+C(a,d)$. Further, $td+(n-d+i)$ belongs to $C(a,d)+C(a,d)$ for each pair of integers $0 \leq i \leq d$ and $t \geq 1$ such that $d \leq td \leq n-d$, hence $n+1, n+2, \ldots, 2n-d-r$ belong to $C(a,d)+C(a,d)$. Clearly, the integers $2n-2d, 2n-2d+1, \ldots, 2n$ belong to $C(a,d)+C(a,d)$, hence the claim holds. □

Proposition 5.2.5. *If A contains $C(a,d)$ for some integer $1 \leq d \leq a$, then $2A = [2a]$.*

Proof. By Lemma 5.2.4, we have that $[2a] = 2C(a,d) \subseteq 2A \subseteq [2a]$. □

Consequently, Proposition 5.2.5 illustrates that any set containing $C(a,d)$ for some integer $1 \leq d \leq a$ must be a complete double of $[a]$. Our next task is to determine (bounds for) the minimum size of a complete double of $[a]$, i.e., $\mu(a) = \min\{\#A \mid A \text{ is a complete double of } [a]\}$.

Proposition 5.2.6. *We have that* $\dfrac{\sqrt{16a+9}-1}{2} \leq \mu(a) \leq 2\sqrt{2a}+1$.

Proof. By Lemma 5.2.4, for any integers $a \geq 1$ and $1 \leq d \leq a$, the set

$$C(a,d) = \{0, 1, \ldots, d, a-d, a-d+1, \ldots, a\} \cup \{td \mid t \geq 1 \text{ is an integer and } d \leq td \leq a-d\}$$

satisfies $2C(a,d) = [2a]$. One can verify that $\#C(a,d) = 2(d+1) + \lfloor \frac{a-d}{d} \rfloor = 2d + \lfloor \frac{a}{d} \rfloor + 1$. Consequently, we have that $\#C(a,d) \leq 2d + \frac{a}{d} + 1 = f_a(d)$ for all integers $d \geq 1$. Using elementary calculus, we find that $f_a(x)$ is minimized when $x = \sqrt{\frac{a}{2}}$ with a minimum value of $2\sqrt{2a}+1$, from which it follows that $\#C(a,d) \leq 2\sqrt{2a}+1$. We conclude that $\mu(a) \leq \#C(a,d) \leq 2\sqrt{2a}+1$.

Conversely, if A is a complete double of $[a]$, then for each integer $0 \leq n \leq 2a$, there exists a pair (x,y) in $A \times A$ such that $n = x+y$. Consequently, we have that $2a+1 = \#[2a] = \binom{\#A+1}{2}$ or $(\#A)^2 + \#A - 2(2a+1) = 0$. Ultimately, the lower bound holds by the Quadratic Formula. □

Corollary 5.2.7. *Given any integer $a \geq 2$, the set $C^*(a,d)$ with $d = \left\lfloor \sqrt{\frac{a}{2}} \right\rfloor$ is a complete double of a whose cardinality is strictly less than the upper bound found in Proposition 5.2.6.*

Remark 5.2.8. For all integers $2 \leq a \leq 7$, we have that $d = \left\lfloor \sqrt{\frac{a}{2}} \right\rfloor = 1$ so that $C^*(a,d) = [a]$ and $\#C^*(a,d) = a+1$; however, we will demonstrate that $\mu(4) = 4 < 5 = \#C^*(a,d)$. By Proposition

5.2.2, we must have that $\{0,1,3,4\} \subseteq A$ for any complete double A of $[4]$, hence we have that $\mu(4) \geq 4$. Conversely, one can immediately verify that $A = \{0,1,3,4\}$ is a complete double of $[4]$ so that $\mu(4) \leq 4$. Consequently, the complete double from Lemma 5.2.4 is not minimal.

Remark 5.2.9. Conversely, [Yu09, Theorem 1.2] shows that $\mu(a)$ does not achieve $2\sqrt{a}$ asymptotically, hence the lower bound from Proposition 5.2.6 could be improved.

Given any complete double A for $[a]$, one naturally wonders if A must be a "complete triple" of $[a]$. Put another way, if we have that $2A = [2a]$, then is it true that $3A = [3a]$? Before we answer this question in the affirmative, we make the following simple observation.

Lemma 5.2.10. *We have that* $[ra] = [(r-1)a] + \{0,a\}$ *for all integers* $r \geq 2$.

Proof. Observe that if $0 \leq t \leq (r-1)a$, then $t = t+0$ is an element of $[(r-1)a] + \{0,a\}$. On the other hand, for any integer $(r-1)a+1 \leq t \leq ra$, we may write $t = (r-2)a+\ell+a$ for some integer $1 \leq \ell \leq a$ so that $(r-2)a+\ell$ is an element $[(r-1)a]$. □

Proposition 5.2.11. *If* A *is a complete double of* $[a]$, *then* $rA = [ra]$ *for all integers* $r \geq 2$.

Proof. We will assume that A is a complete double of $[a]$. By Proposition 5.2.2, we must have $\{0,a\} \subseteq A$. We proceed by induction on r. By Lemma 5.2.10, we have that

$$[3a] = [2a] + \{0,a\} = 2A + \{0,a\} \subseteq 2A + A = 3A.$$

Conversely, by definition of complete double, we have that $A \subseteq [a]$ so that $3A \subseteq 3[a] = [3a]$. We will assume inductively that the claim holds for some integer $r \geq 4$. Using our inductive hypothesis in combination with Lemma 5.2.10, we have that

$$[ra] = [(r-1)a] + \{0,a\} = (r-1)A + \{0,a\} \subseteq rA.$$

Conversely, the other containment holds in a manner analogous to the $r = 3$ case. □

Example 5.2.12. Consider the set $A = \{0,1,4,5\} \subsetneq [5]$. Observe that $1+6 = 4+3 = 5+2$ are the only distinct integer partitions of 7 consisting of $1, 4$, or 5, hence A is not a complete double of $[5]$. Explicitly, we have that $2A = \{0,1,2,4,5,6,8,9,10\}$, from which it is not difficult to see that $3A = [15] = 3[5]$. We turn our attention to this phenomenon in the following definition.

Definition 5.2.13. We refer to $\operatorname{reg}(A) = \inf\{r \geq 1 \mid rA = [ra]\}$ as the **regularity** of A.

Observe that $\operatorname{reg}(A) = 1$ if and only if $A = [a]$. Consequently, if A is a proper subset of $[a]$, then we must have that $\operatorname{reg}(A) \geq 2$ with equality if and only if A is a complete double of $[a]$. Even more, by Proposition 5.2.2, we have that $\operatorname{reg}(A) = \infty$ if $\{0,1,a-1,a\}$ is not contained in A.

One immediate observation regarding the regularity of A is as follows.

Proposition 5.2.14. *If* $\operatorname{reg}(B)$ *is finite, then* $\operatorname{reg}(A) \leq \operatorname{reg}(B)$ *whenever* $B \subseteq A \subseteq [a]$.

Proof. By hypothesis that $\operatorname{reg}(B)$ is finite, there exists an integer $r \geq 1$ such that $rB = [ra]$ and $(r-1)B \subsetneq [(r-1)a]$. Consequently, we have that $[ra] = rB \subseteq rA \subseteq r[a] = [ra]$ so that $rA = [ra]$, from which it follows that $\operatorname{reg}(A) \leq r = \operatorname{reg}(B)$. □

By Proposition 5.2.2, if $\operatorname{reg}(A)$ is finite, then A must contain $\mathscr{L}_a = \{0,1,a-1,a\}$. Further, by Proposition 5.2.14, if $\operatorname{reg}(\mathscr{L}_a)$ is finite, then $\operatorname{reg}(A) \leq \operatorname{reg}(\mathscr{L}_a)$ for any subset $A \subseteq [a]$ with finite regularity. Consequently, it is critical to determine the regularity of $\mathscr{L}_a$. We do so immediately.

Proposition 5.2.15. *Let* $\mathscr{L}_a = \{0,1,a-1,a\}$. *We have that* $\operatorname{reg}(\mathscr{L}_a) = a-2$.

Proof. Observe that $a-2 \notin r\mathscr{L}_a$ for any integer $1 \leq r \leq a-3$. On the other hand, we have that $a-2 = \sum_{i=1}^{a-2} 1$ belongs to $(a-2)\mathscr{L}_a$. Consequently, we must have that $\operatorname{reg}(\mathscr{L}_a) \geq a-2$.

We claim that $(a-2)\mathscr{L}_a = [(a-2)a]$. Observe that any integer $0 \leq n \leq a-2$ can be written as the sum of n copies of 0 and $a-2-n$ copies of 0, hence we have that $\{0,1,\ldots,a-2\} \subseteq (a-2)\mathscr{L}_a$. Likewise, any integer $a-1 \leq n \leq 2(a-2)$ can be written as $n = (a-1)+t\cdot 1$ for some integer $0 \leq t \leq a-3$, hence we have that $\{a-1,\ldots,2(a-)\} \subseteq (a-2)\mathscr{L}_a$. Continuing this analysis yields

$$\bigcup_{i=0}^{a-1} \{i(a-1), i(a-1)+1, \ldots, (i+1)(a-2)\} \subseteq (a-2)\mathscr{L}_a.$$

Ultimately, it suffices to show that the elements $(i+1)(a-2)+1,\ldots,(i+1)(a-1)-1$ belong to $(a-2)\mathscr{L}_a$. One can verify that each of these elements is of the form $ja+t(a-1)+(a-2-i)\cdot 1$ for some integers $j \geq 1$ such that $j+t=i$, hence they all lie in $(a-2)\mathscr{L}_a$, as desired. □

Corollary 5.2.16. *Let $a \geq 3$ be an integer. We have that*

$$\min\{\#A \mid rA = [ra] \text{ for some integer } r \geq 1\} = 4.$$

Particularly, for all integers $a \geq 3$, the set $\mathscr{L}_a$ of Proposition 5.2.14 is the unique subset of $[a]$ of least cardinality that satisfies $rA = [ra]$ for some integer $n \geq 1$.

Proof. By Proposition 5.2.15, we have that $(a-2)\mathscr{L}_a = [(a-2)a]$ and $\#\mathscr{L}_a = 4$, hence the quantity in question does not exceed four. By Proposition 5.2.2, if A satisfies $rA = [ra]$ for some integer $r \geq 1$, then we must have that $\mathscr{L}_a \subseteq A$, hence the quantity is no less than four. □

Corollary 5.2.17. *We have that* $\max\{\mathrm{reg}(A) \mid \{0,1,a-1,a\} \subseteq A \subseteq [a]\} = a-2$.

We will now make use of the results of this section in an application to some two-dimensional monomial subrings. Before moving on, we settle a question that originally motivated this paper.

Definition 5.2.18. We say that a sequence $n_1 < \cdots < n_s$ of positive integers is **Sidon** if the sums $n_i + n_j$ are pairwise distinct for all integers $1 \leq i \leq j \leq s$. We will also refer to the set $A = \{n_1,\ldots,n_s\}$ as Sidon whenever the sequence $n_1 < \cdots < n_s$ is Sidon.

Because the pairwise sums of elements of a Sidon set must be distinct, a Sidon set must be "sparse enough." On the contrary, the subsets of $[a]$ with finite regularity must be "dense enough" to fill out $[ra]$ for some integer $1 \leq r \leq a-2$. Consequently, one wonders if there is a connection between Sidon sets and the subsets of $[a]$ with finite regularity. Our next propositions address this.

Proposition 5.2.19. *Given any non-negative integers $n_1 < \cdots < n_s$ with $n_s \geq 2$, consider the set $A = \{n_1,\ldots,n_s\} \subseteq [n_s]$. If A has finite regularity, then it is not Sidon.*

Proof. By Proposition 5.2.2, if A has finite regularity, we must have that $\{0,1,n_s-1,n_s\} \subseteq A$. Consequently, the sums $0+n_s$ and $1+(n_s-1)$ coincide, hence A is not a Sidon set. □

Proposition 5.2.20. *If A contains three consecutive non-negative integers, then A is not Sidon. Put another way, a Sidon set cannot contain $\{t, t+1, t+2\}$ for any integer $t \geq 0$.*

Proof. Observe that the sums $t + (t+2)$ and $(t+1) + (t+1)$ coincide. □

5.3 The ath Pseudo-Veronese Subring of $k[x,y]$

Given integers $a > n_1 > \cdots > n_s > 0$ and a field k, fix the set $A = \{0, n_s, \ldots, n_1, a\}$. We will henceforth consider the ath **pseudo-Veronese** subring of $k[x,y]$, i.e., the monomial subring

$$k[x,y]^{(A)} = k[x^a, x^{n_1}y^{a-n_1}, \ldots, x^{n_s}y^{a-n_s}, y^a] = k[x^i y^{a-i} \mid i \in A]$$

of $k[x,y]$ with homogeneous maximal ideal $\mathfrak{m} = (x^i y^{a-i} \mid i \in A)$. Observe that x and y are integral over $k[x,y]^{(A)}$, from which it follows by Proposition 2.1.69 that $\dim k[x,y]^{(A)} = \dim k[x,y] = 2$. Considering that $k[x,y]^{(A)}$ is a domain, we have that $1 \leq \operatorname{depth} k[x,y]^{(A)} \leq \dim k[x,y]^{(A)} = 2$.

Observe that $k[x,y]^{(A)}$ generalizes the ath **Veronese** subring of $k[x,y]$, i.e., the monomial subring

$$k[x,y]^{(a)} = k[x^a, x^{a-1}y, \ldots, xy^{a-1}, y^a] = k[x^i y^{a-i} \mid 0 \leq i \leq a]$$

of $k[x,y]$ with maximal irrelevant ideal $\mathfrak{a} = (x^i y^{a-i} \mid 0 \leq i \leq a)$. Explicitly, it is clear that if $A = [a]$, then $k[x,y]^{(A)} = k[x,y]^{(a)}$. We note that $k[x,y]^{(a)}$ is a two-dimensional normal Cohen-Macaulay domain (cf. [Ver18, Theorem 4.3]). Observe that as a standard graded k-algebra, we have that

$$k[x,y] = \bigoplus_{n=0}^{\infty} k\langle x^i y^{n-i} \mid 0 \leq i \leq n \rangle,$$

hence we may view $k[x,y]^{(a)}$ as a standard graded k-vector subspace of $k[x,y]$ by

$$k[x,y]^{(a)} = \bigoplus_{n=0}^{\infty} k\langle x^i y^{na-i} \mid 0 \leq i \leq na \rangle.$$

Consequently, the k-vector space dimension of the nth graded piece of $k[x,y]^{(a)}$ is $na+1$. Even

more, we may identify $k[x,y]_n^{(a)}$ with $k[x,y]_{na}$ via the graded inclusion $k[x,y]^{(a)} \subseteq k[x,y]$. Likewise, there is a graded inclusion $k[x,y]^{(A)} \subseteq k[x,y]^{(a)}$ (and hence a graded inclusion of k-vector spaces).

Our first proposition illustrates that if A contains some "normalizing element," then the integral closure of the ath pseudo-Veronese subring of $k[x,y]$ is precisely the ath Veronese subring of $k[x,y]$.

Proposition 5.3.1. *If $n_s = 1$ or $n_1 = a-1$, the integral closure of $k[x,y]^{(A)}$ is $k[x,y]^{(a)}$.*

Proof. By symmetry, it suffices to prove the claim for $n_s = 1$. By [Vil15, Theorem 9.1.1], we have that $\overline{k[x,y]^{(A)}} = k[x^m y^n \mid (m,n) \in \mathbb{Z}\mathscr{P} \cap \mathbb{Q}_+\mathscr{P}]$, where we denote by $\mathscr{P} = \{(i, a-i) \mid i \in A\}$ and $\mathbb{Z}\mathscr{P}$ the set of all finite $\mathbb{Z}$-linear combinations of the elements of $\mathscr{P}$. By hypothesis that $n_s = 1$, it follows that $(1, a-1)$ is in $\mathscr{P}$, hence we have that $(-1,1) = (0,a) - (1,a-1)$ is in $\mathbb{Z}\mathscr{P}$. Consequently, for each integer $0 \leq j \leq a$, we have that $(j, a-j) = (0,a) - j(-1,1)$ is in $\mathbb{Z}\mathscr{P}$. Considering that $(a,0)$ and $(0,a)$ are in $\mathscr{P}$, it follows that $(1,0)$ and $(0,1)$ are in $\mathbb{Q}_+\mathscr{P}$ so that $\mathbb{Q}_+\mathscr{P} = \mathbb{Q}_+^2$ and $\mathbb{Z}\mathscr{P} \cap \mathbb{Q}_+\mathscr{P} = \mathbb{Z}\mathscr{P} \cap \mathbb{Q}_+^2 = \mathbb{Z}_+\mathscr{P}$. We conclude that $\mathbb{Z}\mathscr{P} \cap \mathbb{Q}_+\mathscr{P} = \{(j, a-j) \mid 0 \leq j \leq a\}$, from which it follows that the integral closure of $k[x,y]^{(A)}$ is $k[x^j y^{a-j} \mid 0 \leq j \leq a] = k[x,y]^{(a)}$. □

Our aim throughout the rest of this section is to understand the following question.

Question 5.3.2. If A has finite regularity, what are $H_{k[x,y]^{(A)}}(t)$, $e(k[x,y]^{(A)})$, and $\operatorname{reg}(k[x,y]^{(A)})$ (the Hilbert series, multiplicity, and regularity of $k[x,y]^{(A)}$, respectively)?

We begin our efforts in this direction with a simple observation.

Proposition 5.3.3. *We have that $\mathfrak{m}^n = (x^j y^{na-j} \mid j \in nA)$ and $\mu(\mathfrak{m}^n) = \#(nA)$ for all $n \geq 1$.*

Proof. By elementary properties of exponentiation of finitely generated ideals, we have that

$$\mathfrak{m}^n = (x^i y^{a-i} \mid i \in A)^n = (x^j y^{na-j} \mid j = i_1 + \cdots + i_n \text{ with } i_1, \ldots, i_n \in A) = (x^j y^{ra-j} \mid j \in nA).$$

Consequently, it follows that $\mu(\mathfrak{m}^n) = \dim_k(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \#(nA)$ for each integer $n \geq 1$. □

Our next proposition follows from the last; it was suggested by Souvik Dey.

Proposition 5.3.4. *The Hilbert function of $R = k[x,y]^{(A)}$ is $H(R,n) = \#(nA)$. Even more, if $rA = [ra]$ for some integer $r \geq 1$, then $e(R) = a$, i.e., the largest element of A.*

Proof. By definition of the Hilbert function, we have that

$$H(R,n) = \ell_R\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) = \ell_k\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) = \dim_k\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) = \mu(\mathfrak{m}^n) = \#(nA),$$

where the last equality holds by Proposition 5.3.3. By the first paragraph of this section, we have that $d = \dim(R) = 2$. Consequently, we find that

$$e(R) = \lim_{n\to\infty} \frac{(d-1)!}{n^{d-1}} \ell_R\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) = \lim_{n\to\infty} \frac{\#(nA)}{n}.$$

By hypothesis that $rA = [ra]$ for some integer $r \geq 1$, it follows that $nA = [na]$ so that $\#(nA) = na+1$ for all integers n sufficiently large. We conclude that $e(R) = a$. □

We can also obtain the Hilbert series and multiplicity of $k[x,y]^{(A)}$ by expounding upon the ideas preceding Proposition 5.3.4, as we illustrate in the next two propositions.

Proposition 5.3.5. *We have that $\mathfrak{m}^r = \mathfrak{a}^r$ if and only if $rA = [ra]$ for some integer $r \geq 1$.*

Proof. If $rA = [ra]$ for some integer $r \geq 1$, then we have that

$$\mathfrak{m}^r = (x^j y^{ra-j} \mid j \in rA) = (x^j y^{ra-j} \mid j \in [ra]) = (x^j y^{ra-j} \mid 0 \leq j \leq ra) = \mathfrak{a}^r.$$

Conversely, if $\mathfrak{m}^r = \mathfrak{a}^r$ for some integer $r \geq 1$, then for each integer $0 \leq i \leq ra$, there exist polynomials f_j in $k[x,y]^{(a)}$ such that $x^i y^{ra-i} = \sum_{j\in rA} f_j x^j y^{ra-j}$. Considering that the multidegree of $x^i y^{ra-i}$ is $(i, ra-i)$, all summands of other multidegrees on the right-hand side must cancel. Put another way, we have that $x^i y^{ra-i} = \sum_{j\in rA} g_j x^j y^{ra-j}$, where g_j are monomials of multidegree $(i-j, j-i)$. Considering that the g_j are monomials in $k[x,y]^{(a)}$, we must have that $i-j \geq 0$ and $j-i \geq 0$ so that $i = j$ is in rA, and we conclude that $rA = [ra]$. □

Using Proposition 5.3.5, we are able to compute the Hilbert series of $k[x,y]^{(A)}$.

Proposition 5.3.6. *If* $\operatorname{reg}(A) = r$ *is finite, then the Hilbert series of* $R = k[x,y]^{(A)}$ *is*

$$H_R(t) = \sum_{n=0}^{r-1} \#(nA)t^n + \frac{at^r(1+r-rt)}{(1-t)^2} - \frac{(a-1)t^r}{1-t}.$$

Proof. By Proposition 5.3.1, we may view R as a graded k-vector subspace of $k[x,y]^{(a)}$. We have a short exact sequence $0 \to R \to S \to V \to 0$ with $S = k[x,y]^{(a)}$ and $V = S/R$. By Proposition 5.3.5, if $rA = [ra]$ for some integer $r \geq 1$, then $\mathfrak{m}^r = \mathfrak{a}^r$ so that $\mathfrak{m}^n = \mathfrak{a}^n$ for each integer $n \geq r$. Consequently, we have that $S_n = R_n$ for all integers $n \geq r$ so that $V_n = 0$ for all integers $n \geq r$. Likewise, we find that $V_0 = 0$, as both R_0 and S_0 are k. Ultimately, we conclude that $V_n = k\langle x^i y^{na-i} \mid i \in [na] \setminus nA\rangle$ for each integer $1 \leq n \leq r-1$. Considering that $\dim_k(S_n) = na+1$, we find that

$$\begin{aligned}
H_R(t) = H_S(t) - H_V(t) &= \sum_{n=0}^{\infty}(na+1)t^n - \sum_{n=1}^{r-1}[na+1-\#(nA)]t^n \\
&= 1 + \sum_{n=1}^{r-1}\#(nA)t^n + \sum_{n=r}^{\infty}(na+1)t^n \\
&= \sum_{n=0}^{r-1}\#(nA)t^n + \sum_{n=r}^{\infty}(na+1)t^n \\
&= \sum_{n=0}^{r-1}\#(nA)t^n + \sum_{n=r}^{\infty}(a(n+1)-(a-1))t^n \\
&= \sum_{n=0}^{r-1}\#(nA)t^n + t^r\sum_{n=0}^{\infty}(a(n+r+1)-(a-1))t^n \\
&= \sum_{n=0}^{r-1}\#(nA)t^n + \frac{at^r(1+r-rt)}{(1-t)^2} - \frac{(a-1)t^r}{1-t}.
\end{aligned}$$

□

Remark 5.3.7. Continuing with the notation of Proposition 5.3.6, we find once again that $e(R) = a$.

Observe that the numerator of $H_R(t)$ as a rational function is given by

$$f(t) = (1-t)^2 \sum_{n=0}^{r-1} \#(nA)t^n - (a-1)(1-t)t^r + at^r(1+r-rt).$$

We conclude that $e(R) = f(1) = a$ (cf. [BH93, Proposition 4.1.9]).

Remark 5.3.8. Continuing with the notation of Proposition 5.3.6, it follows by the above proof that if $\operatorname{reg}(A) = r$ is finite, then the R-module S/R has finite length over R.

Our next proposition was also suggested to me by Souvik Dey.

Proposition 5.3.9. *If* $\operatorname{reg}(A) = r$ *is finite, then* $k[x,y]^{(A)}$ *is Cohen-Macaulay if and only if* $A = [a]$.

Proof. Observe that if $A = [a]$, then $k[x,y]^{(A)} = k[x,y]^{(a)}$ is Cohen-Macaulay (cf. [Ver18, Theorem 4.3]). Conversely, if $r \geq 2$, then by the proof of Proposition 5.3.6, we have that

$$f(t) = (1-t)^2 \sum_{n=0}^{r-1} \#(nA)t^n - (a-1)(1-t)t^r + at^r(1+r-rt),$$

hence the coefficient of t^{r+1} in $f(t)$ is $\#[(r-1)A] - 1 - ar < [(r-1)a+1] - 1 - ar < 0$. Consequently, [BH93, Corollary 4.1.10] implies that $k[x,y]^{(A)}$ cannot be Cohen-Macaulay. □

Consider the polynomial ring $S = k[x_0, x_1, \ldots, x_s, x_{s+1}]$. We may view $k[x,y]^{(A)}$ as a standard graded S-module via the isomorphism $k[x,y]^{(A)} \cong S/\ker\varphi$ induced by the ring homomorphism $\varphi : S \to k[x,y]$ obtained by the assignments $\varphi(x_0) = x^a$, $\varphi(x_{s+1}) = y^a$, and $\varphi(x_i) = x^{n_i}y^{a-n_i}$ for each integer $1 \leq i \leq s$. Considering that S is regular, it follows by the Auslander-Buchsbaum Formula that every finitely generated S-module has finite projective dimension, hence $k[x,y]^{(A)}$ has a finite free resolution as an S-module. Consequently, we may consider a minimal graded free resolution

$$F_\bullet : 0 \to \bigoplus_{j\in\mathbb{Z}} S(-j)^{\beta_{rj}} \to \cdots \to \bigoplus_{j\in\mathbb{Z}} S(-j)^{\beta_{1j}} \to S(0) \to R \to 0$$

of $R = k[x,y]^{(A)}$, where the positive integer β_{ij} (commonly known as a **Betti number**) enumerates

the copies of degree j summands of the ith free module. We define the **(Castelnuovo-Mumford) regularity** of R to be the positive integer $\mathrm{reg}(R) = \max_{i,j}\{j-i \mid \beta_{ij} \neq 0\}$.

Example 5.3.10. By Proposition 5.2.15, the set $\mathscr{L}_4 = \{0,1,3,4\}$ has $\mathrm{reg}(\mathscr{L}_4) = 2$. Considering that $R = k[x,y]^{(\mathscr{L}_4)} = k[x^4, x^3y, xy^3, y^4]$ is a quotient of $S = k[a,b,c,d]$, we may obtain a minimal graded free resolution of R as an S-module. Explicitly, we find that

$$F_\bullet : 0 \to S(-5) \xrightarrow{A\cdot} S(-4)^4 \xrightarrow{B\cdot} S(-2) \oplus S(-3)^3 \xrightarrow{C\cdot} S(0) \to R \to 0,$$

where the above resolution and the following matrices A, B, and C were found via [GS, Macaulay2].

$$A = \begin{pmatrix} d \\ -c \\ -b \\ a \end{pmatrix}$$

$$B = \begin{pmatrix} -b^2 & -ac & -bd & -c^2 \\ c & d & 0 & 0 \\ a & b & -c & -d \\ 0 & 0 & a & b \end{pmatrix}$$

$$C = \begin{pmatrix} bc-ad & b^3-a^2c & ac^2-b^2d & c^3-bd^2 \end{pmatrix}$$

Consequently, we find that $\mathrm{reg}(k[x,y]^{(\mathscr{L}_4)} = \max\{0-0, 2-1, 3-1, 4-2, 5-3\} = 2$.

Our next proposition establishes that the equality of Example 5.3.10 is no coincidence.

Lemma 5.3.11. *For any integer $a \geq 2$, we have that* $\mathrm{reg}(k[x,y]^{(a)}) = 1$.

Proof. By [BS13, Definition 14.1.1 and Definition 16.2.9], it suffices to show that

$$\max\{i+\max\{n \mid H^i_{\mathfrak{a}}(k[x,y]^{(a)})_n \neq 0\}\} = 1.$$

Observe that $k[x,y]^{(a)}_n = k[x,y]_{na}$ as standard graded k-algebras. Consequently, by [GW78, Theorem 3.1.1], we have that $H^i_{\mathfrak{a}}(k[x,y]^{(a)})_n \cong H^i_{\mathfrak{M}}(k[x,y])_{na}$, where we denote by $\mathfrak{M}$ the homogeneous maximal ideal of $k[x,y]$. Considering that $k[x,y]$ and $k[x,y]^{(a)}$ are Cohen-Macaulay of dimension two, it follows that the local cohomology modules of $k[x,y]$ and $k[x,y]^{(a)}$ vanish in all indices other than $i = 2$ by Grothendieck's Vanishing Theorem. Further, we have that $\operatorname{reg}(k[x,y]) = 0$ so that

$$0 = \operatorname{reg}(k[x,y]) = 2+\max\{n \mid H^2_{\mathfrak{M}}(k[x,y])_n \neq 0\}$$

implies that $H^2_{\mathfrak{a}}(k[x,y]^{(a)})_n \cong H^2_{\mathfrak{M}}(k[x,y])_{na} \neq 0$ if and only if $na \leq -2$ if and only if $n \leq -1$. Ultimately, we find that $\operatorname{reg}(k[x,y]^{(a)}) = 2+\max\{n \mid H^2_{\mathfrak{a}}(k[x,y]^{(a)})_n \neq 0\} \leq 2-1 = 1$. Conversely, we must have that $\operatorname{reg}(k[x,y]^{(a)}) \geq 1$, hence the desired equality holds. □

Proposition 5.3.12. *If* $\operatorname{reg}(A)$ *is finite, we have that* $\operatorname{reg}(k[x,y]^{(A)}) = \operatorname{reg}(A)$. *Put in other terms, if* $r = \min\{m \geq 1 \mid mA = [ma]\}$, *then we have that* $\operatorname{reg}(k[x,y]^{(A)}) = r$.

Proof. If $\operatorname{reg}(A)$ is finite, then Proposition 5.2.2 yields that $n_1 = a-1$ and $n_s = 1$. We conclude by Proposition 5.3.1 that $S = k[x,y]^{(a)}$ is the integral closure of $R = k[x,y]^{(A)}$. Consequently, the monomials $x^i y^{a-i}$ with $0 \leq i \leq a$ are integral over R so that $S = R[x^i y^{a-i} \mid 0 \leq i \leq a \text{ and } i \notin A]$ and S/R are finitely generated R-modules by Corollary 2.1.61. We obtain a long exact sequence

$$0 \to H^0_{\mathfrak{m}}(R) \to H^0_{\mathfrak{m}}(S) \to H^0_{\mathfrak{m}}(S/R) \to H^1_{\mathfrak{m}}(R) \to H^1_{\mathfrak{m}}(S) \to H^1_{\mathfrak{m}}(S/R) \to \cdots$$

of local cohomology modules from the short exact sequence $0 \to R \to S \to S/R \to 0$ by Proposition 2.2.55, where $\mathfrak{m} = \bigoplus_{n\geq 1} R_n$ is the homogeneous maximal ideal of R. By Grothendieck's Vanishing Theorem, we have that $H^0_{\mathfrak{m}}(R) = 0$ and $H^i_{\mathfrak{m}}(R) = 0$ for all integers $i \geq 3$. Observe that the inclusion $R \subseteq S$ is a graded local ring homomorphism and $\mathfrak{m}$ is an $\mathfrak{a}$-primary ideal by Proposition 5.3.5,

hence the proof of Grothendieck's Vanishing Theorem yields that $H^i_{\mathfrak{m}}(S) \cong H^i_{\mathfrak{a}}(S)$ for all integers $i \geq 0$. We conclude that $H^i_{\mathfrak{m}}(S) = 0$ for all integers $i \neq 2$ and $H^2_{\mathfrak{m}}(S) \neq 0$, as S is Cohen-Macaulay. Consequently, the long exact sequence of local cohomology splits into the short exact sequences

$$0 \to H^0_{\mathfrak{m}}(S/R) \to H^1_{\mathfrak{m}}(R) \to 0 \text{ and} \tag{1.}$$

$$0 \to H^1_{\mathfrak{m}}(S/R) \to H^2_{\mathfrak{m}}(R) \to H^2_{\mathfrak{m}}(S) \to H^2_{\mathfrak{m}}(S/R) \to 0. \tag{2.}$$

Observe that (1.) implies that $H^1_{\mathfrak{m}}(R) \cong H^0_{\mathfrak{m}}(S/R)$, where by Proposition 2.2.55, we have that

$$H^0_{\mathfrak{m}}(S/R) \cong \Gamma_{\mathfrak{m}}(S/R) = \{s+R \mid \mathfrak{m}^t(s+R) = 0_R + R \text{ for some integer } t \geq 0\}.$$

We claim that $H^0_{\mathfrak{m}}(S/R) \cong S/R$, from which it follows that $H^1_{\mathfrak{m}}(R) \cong S/R$ so that

$$1 + \max\{n \mid H^1_{\mathfrak{m}}(R)_n \neq 0\} = 1 + (\operatorname{reg}(A) - 1) = \operatorname{reg}(A).$$

It suffices to establish that $S/R \subseteq \Gamma_{\mathfrak{m}}(S/R)$. But this holds by Remark 5.3.8: the R-module S/R has finite length over R, hence in particular, there exists an integer $n \gg 0$ such that $\mathfrak{m}^n(S/R) = 0$. Even more, Remark 5.3.8 implies that $H^1_{\mathfrak{m}}(S/R) \cong H^2_{\mathfrak{m}}(S/R) = 0$ so that $H^2_{\mathfrak{m}}(R) \cong H^2_{\mathfrak{m}}(S) \cong H^2_{\mathfrak{a}}(S)$ by the above displayed equation (2.). Explicitly, the Depth Lemma implies that $\operatorname{depth}(S/R) = 0$, hence all higher local cohomology modules vanish. By the proof of Lemma 5.3.11, we find that

$$2 + \max\{n \mid H^2_{\mathfrak{m}}(R)_n \neq 0\} = 2 + \max\{n \mid H^2_{\mathfrak{a}}(S)_n \neq 0\} = 1.$$

Combined, the above two displayed equations imply the desired result that

$$\operatorname{reg}(R) = \max\{i + \max\{n \mid H^i_{\mathfrak{m}}(R)_n \neq 0\} \mid i \geq 0\} = \max\{\operatorname{reg}(A), 1\} = \operatorname{reg}(A),$$

where the last equality holds by the fact that $\operatorname{reg}(A) \geq 1$. Our proof is complete. $\square$

Further Directions

We pose several questions toward future work on Complete Doubles and the Regularity of a Set.

Question 5.3.13. What are the bounds on $\#A$ such that $\operatorname{reg}(A) = 3$?

Question 5.3.14. Is there a sharper bound between $\operatorname{reg}(A)$ and $\max \operatorname{reg}(A) = a-2$?

Question 5.3.15. Is there a concise relationship between $\#A$ and $\operatorname{reg}(A)$?

Recall that the **Eisenbud-Goto Conjecture (EGC)** states that for any homogeneous prime ideal $P \subseteq (x_1,\ldots,x_n)^2$ of $S = k[x_1,\ldots,x_n]$, we have that $\operatorname{reg}(S/P) \leq e(S/P) - \operatorname{ht}(P)$. By the commentary preceding Example 5.3.10, the ath pseudo-Veronese subring $k[x,y]^{(A)}$ is the quotient of $S = k[x_0,x_1,\ldots,x_s,x_{s+1}]$ by a homogeneous prime ideal P contained in $(x_0,x_1,\ldots,x_s,x_{s+1})^2$.

Question 5.3.16. Let A be a subset of $[a]$ that contains $0, 1, a-1$, and a. Let k be an algebraically closed field. Under what additional conditions does $k[x,y]^{(A)}$ satisfy the EGC?

For more details about the EGC, we refer the reader to [CM18, Conjecture 2.2]. Considering that $R = k[x,y]^{(A)}$ is a domain that is finitely generated as k-algebra, it follows that $\operatorname{ht}(P) = s$, so our previous question asks when it is true that $\operatorname{reg}(R) \leq e(R) - \operatorname{ht}(P) = a - s$, where the last equality holds by Proposition 5.3.4. Combined, Corollary 5.2.17 and Proposition 5.3.12 imply that $\operatorname{reg}(R) = \operatorname{reg}(A) \leq a-2$ whenever $\operatorname{reg}(A)$ is finite. Consequently, if $s = 2$, then the EGC holds. On the other hand, if $A = [a]$, it follows by Lemma 5.3.11 that $\operatorname{reg}(R) = 1 = a - s$.

Question 5.3.17. Given an integer $a \geq 3$, consider the set $A = \{0, 1, 2, a-1, a\}$ and the corresponding monomial ring $R = k[x,y]^{(A)}$ of $k[x,y]$. Does it hold that $\operatorname{reg}(R) \leq a-3$?

Acknowledgements

We gratefully acknowledge Hailong Dao for bringing this project to our attention and for his suggestion of the statement and proof of Proposition 5.3.12. We thank Souvik Dey for his useful comments and suggestions regarding The ath Pseudo-Veronese Subring of $k[x,y]$.

Chapter 6

Appendix

We continue to assume that all commutative rings possess a multiplicative identity.

6.1 Artinian Rings and Modules

By definition, a commutative ring R has Krull dimension 0 if and only if every prime ideal of R is maximal. Using this observation, we make the following generalization of Example 2.1.29.

Lemma 6.1.1. *Let R be a commutative unital ring. Let I be a finitely generated nilpotent ideal of R. We have that R is Artinian (as an R-module) if and only if R/I is Artinian (as an R/I-module).*

Proof. By Definition 2.1.21, if R is Artinian as an R-module, then every descending chain of ideals of R stabilizes. By the Correspondence Theorem, a descending chain of ideals of R/I induces a descending chain of ideals of R that must stabilize. We conclude that the corresponding chain in R/I must stabilize, hence R/I is Artinian as an R/I-module. Conversely, assume that R/I is Artinian as an R/I-module. By Propositions 2.1.22 and 2.1.26, it follows that R/I is an Artinian R-module. By hypothesis that I is a finitely generated nilpotent ideal, there exists an integer $n \gg 0$ such that $I^n = \{0_R\}$. Consequently, we have that I^{n-1} is a finitely generated R/I-module by the fifth paragraph following Definition 2.1.13. We conclude by Definition 2.1.21 that I^{n-1} is an Artinian R-module. Likewise, it follows that I^{n-2}/I^{n-1} is an Artinian R/I-module. Considering that there is an exact sequence of R/I-modules $0 \to I^{n-1} \to I^{n-2} \to I^{n-2}/I^{n-1} \to 0$ for which the outer two nonzero modules are Artinian, we conclude that I^{n-2} is Artinian as an R-module. Continuing in this manner for all non-negative integers yields that $R = I^0$ is Artinian as an R-module. □

Proposition 6.1.2. *Let R be a commutative unital ring. The following conditions are equivalent.*

(i.) *R is Artinian.*

(ii.) *R is Noetherian and* $\dim(R) = 0$.

Proof. We prove that an Artinian local ring is Noetherian; however, we note that this holds in general. If $(R, \mathfrak{m})$ is Artinian, then R is Noetherian by Proposition 2.1.25. Consider a prime ideal P of R. Observe that the integral domain R/P is Artinian by the Correspondence Theorem. If $\bar{x}$ is any nonzero element of R/P, the descending chain of ideals $R/P \supseteq (\bar{x}) \supseteq (\bar{x}^2) \supseteq \cdots$ stabilizes for some integer $n \gg 0$. Put another way, there exists an integer $n \gg 0$ such that $(\bar{x}^n) = (\bar{x}^{n+1})$, hence there exists an element $\bar{y} \in R/P$ such that $\bar{x}^n = \bar{x}^{n+1}\bar{y}$. Cancellation holds in R/P, hence we find that $\bar{1}_R = \bar{x}\bar{y}$, i.e., $\bar{x}$ is a unit of R/P. We conclude that R/P is a field so that P is a maximal ideal.

Conversely, suppose that R is Noetherian and $\dim(R) = 0$. By Proposition 2.1.51, there are only finitely many minimal prime ideals $P_1, \ldots, P_n$ of R; they are maximal ideals by assumption that $\dim(R) = 0$. By Proposition 2.1.50, every maximal ideal of R must contain a minimal prime ideal of R, hence the minimal prime ideals $P_1, \ldots, P_n$ constitute an exhaustive list of the maximal ideals of R. Consequently, the Jacobson radical $\mathrm{Jac}(R)$ and the nilradical $\sqrt{0_R}$ of R coincide. By Proposition 2.1.41, it follows that $\mathrm{Jac}(R)$ is nilpotent, hence it suffices to show that $R/\mathrm{Jac}(R)$ is Artinian by Lemma 6.1.1. By the Chinese Remainder Theorem, we have that $R/\mathrm{Jac}(R) \cong \prod_{i=1}^n R/P_i$. Each field R/P_i has dimension one as an R/P_i-vector space, hence the R-modules R/P_i have finite length over R by Proposition 2.1.26. Consequently, we find that $R/\mathrm{Jac}(R) \cong \prod_{i=1}^n R/P_i$ has finite length as an R-module, from which we conclude that $R/\mathrm{Jac}(R)$ is Artinian by Proposition 2.1.22. □

We have already seen throughout the first chapter that Artinian local rings arise in many useful contexts. Even more, in a Cohen-Macaulay local ring, one can always obtain an Artinian local ring by going modulo a maximal regular sequence. Consequently, it is important to understand the properties of Artinian rings. We record several important facts about these rings below.

Corollary 6.1.3. *Every commutative unital Artinian ring admits only finitely many maximal ideals.*

Proposition 6.1.4. *Every reduced Noetherian commutative unital ring that is the disjoint union of the set of its units and the set of its zero divisors is Artinian. Conversely, every Artinian commutative unital ring can be written as the disjoint union of its units and its zero divisors.*

Proof. If R is Noetherian, then there are finitely many minimal prime ideals $P_1, \ldots, P_n$ of R by Proposition 2.1.51. Even more, if R is reduced, then the nilradical $\sqrt{0_R}$ of R is zero, hence the intersection of all the minimal primes of R is zero by Proposition 2.1.52. Every nonzero element of every prime ideal of R must be a zero divisor by hypothesis. Consequently, for any nonzero element x of any prime ideal P of R, there exists a nonzero element $y \in R$ such that $xy = 0_R$, from which it follows that xy is contained in every minimal prime P_i of R. If x is not contained in any minimal prime P_i of R, then $y \in P_1 \cap \cdots \cap P_n = 0$ — a contradiction; thus, every element of P belongs to some minimal prime P_i of R and $P \subseteq P_1 \cup \cdots \cup P_n$. By the contrapositive of the Prime Avoidance Lemma, we have that $P \subseteq P_i$ for some integer $1 \leq i \leq n$ so that $P = P_i$ by the minimality of P_i. Ultimately, we conclude that $\dim(R) = 0$, hence R is Artinian by Proposition 6.1.2.

Conversely, every element of an Artinian commutative unital ring R is either a zero divisor or not. Observe that if x is a non-zero divisor of R, then $R \supseteq xR \supseteq x^2R \supseteq \cdots$ constitutes a descending chain of ideals of R. By hypothesis that R is Artinian, we have that $x^nR = x^{n+1}R$ for some integer $n \gg 0$, from which it follows that $x^n = x^{n+1}r$ and $x(x^nr - 1_R) = 0$ for some nonzero element $r \in R$. Considering that x is a non-zero divisor, it follows that $xr = 1_R$, hence x is a unit. □

Corollary 6.1.5. *Let R be an Artinian commutative ring. Every nonzero R-module is torsion-free.*

Proof. By Proposition 6.1.4, the non-zero divisors of R are precisely the units of R. But any unit u must be a non-zero divisor on M because $m = 0$ if $um = 0$, hence M is torsion-free. □

6.2 Localization as a Functor

Let S be a multiplicatively closed subset of a commutative ring R. Our aim in this section is to illustrate that localization of an R-module with respect to S is an exact functor. Localization of a commutative ring at a prime ideal yields a commutative local ring, hence this fact reduces many

questions to the local case. Given an R-module M, we may construct its localization at S in the same manner as in the section on Basic Properties and Invariants of Commutative Rings. Consider the equivalence relation on $M \times S$ induced by declaring that $(m,s) \sim (m',s')$ if and only if there exists an element $t \in S$ such that $t(s'm - sm') = 0$; then, the localization of M with respect to S is

$$S^{-1}M = \left\{ \frac{m}{s} : m \in M, s \in S, \text{ and } \frac{m}{s} = \frac{m'}{s'} \iff \text{there exists } t \in S \text{ such that } t(s'm - sm') = 0 \right\}.$$

Observe that if P is a prime ideal of a commutative ring R, then $W = R \setminus P$ is a multiplicatively closed subset of R and $M_P = W^{-1}M$; the **support** of M is $\text{Supp}_R(M) = \{P \in \text{Spec}(R) \mid M_P \neq 0\}$. Our next proposition illustrates that any prime ideal in the support of an R-module must contain the annihilator of M; the converse statement holds if M is finitely generated.

Proposition 6.2.1. *Let R be a commutative ring. Let M be an R-module. We have that* $\text{Supp}_R(M) \subseteq V(\text{ann}_R(M)) = \{P \in \text{Spec}(R) \mid P \supseteq \text{ann}_R(M)\}$. *If M is finitely generated, then equality holds.*

Proof. Observe that if $P \not\supseteq \text{ann}_R(M)$, then there exists an element $x \in R \setminus P$ such that $xm = 0$ for all elements $m \in M$. By definition, we find that $M_P = 0$. By taking the contrapositive of this chain of implications, it follows that if $P \in \text{Supp}_R(M)$, then $P \supseteq \text{ann}_R(M)$ and $P \in V(\text{ann}_R(M))$.

Conversely, we will assume that M is finitely generated. Observe that if $P \notin \text{Supp}_R(M)$, then $M_P = 0$. By definition, for every element m_i of a system of generators of M, there exists an element $x_i \in R \setminus P$ such that $x_i m_i = 0$. Consequently, the product $x = x_1 \cdots x_n$ lies in $R \setminus P$ and satisfies $xm = 0$ for all elements $m \in M$. We conclude that there exists an element $x \in \text{ann}_R(M)$ and $x \notin P$, from which it follows that $P \not\supseteq \text{ann}_R(M)$. Once again, by taking the contrapositive of these implications, we find that if $P \in V(\text{ann}_R(M))$, then $P \supseteq \text{ann}_R(M)$ so that $M_P \neq 0$ and $P \in \text{Supp}(M)$. □

We prove next that the localization of a module is a module over the localization of the ring.

Proposition 6.2.2. *Let S be a multiplicatively closed subset of a commutative ring R. Let M be an R-module. The localization of M with respect to S is an $S^{-1}R$-module via the action* $\frac{r}{u} \cdot \frac{m}{v} = \frac{rm}{uv}$.

Proof. We illustrate first that this action is well-defined. By definition, if $\frac{r}{u} = \frac{s}{v}$ in $S^{-1}R$, then there exists an element $t \in S$ such that $rtv = stu$. Given any element $\frac{m}{w}$ of $S^{-1}M$, we have that $rtvwm = stuwm$ so that $\frac{r}{u} \cdot \frac{m}{w} = \frac{rm}{uw} = \frac{sm}{vw} = \frac{s}{v} \cdot \frac{m}{w}$, hence the action is well-defined, as desired. We must now verify that the action satisfies the distributive laws; the other two properties hold by definition. Observe that for any elements $r_1, r_2 \in R$, $u_1, u_2, v \in S$, and $m \in M$, we have that

$$\left(\frac{r_1}{u_1} + \frac{r_2}{u_2}\right) \cdot \frac{m}{v} = \frac{r_1u_2 + r_2u_1}{u_1u_2} \cdot \frac{m}{v} = \frac{r_1u_2m + r_2u_1m}{u_1u_2v} = \frac{r_1u_2m}{u_1u_2v} + \frac{r_2u_1m}{u_1u_2v} = \frac{r_1}{u_1} \cdot \frac{m}{v} + \frac{r_2}{u_2} \cdot \frac{m}{v}.$$

We note that a similar analysis shows that multiplication distributes over addition in $S^{-1}M$. □

Consequently, localization with respect to S converts an R-module into an $S^{-1}R$-module. Given any R-module homomorphism $\varphi : M \to N$, consider the map $S^{-1}\varphi : S^{-1}M \to S^{-1}N$ defined by $S^{-1}\varphi\left(\frac{m}{s}\right) = \frac{\varphi(m)}{s}$. Observe that for any elements $r \in R$, $u, v, w \in S$, and $m, n \in M$, we have that

$$S^{-1}\varphi\left(\frac{r}{u} \cdot \frac{m}{v} + \frac{n}{w}\right) = \varphi\left(\frac{rwm + uvn}{uvw}\right) = \frac{\varphi(rwm + uvn)}{uvw} = \frac{rw\varphi(m) + uv\varphi(n)}{uvw} = \frac{r}{u} \cdot \frac{\varphi(m)}{v} + \frac{\varphi(n)}{w},$$

hence the induced map $S^{-1}\varphi$ is an $S^{-1}R$-module homomorphism. Considering that $S^{-1}M$ is an R-module with respect to the action $r \cdot \frac{m}{s} = \frac{rm}{s}$, the map $S^{-1}\varphi$ is also an R-module homomorphism.

Proposition 6.2.3. *Let S be a multiplicatively closed subset of a commutative ring R. Let $\mathscr{R}$ be the category of R-modules. The map $S^{-1}(-)$ that sends an R-module M to $S^{-1}M$ (viewed as either an R-module or an $S^{-1}R$-module) and sends an R-module homomorphism $\varphi : M \to N$ to the module homomorphism $S^{-1}\varphi : S^{-1}M \to S^{-1}N$ is a covariant functor that preserves bijections.*

Proof. Clearly, the induced map $S^{-1}\,\mathrm{id}_M$ is the identity on $S^{-1}M$. Given any R-module homomorphisms $\varphi : A \to B$ and $\psi : B \to C$, it is straightforward to verify that $S^{-1}(\psi \circ \varphi) = S^{-1}\psi \circ S^{-1}\varphi$. We conclude that $S^{-1}(-)$ is a functor. Consider a bijective R-module homomorphism $\gamma : M \to N$. If $\frac{m}{s}$ lies in the kernel of $S^{-1}\gamma$, then there exists an element $t \in S$ such that $\gamma(tm) = t\gamma(m) = 0$. By hypothesis that γ is injective, we conclude that $tm = 0$, from which it follows that $\frac{m}{s} = 0$. On the other

hand, for any element $\frac{n}{s}$ of $S^{-1}M$, there exists an element $m \in M$ such that $\frac{n}{s} = \frac{\gamma(m)}{s} = S^{-1}\gamma\left(\frac{m}{s}\right)$ by assumption that γ is surjective. We conclude that $S^{-1}\gamma$ is a bijection, as desired. $\square$

Corollary 6.2.4. *Let S be a multiplicatively closed subset of a commutative ring R. If there is a short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$, then there is an induced short exact sequence $0 \to S^{-1}A \xrightarrow{S^{-1}\alpha} S^{-1}B \xrightarrow{S^{-1}\beta} S^{-1}C \to 0$ (of either R-modules or $S^{-1}R$-modules).*

Proof. By Proposition 6.2.3, we have that $S^{-1}\alpha$ is injective and $S^{-1}\beta$ is surjective, so it suffices to check the exactness of the sequence at $S^{-1}B$. Considering that $S^{-1}\beta \circ S^{-1}\alpha = S^{-1}(\beta \circ \alpha) = 0$, we have that $\operatorname{img}(S^{-1}\alpha) \subseteq \ker(S^{-1}\beta)$. If $\frac{b}{s}$ lies in the kernel of $S^{-1}\beta$, then there exists an element $t \in S$ such that $\beta(tb) = t\beta(b) = 0$. Consequently, we may find an element $a \in A$ such that $\alpha(a) = tb$ and $1_R(s\alpha(a) - stb) = 0$. We conclude that $\frac{b}{s} = \frac{\alpha(a)}{st} = S^{-1}\alpha\left(\frac{a}{st}\right)$ and $\ker(S^{-1}\beta) \subseteq \operatorname{img}(S^{-1}\alpha)$. $\square$

Observe that if $S \subseteq T$ are multiplicatively closed subsets of R, then one can "further localize" the R-module $S^{-1}M$ by inverting the elements of T, as well. Our next proposition and the following corollary illustrate that this further localization is "essentially the same" as localizing at T.

Proposition 6.2.5. *If $S \subseteq T$ are multiplicatively closed subsets of a commutative ring R, then for any R-module M, we have that $T^{-1}M \cong T^{-1}(\lambda(M))$, where $\lambda : M \to S^{-1}M$ is the canonical map.*

Proof. By definition, $T^{-1}(S^{-1}M)$ consists of all fractions $\frac{m/s}{t}$ with $m \in M$, $s \in S$, and $t \in T$ such that $\frac{m/s}{t} = \frac{m'/s'}{t'}$ if and only if there exist elements $s'' \in S$ and $t'' \in T$ such that $s''(s't't''m - stt''m') = 0$; it is an R-module in the obvious manner. Consider the R-module homomorphism $\varphi : T^{-1}M \to T^{-1}(S^{-1}M)$ defined by $\varphi\left(\frac{m}{t}\right) = \frac{m/1_R}{t}$. Observe that if $\frac{m}{t} = \frac{m'}{t'}$, then there exists an element $t'' \in T$ such that $t't''m - tt''m' = 0$. By setting the elements s, s', and s'' equal to 1_R, we conclude that $\frac{m/1_R}{t} = \frac{m'/1_R}{t'}$, hence φ is well-defined. Conversely, if $\frac{m/1_R}{t} = 0$, then there exist elements $s'' \in S$ and $t'' \in T$ such that $s''t''m = 0$. Considering that $s''t'' \in T$, we conclude that $\frac{m}{t} = 0$, hence φ is injective and $T^{-1}M \cong \operatorname{img}\varphi = T^{-1}(\lambda(M))$ by the First Isomorphism Theorem. $\square$

Corollary 6.2.6. *If P and Q are prime ideals of a commutative ring such that $P \subseteq Q$, then for any R-module M, we have that $M_P \cong (M_Q)_P$.*

Proof. By hypothesis that P and Q are prime ideals of R with $P \subseteq Q$, it follows that $S = R \setminus Q$ and $T = R \setminus P$ are multiplicatively closed subsets of R with $S \subseteq T$. By Proposition 6.2.5, we conclude that $T^{-1}M \cong T^{-1}(\lambda(M))$. Observe that for any elements $\dfrac{m}{1_R} \in \lambda(M)$ and $t \in R \setminus P$, we have that $\dfrac{m/1_R}{t} = \dfrac{sm/s}{t}$ lies in $T^{-1}(S^{-1}M)$ so that $T^{-1}(\lambda(M)) \subseteq T^{-1}(S^{-1}M)$. Conversely, for any elements $\dfrac{m}{s} \in S^{-1}M$ and $t \in R \setminus P$, we have that $\dfrac{m/s}{t} = \dfrac{m/1_R}{st}$ lies in $T^{-1}(\lambda(M))$. Ultimately, we conclude that $M_P = T^{-1}M \cong T^{-1}(\lambda(M)) = T^{-1}(S^{-1}M) = (M_Q)_P$. □

Observe that if M is an R-module, then $S^{-1}R \otimes_R M$ is an R-module. On the other hand, we may view $S^{-1}R \otimes_R M$ as an $S^{-1}R$-module via the action $\dfrac{a}{b} \cdot \left(\dfrac{r}{s} \otimes_R m\right) = \dfrac{ar}{bs} \otimes_R m$ by the proof of Proposition 6.2.3. Consider the map $\varphi : S^{-1}R \times M \to S^{-1}M$ defined by $\varphi\left(\dfrac{r}{s}, m\right) = \dfrac{rm}{s}$. Observe that φ is multiplication in the second coordinate, hence it is R-linear in the second coordinate. On the other hand, for any elements $a, r, s \in R$, $u, v \in S$, and $m \in M$, we have that

$$\varphi\left(a \cdot \frac{r}{u} + \frac{s}{v}, m\right) = \varphi\left(\frac{arv + su}{uv}, m\right) = \frac{(arv + su)m}{uv} = \frac{arvm}{uv} + \frac{sum}{uv} = a \cdot \varphi\left(\frac{r}{u}, m\right) + \varphi\left(\frac{s}{v}, m\right),$$

hence φ is R-linear in the first coordinate. We conclude that φ is a bilinear R-module homomorphism. By the Universal Property of the Tensor Product, there exists a bilinear R-module homomorphism $\gamma : S^{-1}R \otimes_R M \to S^{-1}M$ that satisfies $\gamma\left(\dfrac{r}{s} \otimes_R m\right) = \dfrac{rm}{s}$. We exhibit an R-module homomorphism $\psi : S^{-1}M \to S^{-1}R \otimes_R M$ such that $\gamma \circ \psi$ and $\psi \circ \gamma$ are the identity homomorphisms. Given any element $\dfrac{m}{s} \in S^{-1}M$, define $\psi\left(\dfrac{m}{s}\right) = \dfrac{1_R}{s} \otimes_R m$. Observe that if $\dfrac{m}{s} = \dfrac{m'}{s'}$, then there exists an element $t \in S$ such that $s'tm = stm'$. Consequently, we have that

$$\frac{1_R}{s} \otimes_R m = \frac{s't}{ss't} \otimes_R m = \frac{1_R}{ss't} \otimes_R (s'tm) = \frac{1_R}{ss't} \otimes_R (stm') = \frac{st}{ss't} \otimes_R m' = \frac{1_R}{s'} \otimes_R m',$$

hence ψ is well-defined. By definition of the tensor product, ψ is R-linear, hence it is an R-module homomorphism. Clearly, we have that $\gamma \circ \psi$ is the identity of $S^{-1}M$. Conversely, we have that $\psi \circ \gamma$ is the identity on the pure tensors of $S^{-1}R \otimes_R M$, hence it is the identity on $S^{-1}R \otimes_R M$. One can easily verify that both γ and ψ are $S^{-1}R$-module homomorphisms, hence we obtain the following.

Proposition 6.2.7. *Let S be a multiplicatively closed subset of a commutative ring R. Let M be an R-module. We have that $S^{-1}M \cong S^{-1}R \otimes_R M$ as an R-module and as an $S^{-1}R$-module.*

Corollary 6.2.8. *Let S be a multiplicatively closed subset of a commutative ring R. The R-module $S^{-1}R$ is flat, i.e., the tensor product $S^{-1}R \otimes_R -$ preserves exact sequences.*

Proof. This follows as a direct consequence of Propositions 6.2.4 and 6.2.7. □

Corollary 6.2.9. *Let S be a multiplicatively closed subset of a commutative ring R. Localization commutes with direct sums, i.e., for any (possibly infinite) index set I and any family of R-modules $(M_i)_{i \in I}$, we have that $S^{-1}(\bigoplus_{i \in I} M_i) \cong \bigoplus_{i \in I}(S^{-1}M_i)$.*

Proof. By Proposition 6.2.7, we have that $S^{-1}M_i \cong S^{-1}R \otimes_R M_i$ for each index i. Consequently, the desired result follows immediately from Proposition 2.1.89. □

Our next proposition lists many of the desirable properties of localization.

Proposition 6.2.10. *Let S be a multiplicatively closed subset of a commutative ring R. Let $N \subseteq M$, A, and B be R-modules. The following properties hold.*

(1.) *Localization detects the zero module, i.e., if $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of R, then $M = 0$.*

(2.) *Localization commutes with quotients, i.e., $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$.*

(3.) *Localization preserves the property of being finitely generated.*

(4.) *Localization preserves the property of being Noetherian.*

(5.) *Localization preserves the property of being free (or projective).*

(6.) *Localization preserves integral extensions.*

(7.) *Localization commutes with the integral closure, i.e., $S^{-1}\overline{R} = \overline{S^{-1}R}$.*

(8.) *Localization preserves reducedness.*

(9.) *Localization commutes with tensor products, i.e., $S^{-1}(A \otimes_R B) \cong S^{-1}A \otimes_{S^{-1}R} S^{-1}B$.*

Proof. (1.) On the contrary, suppose that there exists a nonzero element $m \in M$. Consequently, the annihilator of m in R is a proper ideal $\operatorname{ann}_R(m)$ of R, hence there exists a maximal ideal $\mathfrak{m}$ of R such that $\operatorname{ann}_R(m) \subseteq \mathfrak{m}$. By assumption that $M_{\mathfrak{m}} = 0$, there exists an element $r \in R \setminus \mathfrak{m}$ such that $rm = 0$. Observe that $r \in \operatorname{ann}_R(m)$ by definition and $r \notin \operatorname{ann}_R(m)$ by construction — a contradiction.

(2.) Use Corollary 6.2.4 on the short exact sequence of R-modules $0 \to N \to M \to M/N \to 0$; then, apply the First Isomorphism Theorem to obtain the desired result.

(3.) Consider a finitely generated R-module $M = R\langle x_1, \ldots, x_n \rangle$. Every element $m \in M$ can be written as $m = r_1 x_1 + \cdots + r_n x_n$ for some elements $r_1, \ldots, r_n \in R$. Consequently, every element $\dfrac{m}{s} \in S^{-1}M$ can be written as $\dfrac{m}{s} = \dfrac{r_1}{s}\dfrac{x_1}{1_R} + \cdots + \dfrac{r_n}{s}\dfrac{x_n}{1_R}$ so that $S^{-1}M = S^{-1}R\left\langle \dfrac{x_1}{1_R}, \ldots, \dfrac{x_n}{1_R} \right\rangle$.

(4.) If M is Noetherian, then every R-submodule of M is finitely generated. One can verify that every $S^{-1}R$-submodule of $S^{-1}M$ is of the form $S^{-1}N$ for some R-submodule N of M. By part (2.) above, every $S^{-1}R$-submodule of $S^{-1}M$ is finitely generated, hence $S^{-1}M$ is Noetherian.

(5.) If F is a free R-module, then it is a direct sum of copies of R, hence $S^{-1}F$ is a direct sum of copies of $S^{-1}R$ by Proposition 6.2.9. Likewise, if P is a projective R-module, then it is a direct summand of a free R-module, and $S^{-1}P$ is a direct summand of a free $S^{-1}R$-module.

(6.) Let $R \subseteq T$ be an integral extension. By Corollary 6.2.4, the inclusion $S^{-1}R \subseteq S^{-1}T$ is a ring extension. Given any element $\dfrac{x}{s}$ of $S^{-1}T$, there exist elements $a_1, \ldots, a_{n-1}, a_n \in R$ such that

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0_R.$$

By assumption that S is multiplicatively closed, the elements $s, \ldots, s^{n-1}, s^n$ belong to S, hence

$$\left(\frac{x}{s}\right)^n + \frac{a_1}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_{n-1}}{s^{n-1}}\left(\frac{x}{s}\right) + \frac{a_n}{s^n} = \frac{0_R}{s^n}$$

demonstrates that $\dfrac{x}{s}$ is integral over $S^{-1}R$. We conclude that $S^{-1}T$ is integral over $S^{-1}R$.

(7.) By part (4.) above, we find that $S^{-1}\overline{R} \subseteq \overline{S^{-1}R}$. Conversely, consider an equation

$$\left(\frac{x}{u}\right)^n + \frac{a_1}{v_1}\left(\frac{x}{u}\right)^{n-1} + \cdots + \frac{a_{n-1}}{v_{n-1}}\left(\frac{x}{u}\right) + \frac{a_n}{v_n} = 0$$

of integral dependence over $S^{-1}R$. Observe that if $d = uv_1 \cdots v_{n-1}v_n$, then by multiplying the previous displayed equation by $d^n/1_R$ and setting $c_i = a_i(uv_1 \cdots v_{n-1}v_n)^i/v_i$, we find that

$$\frac{(v_1 \cdots v_{n-1}v_n x)^n + c_1(v_1 \cdots v_{n-1}v_n x)^{n-1} + \cdots + c_{n-1}(v_1 \cdots v_{n-1}v_n x) + c_n}{1_R} = 0.$$

Consequently, there exists an element $t \in S$ such that t annihilates the element of R in the numerator. By multiplying this element by t^n, we obtain an expression of integral dependence

$$(tv_1 \cdots v_{n-1}v_n x)^n + tc_1(tv_1 \cdots v_{n-1}v_n x)^{n-1} + \cdots + t^{n-1}c_{n-1}(tv_1 \cdots v_{n-1}v_n x) + t^n c_n = 0_R.$$

We conclude that $tv_1 \cdots v_{n-1}v_n x$ belongs to $\overline{R}$. Considering that each of the elements $t, v_1, \ldots, v_{n-1}$ lies in S, the element $\frac{x}{u} = \frac{tv_1 \cdots v_{n-1}v_n x}{tv_1 \cdots v_{n-1}v_n u}$ belongs to $S^{-1}\overline{R}$ and $\overline{S^{-1}R} \subseteq S^{-1}\overline{R}$.

(8.) We prove the contrapositive, i.e., we show that if $S^{-1}R$ is not reduced, then R is not reduced. Consider a nonzero nilpotent element $\frac{r}{s} \in S^{-1}R$ such that $\frac{r^n}{s^n} = \left(\frac{r}{s}\right)^n = 0$. By definition of $S^{-1}R$, there exists a nonzero element $t \in S$ such that $r^n t = 0_R$ and $(rt)^n = 0_R$, hence the element $rt \in R$ is nilpotent; it must be nonzero because $\frac{r}{s}$ is nonzero by assumption.

(9.) By Proposition 6.2.7 and the associativity of the tensor product, we have that

$$S^{-1}(A \otimes_R B) \cong S^{-1}R \otimes_R (A \otimes_R B) \cong (S^{-1}R \otimes_R A) \otimes_R B \cong S^{-1}A \otimes_R B.$$

By the second part of Proposition 2.1.89, we have that $S^{-1}A \cong S^{-1}A \otimes_{S^{-1}R} S^{-1}R$, from which it follows that $S^{-1}A \otimes_R B \cong (S^{-1}A \otimes_{S^{-1}R} S^{-1}R) \otimes_R B$. Considering that $S^{-1}R$ is both an R-module and an $S^{-1}R$-module, the associative property of the tensor product yields that

$$(S^{-1}A \otimes_{S^{-1}R} S^{-1}R) \otimes_R B \cong S^{-1}A \otimes_{S^{-1}R} (S^{-1}R \otimes_R B) \cong S^{-1}A \otimes_{S^{-1}R} S^{-1}B. \qquad \square$$

Under certain conditions, localization commutes with Hom in the following sense.

Proposition 6.2.11. *[Rot09, Lemma 4.87] Let R be a Noetherian commutative unital ring. Let*

S be a multiplicatively closed subset of R. Let M be a finitely generated R-module. Let N be an arbitrary R-module. We have that $S^{-1}\operatorname{Hom}_R(M,N) \cong \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$.

Localization admits even more useful properties that we omit for the sake of brevity. We direct the reader to the end of [Rot09, Section 4.7] for further information (cf. pages 198 to 202).

6.3 The Total Ring of Fractions

We say that a nonzero element r of a commutative unital ring R is a **non-zero divisor** if $rs = 0_R$ implies that $s = 0_R$. Units are always non-zero divisors. Even more, the product of any two non-zero divisors is itself a non-zero divisor. Consequently, the collection S of all non-zero divisors of R is a multiplicatively closed subset; the ring $Q(R) = S^{-1}R$ is the **total ring of fractions** of R.

We record throughout this section the many useful properties of the total ring of fractions of a commutative unital ring. We begin by establishing that R is always an R-submodule of $Q(R)$.

Proposition 6.3.1. *Let R be a commutative unital ring with total ring of fractions* $Q(R)$. *We may identify R with an R-submodule of* $Q(R)$ *via the localization map* $\lambda : R \to Q(R)$.

Proof. We claim that the localization map $\lambda : R \to Q(R)$ defined by $\lambda(r) = \dfrac{r}{1_R}$ is injective. By definition, if $\lambda(r) = 0$, then there exists an element $t \in S$ such that $tr = 0_R$. Considering that S consists of non-zero divisors of R, we conclude that $r = 0_R$, as desired. □

Corollary 6.3.2. *We have that* $Q(Q(R)) \cong Q(R)$ *for any commutative unital ring R.*

Proof. By Proposition 6.3.1, we have that $\lambda(R) \cong R$. Consequently, it follows from Propositions 6.2.4 and 6.2.5 that $Q(R) = S^{-1}R \cong S^{-1}\lambda(R) \cong S^{-1}(S^{-1}\lambda(R)) \cong S^{-1}Q(R) = Q(Q(R))$. □

Consequently, we will henceforth distinguish neither R from $\lambda(R)$ nor $Q(R)$ from $Q(Q(R))$. Under these identifications, we state and prove our next general observation.

Proposition 6.3.3. *Let R be a commutative unital ring with total ring of fractions* $Q(R)$. *Let I and J be R-submodules of* $Q(R)$. *Every R-module homomorphism* $\varphi : I \to J$ *is* $Q(R)$*-linear.*

Proof. Let $\varphi : I \to J$ be an R-module homomorphism. By hypothesis that $I \subseteq Q(R)$, every element of I can be written as $\dfrac{a}{b}$ for some non-zero divisor $b \in R$. Observe that

$$\varphi\left(\frac{a}{b}\right) = \frac{a}{1_R}\varphi\left(\frac{1_R}{b}\right) = \frac{a}{b}\cdot\frac{b}{1_R}\varphi\left(\frac{1_R}{b}\right) = \frac{a}{b}\varphi(1),$$

where the first and third equalities hold since φ is R-linear. We conclude that φ is $Q(R)$-linear. □

Even more, if R is reduced and $Q(R)$ is a direct product of fields, then the R-module homomorphisms between R-submodules of $Q(R)$ are precisely multiplication by fractions of $Q(R)$.

Proposition 6.3.4. *[HS06, Lemma 2.4.1] Let R be a reduced commutative unital ring with total ring of fractions $Q(R)$. Let I and J be R-submodules of $Q(R)$. If $Q(R)$ is a direct product of finitely many fields, then any R-module homomorphism $\varphi : I \to J$ is multiplication by an element of $Q(R)$.*

Proof. We will assume that $Q(R) = k_1 \times \cdots \times k_r$ for some integer $r \geq 1$ and some fields $k_1, \ldots, k_r$. By definition, we have that $Q(R) = S^{-1}R$ for the multiplicatively closed subset S of R consisting of the non-zero divisors of R; therefore, if I and J are R-submodules that lie in $Q(R)$, then $S^{-1}I$ and $S^{-1}J$ are $Q(R)$-modules that can be identified with $Q(R)$-submodules of $Q(R)$ by 6.3.2. Considering that I is a submodule of a direct product of fields, it follows that $S^{-1}I = k_{i_1} \times \cdots \times k_{i_s}$ for some integers $1 \leq s \leq r$ and $i_1, \ldots, i_s$. Let e_i denote the element of $Q(R)$ that is 1 on k_i and 0 elsewhere, i.e., $e_i = (\delta_{ij} \mid 1 \leq j \leq r)$ for the Kronecker delta δ_{ij}. Observe that $\sum_{i=1}^{r} e_i = 1$. By the identification $R \cong \lambda(R)$, there exists an element $x \in S$ such that $xe_i \in R$ for all integers $1 \leq i \leq r$ and $xe_i \in I$ for all integers $i \in \{i_1, \ldots, i_s\}$. By definition of e_i, we have that $e_i I = 0$ for all integers $i \notin \{i_1, \ldots, i_s\}$. Consider an R-module homomorphism $\varphi : I \to J$. By Proposition 6.3.3, we have that

$$x\varphi(\alpha) = \varphi(x\alpha) = \varphi(x\alpha(e_1 + \cdots + e_r)) = \varphi(\alpha(xe_{i_1} + \cdots + xe_{i_s}) = \alpha\varphi(xe_{i_1} + \cdots + xe_{i_s})$$

for each element $\alpha \in I$, hence φ is multiplication by an element of $Q(R)$. □

Earlier in our discussion of Canonical Blow-Up of One-Dimensional Singularities, we required

an identification between the colon submodules of two R-submodules of $Q(R)$ and the R-module homomorphisms between the specified R-submodules of $Q(R)$. We provide the details here.

Proposition 6.3.5. *[HS06, Lemma 2.4.2] Let R be a reduced commutative unital ring with total ring of fractions $Q(R)$. Let I and J be R-submodules of $Q(R)$. If $Q(R)$ is the direct product of finitely many fields, then there exists a surjective R-module homomorphism $(J:I) \to \mathrm{Hom}_R(I,J)$ with kernel $(0:I)$, where $(J:I) = \{\alpha \in Q(R) \mid \alpha I \subseteq J\}$ is the* **colon submodule** *of I into J.*

Proof. By Proposition 6.3.4, every element of $\mathrm{Hom}_R(I,J)$ is multiplication by an element of $Q(R)$. Explicitly, there exists a surjective R-module homomorphism $(J:I) \to \mathrm{Hom}_R(I,J)$ that sends an element $\alpha \in (J:I)$ to multiplication by α. Consequently, it suffices to prove that its kernel is $(0:I)$. But this is immediate because the kernel consists of all elements $\alpha \in (J:I)$ such that $\alpha I = 0$. □

Proposition 6.3.6. *Let R be a reduced commutative unital ring with total ring of fractions $Q(R)$. Let I and J be R-submodules of $Q(R)$. Let $Q(R)$ be the direct product of finitely many fields.*

(1.) *The R-module $\mathrm{Hom}_R(I,J)$ is isomorphic to the R-submodule $(J:I)/(0:I)$ of $Q(R)/(0:I)$.*

(2.) *The R-module $\mathrm{Hom}_R(I,I)$ can be identified with a commutative unital subring of $Q(R)/(0:I)$.*

(3.) *If I contains a non-zero divisor of R, then $\mathrm{Hom}_R(I,J) \cong (J:I)$. Particularly, the R-module $\mathrm{Hom}_R(I,I)$ can be identified with a commutative unital subring of $Q(R)$.*

(4.) *If I is finitely generated and contains a non-zero divisor of R, then $\mathrm{Hom}_R(I,I)$ can be identified with a subring of the integral closure $\overline{R}$ of R in $Q(R)$.*

Proof. Using Proposition 6.3.5 and the First Isomorphism Theorem, we conclude that statement (1.) holds; thus, statement (2.) follows by observing that $(I:I)/(0:I)$ is a unital subring of the commutative ring $Q(R)/(0:I)$. Observe that if I contains a non-zero divisor x of R, then $(0:I)$ must be zero because $\alpha x = 0$ implies that $\alpha = 0$, hence statement (3.) holds. Last, suppose that I is finitely generated and contains a non-zero divisor of R. Observe that if $\alpha \in (I:I)$ is nonzero, then $\alpha I \subseteq I$. Even more, I is a faithful $R[\alpha]$-module because α is nonzero and I contains a non-zero divisor. By the Determinantal Trick with $S = Q(R)$ and the ideal R, we conclude that $\alpha \in \overline{R}$. □

Our next proposition illustrates that division of the colon submodule behaves well with respect to division by a non-zero divisor of R. We will denote $(N :_R M) = (N : M) \cap R$.

Proposition 6.3.7. *[HS06, Lemma 2.4.3] Let R be a reduced commutative unital ring with only finitely many minimal prime ideals. Let I and J be R-submodules of the total ring of fractions $Q(R)$ such that yI and yJ can be identified with ideals of R for some non-zero divisor y of R (cf. Proposition 6.3.1). If I contains a non-zero divisor x of R, then* $\mathrm{Hom}_R(J,I) \cong \frac{1_R}{xy}(xyJ :_R I)$.

Proof. By Proposition 2.1.56, we have that $Q(R)$ is a direct product of finitely many fields, hence it follows that $\mathrm{Hom}_R(I,J) \cong (J : I)$ by the third part of Proposition 6.3.6. Observe that multiplication of I by an element of $\frac{1_R}{xy}(xyJ :_R I)$ gives an element of J, hence we have that $\frac{1_R}{xy}(xyJ :_R I) \subseteq (J : I)$. Conversely, if $\alpha \in (J : I)$, then $\alpha yI \subseteq yJ$ implies that $\alpha xy \in (xyJ : I) \cap R$ and $\alpha \in \frac{1_R}{xy}(xyJ :_R I)$. □

One additional delightful property of $Q(R)$ is that its R-submodules are torsion-free.

Corollary 6.3.8. *Let R be a commutative unital ring. Every R-submodule of $Q(R)$ is torsion-free.*

Proof. By definition, the zero module is torsion-free. Let M be a nonzero R-submodule of $Q(R)$. Observe that a torsion element $\frac{a}{b} \in M$ satisfies $\frac{ra}{b} = 0$ for some non-zero divisor $r \in R$, hence there exists a non-zero divisor $s \in R$ such that $s(ra) = 0_R$. Observe that rs must be a non-zero divisor because r and s are. By Definition 2.1.166, we conclude that $a = 0_R$ so that M is torsion-free. □

Even more, the total ring of fractions of a commutative unital ring R gives a way to measure the "size" of certain R-modules. Explicitly, if M is any R-module such that $M \otimes_R Q(R)$ is a free $Q(R)$-module, then we define the **rank** of M to be the number of summands of $Q(R)$ in $M \otimes_R Q(R)$. If $M \otimes_R Q(R)$ is not a free $Q(R)$-module, then we say that M does not have a rank. Observe that if R is a domain with field of fractions $F = \mathrm{Frac(R)}$, then for any R-module M that has a rank, we have that $\mathrm{rank}(M) = \dim_F M \otimes_R F$, i.e., the rank of M is the F-vector space dimension of $M \otimes_R F$.

We demonstrate first that the rank detects the freeness of finitely generated projective modules over commutative unital rings with only finitely many maximal ideals.

Proposition 6.3.9. *[BH93, Lemma 1.4.4] Let R be a commutative unital ring that admits only finitely many maximal ideals. Let M be a finitely generated projective R-module. If we have that* $\operatorname{rank}(M_{\mathfrak{m}}) = n$ *for all maximal ideals* $\mathfrak{m}$ *of R, then M is a free R-module of rank n.*

Proof. We proceed by induction on $\operatorname{rank}(M_{\mathfrak{m}}) = n$. Observe that $R_{\mathfrak{m}}$ is a local ring for each maximal ideal $\mathfrak{m}$ of R, hence $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module for each maximal ideal $\mathfrak{m}$ of R by Corollary 2.1.98. Consequently, if $\operatorname{rank}(M_{\mathfrak{m}}) = 0$ for all maximal ideals $\mathfrak{m}$ of R, then $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ of R. We conclude that $M = 0$ by Proposition 6.2.10; it is a free R-module, as the empty set forms a basis. We may assume therefore that $\operatorname{rank}(M_{\mathfrak{m}}) = n \geq 1$ for all maximal ideals $\mathfrak{m}$ of R. By Nakayama's Lemma, we have that $M_{\mathfrak{m}} \not\subseteq \mathfrak{m}M_{\mathfrak{m}}$ for each maximal ideal $\mathfrak{m}$ of R. By the Prime Avoidance Lemma, there exists an element $x \in M$ such that $x/1_R \notin \mathfrak{m}M_{\mathfrak{m}}$ for each maximal ideal $\mathfrak{m}$ of R. Once again, by Nakayama's Lemma, we conclude that $x/1_R$ belongs to a minimal system of generators of $M_{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$ of R. Considering that every minimal system of generators of $M_{\mathfrak{m}}$ forms a basis for the free $R_{\mathfrak{m}}$-module $M_{\mathfrak{m}}$, it follows that $(M/Rx)_{\mathfrak{m}} \cong M_{\mathfrak{m}}/R_{\mathfrak{m}}(x/1_R)$ is a free $R_{\mathfrak{m}}$-module of rank $n-1$. By induction, it follows that M/Rx is a free R-module of rank $n-1$, from which we conclude by Proposition 2.1.81 that the short exact sequence of R-modules $0 \to Rx \to M \to M/Rx \to 0$ splits. Consequently, we find that $M \cong Rx \oplus (M/Rx)$. Considering that Rx is a direct summand of a projective module, it follows that Rx is projective so that $(Rx)_{\mathfrak{m}}$ is free by Proposition 2.1.98. Localization is exact by Proposition 6.2.4, hence the natural surjection $\pi : R \to Rx$ yields a surjection $\pi_{\mathfrak{m}} : R_{\mathfrak{m}} \to (Rx)_{\mathfrak{m}}$ of free $R_{\mathfrak{m}}$-modules of rank one for each maximal ideal $\mathfrak{m}$ of R. We conclude that $\ker(\pi)_{\mathfrak{m}} = \ker(\pi_{\mathfrak{m}}) = 0$ for all maximal ideals of R so that $\ker \pi = 0$ and Rx is free. Ultimately, this shows that $M \cong Rx \oplus (M/Rx)$ is a free R-module of rank n. □

We illustrate next that if a nonzero R-module M has a rank, then M admits a free R-module of the same rank that contains all of the elements of M that are not torsion.

Proposition 6.3.10. *Let R be a commutative unital ring with total ring of fractions $Q(R)$. Let M be a nonzero R-module. We have that* $\operatorname{rank}(M) = n$ *if and only if there exists a free R-submodule N of M of rank n (i.e., we have that $N \cong R^n$) such that M/N is torsion.*

Proof. By definition, if $\text{rank}(M) = n$, then $T = M \otimes_R Q(R) \cong S^{-1}M$ is a free $Q(R)$-module of rank n with a free basis $t_1 = m_1/d_1, \ldots, t_n = m_n/d_n$. Consider the product $d = d_1 \cdots d_n$. By hypothesis that $t_1, \ldots, t_n$ are $Q(R)$-linearly independent, if there were a $Q(R)$-relation among the elements $dt_1, \ldots, dt_n$, then there would be a $Q(R)$-relation among the elements $t_1, \ldots, t_n$ because d is a non-zero divisor of R — a contradiction. Consequently, the elements $dt_i = d_1 \cdots \widehat{d_i} \cdots d_n m_i/1_R$ are $Q(R)$-linearly independent, where a hat denotes the absence of a specified element from the product. Consider the R-submodule $N = R\langle d_2 \cdots d_n m_1, \ldots, d_1 \cdots d_{n-1} m_n \rangle$. If there were an R-relation among these generators, there would be a $Q(R)$-relation among the elements $dt_1, \ldots, dt_n$, hence N is a free R-submodule of M. Even more, we have that $(M/N) \otimes_R Q(R) = 0$ by construction, hence M/N is torsion. Conversely, if N is a free R-submodule of M of rank n and M/N is torsion, then $M \cong N \oplus (M/N)$ implies that $M \otimes_R Q(R) \cong N \otimes_R Q(R)$ is a free $Q(R)$-module of rank n. □

One of the most useful characterizations of the rank of an R-module is the following.

Proposition 6.3.11. *Let R be a Noetherian commutative unital ring with total ring of fractions $Q(R)$. Let M be a finitely generated R-module. We have that* $\text{rank}(M) = n$ *if and only if M_P is a free R_P-module of rank n for all associated prime ideals P of R.*

Proof. By Proposition 2.1.178, the collection of zero divisors of R is the union of all associated prime ideals of R. Consequently, the set S of non-zero divisors of R belongs to $R \setminus P$ for all associated prime ideals P of R. By the proof of Corollary 6.2.6, it follows that $Q(R)_P = (S^{-1}R)_P \cong R_P$. If $\text{rank}(M) = n$, then $M \otimes_R Q(R)$ is by definition a free $Q(R)$-module of rank n, hence we have that

$$M_P \cong M_P \otimes_{R_P} R_P \cong M_P \otimes_{R_P} Q(R)_P \cong (M \otimes_R Q(R))_P \cong (Q(R)^{\oplus n})_P \cong Q(R)_P^{\oplus n} \cong R_P^{\oplus n}$$

is a free R_P-module of rank n for all associated prime ideals P of R.

Conversely, we will assume that M_P is a free R_P-module of rank n for all associated prime ideals P of R. By Corollary 2.1.181, $Q(R)$ admits only finitely many maximal ideals, and the localizations at its maximal ideals are equal to the localizations of R at the associated prime ideals of R that are maximal under inclusion. Put another way, for each maximal ideal $\mathfrak{m}_i$ of $Q(R)$, we

have that $Q(R)_{\mathfrak{m}_i} \cong R_{P_i}$ for some ideal $P_i \in \operatorname{Ass}_R(R)$. Consequently, we have that

$$(M \otimes_R Q(R))_{\mathfrak{m}_i} \cong M_{\mathfrak{m}_i} \otimes_R Q(R)_{\mathfrak{m}_i} \cong M_{\mathfrak{m}_i} \otimes_R R_{P_i} \cong (M_{\mathfrak{m}_i})_{P_i} = M_{P_i}$$

is a free $Q(R)_{\mathfrak{m}_i}$-module of rank n for each maximal ideal $\mathfrak{m}_i$ of $Q(R)$. By Corollary 2.1.101, we conclude that $M \otimes_R Q(R)$ is a projective $Q(R)$-module whose localizations at the maximal ideals of $Q(R)$ have rank n. By Proposition 6.3.9, $M \otimes_R Q(R)$ is a free $Q(R)$-module of rank n. □

Proposition 6.3.12. *Let R be a Noetherian commutative unital ring with total ring of fractions $Q(R)$. Let I be an ideal of R. If* $\operatorname{rank}(I) > 0$, *then I contains a non-zero divisor of R.*

Proof. By Proposition 6.3.11, if $\operatorname{rank}(I) > 0$, then IR_P is a nonzero free R_P-module for all associated prime ideals P of R. Consequently, we have that $I \not\subseteq P$ for any associated prime ideal P of R, hence the Prime Avoidance Lemma implies that I contains an non-zero divisor of R: indeed, the set of zero divisors of R is the union of all associated primes of R by Proposition 2.1.178. □

Proposition 6.3.13. *[BH93, Exercise 1.4.23] Let R be a Noetherian commutative unital ring. Let M be a finitely generated R-module. We have that M has a rank if and only if $M^* = \operatorname{Hom}_R(M,R)$ has a rank. Further, if one of these conditions holds, then* $\operatorname{rank}(M) = \operatorname{rank}(M^*)$.

Proof. By Proposition 6.3.11, the R-module M has a rank if and only if M_P is a free R_P-module for all associated prime ideals P of R. We may assume therefore that $(R,\mathfrak{m})$ is a local ring with $\operatorname{depth}(R) = 0$ so that $\mathfrak{m}$ is an associated prime ideal of R by Corollary 2.2.6. Consequently, if M has a rank, then $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module by Proposition 6.3.11 so that M is a projective R-module by Corollary 2.1.101. By Proposition 6.3.9, it follows that M is a free R-module of rank $n \geq 0$, hence $\operatorname{Hom}_R(M,R)$ is a free R-module of rank $n \geq 0$ by Proposition 6.4.1. Conversely, if $\operatorname{Hom}_R(M,R)$ has a rank, then by Propositions 6.3.11 and 6.2.11, $\operatorname{Hom}_R(M,R)_{\mathfrak{m}} \cong \operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}},R_{\mathfrak{m}})$ is a free $R_{\mathfrak{m}}$-module so that M^* and M^{**} are free of the same rank $n \geq 0$ by the first part of the proof. By [BH93, Exercise 1.4.22], we conclude that M is reflexive so that $M \cong M^{**}$ has rank $n \geq 0$. □

We conclude this section with two results on module-finite extensions of integral domains.

Lemma 6.3.14. *If $R \subseteq S$ is a module-finite extension of integral domains, then* $\mathrm{Frac}(S) = N^{-1}S$, *where N is the set of nonzero elements of R. Put another way, the field of fractions of S is obtained by inverting only the nonzero elements of R (and not necessarily all nonzero elements of S).*

Proof. By Proposition 6.2.4, we have that $\mathrm{Frac}(R) = N^{-1}R \subseteq N^{-1}S$. By hypothesis that $R \subseteq S$ is a module-finite extension, it follows that $\mathrm{Frac}(R) \subseteq N^{-1}S$ is a module-finite extension by Propositions 2.1.65 and 6.2.10. Consequently, $N^{-1}S$ is a finite-dimensional $\mathrm{Frac}(R)$-vector space that is an integral domain, hence $N^{-1}S$ is a field satisfying $S \subseteq N^{-1}S \subseteq \mathrm{Frac}(S)$. But this implies that $\mathrm{Frac}(S) = N^{-1}S$ because $\mathrm{Frac}(S)$ is by definition the smallest field containing S. □

Proposition 6.3.15. *Let $R \subseteq S$ be a module-finite extension of integral domains with the same field of fractions $F = \mathrm{Frac}(R) = \mathrm{Frac}(S)$. We have that* $\mathrm{rank}(S) = 1$.

Proof. By definition, we have that $F = N^{-1}R$, where N is the set of nonzero elements of R. Consequently, we have that $F \otimes_R S = N^{-1}R \otimes_R S \cong N^{-1}S$ by Proposition 6.2.7. By assumption that $R \subseteq S$ is a module-finite extension of integral domains, we have that $\mathrm{Frac}(S) = N^{-1}S$ by Lemma 6.3.14. But this implies that $F \otimes_R S \cong N^{-1}S = \mathrm{Frac}(S) = F$, from which we conclude that $\mathrm{rank}(S) = 1$. □

6.4 Further Properties of Hom and Ext

We begin with the observation that Hom commutes with direct products.

Proposition 6.4.1. *Let R be a commutative ring. For any (possibly infinite) index set I and any families of R-modules $(M_i)_{i\in I}$ and $(N_i)_{i\in I}$, we have that* $\mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$ *and* $\mathrm{Hom}_R\left(M, \prod_{i\in I} N_i\right) \cong \prod_{i\in I} \mathrm{Hom}_R(M, N_i)$. *Particularly, it holds that* $\mathrm{Hom}_R(R^n, N) \cong N^n$.

Proof. Let $\sigma_i : M_i \to \bigoplus_{i\in I} M_i$ denote the ith component inclusion map, i.e., the R-module homomorphism that sends an element $m \in M_i$ to the I-tuple of elements with m in the ith component and zeros elsewhere. Given any R-module homomorphism $\varphi : \bigoplus_{i\in I} M_i \to N$, the I-tuple of composite maps $(\varphi \circ \sigma_i)_{i\in I}$ yields an element of $\prod_{i\in I} \mathrm{Hom}_R(M_i, N)$. Consider the R-module homomorphism $\psi : \mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, N\right) \to \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$ defined by $\psi(\varphi) = (\varphi \circ \sigma_i)_{i\in I}$. Observe that

φ belongs to $\ker \psi$ if and only if $\varphi \circ \sigma_i$ is the zero homomorphism for each index $i \in I$ if and only if φ is the zero homomorphism on $\bigoplus_{i\in I} M_i$, hence ψ is injective. Given any element γ of $\prod_{i\in I} \mathrm{Hom}_R(M_i,N)$, we may write $\gamma = (\gamma_i)_{i\in I}$ for some R-module homomorphisms $\gamma_i : M_i \to N$. Consider the R-module homomorphism $\varphi : \bigoplus_{i\in I} M_i \to N$ that sends $(m_i)_{i\in I} \mapsto \sum_{i\in I} \gamma_i(m_i)$. By definition, an element of $\bigoplus_{i\in I} M_i$ has only finitely many nonzero components, so $\sum_{i\in I} \gamma_i(m_i)$ is a well-defined element of N. Observe that for each index $i \in I$, we have that $\gamma_i(m_i) = \varphi \circ \sigma_i(m_i)$, hence we conclude that $\gamma = (\gamma_i)_{i\in I} = (\varphi \circ \sigma_i)_{i\in I}$ so that ψ is surjective.

Let $\pi_i : \prod_{i\in I} N_i \to N_i$ denote ith component projection map, i.e., the R-module homomorphism that sends an element $(n_i)_{i\in I} \in \prod_{i\in I} N_i$ to the element $n_i \in N_i$. One can show that the R-module homomorphism $\tau : \mathrm{Hom}_R(M, \prod_{i\in I} N_i) \to \prod_{i\in I} \mathrm{Hom}_R(M,N_i)$ defined by $\tau(\varphi) = (\pi_i \circ \varphi)_{i\in I}$ is bijective in an analogous manner to the previous paragraph. We note that the last statement of the proposition follows by Proposition 2.1.78 applied to $\mathrm{Hom}_R(R^n,N) \cong \mathrm{Hom}_R(R,N)^n$. □

Our next corollary illustrates sufficient conditions for which Hom is finitely generated.

Corollary 6.4.2. *Let R be a commutative ring. Let M and N be R-modules. If M is finitely generated and N is Noetherian, then $\mathrm{Hom}_R(M,N)$ is finitely generated as an R-module. Particularly, if R is Noetherian and M and N are finitely generated, then $\mathrm{Hom}_R(M,N)$ is finitely generated.*

Proof. By assumption, we have that $M = R\langle x_1, \ldots, x_n\rangle$ for some elements $x_1, \ldots, x_n$. Consequently, there exists a short exact sequence of R-modules $0 \to K \to R^n \to M \to 0$; the induced sequence of R-modules $0 \to \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(R^n,N) \to \mathrm{Hom}_R(K,N)$ is exact by Proposition 2.1.80. Put another way, there is an injective R-module homomorphism $\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_R(R^n,N)$, so we may identity $\mathrm{Hom}_R(M,N)$ as an R-submodule of $\mathrm{Hom}_R(R^n,N)$. By Proposition 6.4.1, the latter R-module is isomorphic to N^n; it is Noetherian by hypothesis, hence we conclude that $\mathrm{Hom}_R(M,N)$ is finitely generated. We note that the last statement holds because if R is Noetherian, then an R-module is Noetherian if and only if it is finitely generated. □

Ext “commutes" the operations of localization and completion as follows.

Proposition 6.4.3. *Let R be a commutative unital ring. Let S be a multiplicatively closed subset of R. Let M and N be R-modules. We have that $S^{-1}\operatorname{Ext}^i_R(M,N) \cong \operatorname{Ext}^i_{S^{-1}R}(S^{-1}M, S^{-1}N)$ for all $i \geq 1$.*

Proof. By definition, the Ext modules are the (co)homology modules of a long exact sequence of Hom. Localization is an exact functor that commutes with quotients, hence the claim holds. □

Proposition 6.4.4. *Let R be a Noetherian commutative unital ring. Let I be a proper ideal of R. Let M be a finitely generated R-module. We have that $\operatorname{Ext}^i_R(M,N)^\wedge_I \cong \operatorname{Ext}^i_{\widehat{R}_I}(\widehat{M}_I, \widehat{N}_I)$ for all $i \geq 1$.*

Proof. By Proposition 2.1.151, completion with respect to the I-adic topology is exact on finitely generated R-modules. Completion commutes with direct sums, hence the completion of any projective R-module with respect to the I-adic topology yields a projective $\widehat{R}_I$-module. Consequently, the completion of any projective resolution of M yields a projective resolution of $\widehat{M}_I$ as a $\widehat{R}_I$-module. Last, Proposition 2.1.153 implies that completion commutes with quotients, as well. □

We conclude this section with a few results toward the injective dimension.

Proposition 6.4.5. *Let R be a commutative unital ring. Let M and N be R-modules. We have that $\operatorname{Hom}_{R/I}(M/IM,N) \cong \operatorname{Hom}_R(M,N)$ for any ideal I of R such that $I \subseteq \operatorname{ann}_R(N)$.*

Proof. Observe that if the ideal I lies in $\operatorname{ann}_R(N)$, then N is an R/I-module. Particularly, Proposition 2.1.78 implies that $\operatorname{Hom}_{R/I}(R/I,N) \cong N$ as R/I-modules. By Proposition 2.1.89, we have that $M/IM \cong M \otimes_R (R/I)$ as R-modules. Consequently, the Tensor-Hom Adjunction yields

$$\operatorname{Hom}_{R/I}(M/IM,N) \cong \operatorname{Hom}_R(M, \operatorname{Hom}_{R/I}(R/I,N)) \cong \operatorname{Hom}_R(M,N). \qquad \square$$

Proposition 6.4.6. *Let R be a commutative unital ring. Let M and N be R-modules. Consider an R- and M-regular sequence $(x_1,\ldots,x_n)$ in $\operatorname{ann}_R(N)$. Let $R_i = R/(x_1,\ldots,x_i)R$ for each integer i. For all integers $m \geq i$ and $0 \leq i \leq n$, we have that $\operatorname{Ext}^m_R(N,M) \cong \operatorname{Ext}^{m-i}_{R_i}(N, M/(x_1,\ldots,x_i)M)$.*

Proof. By the proof of Proposition 2.1.185, we have $\operatorname{Ext}^m_R(N,M) \cong \operatorname{Ext}^{m-i}_R(N, M/(x_1,\ldots,x_i)M)$. Considering that the elements $x_1,\ldots,x_n$ lie in $\operatorname{ann}_R(N)$, we may view N as an R_i-module for each

$0 \leq i \leq n$. Under this identification, an R-module homomorphism from N to $M/(x_1,\ldots,x_i)M$ induces an R_i-module homomorphism from N to $M/(x_1,\ldots,x_i)M$ (and vice-versa). $\square$

Corollary 6.4.7. *Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Let M be a finitely generated R-module of finite injective dimension. If $\underline{x} = (x_1,\ldots,x_n) \subseteq \mathfrak{m}$ is R- and M-regular, then*

$$\operatorname{injdim}_{R/\underline{x}R}(M/\underline{x}M) = \operatorname{injdim}_R(M) - n.$$

6.5 Further Properties of Tensor Products and Tor

Our next proposition provides an analog of Corollary 6.4.2 for the tensor product.

Proposition 6.5.1. *Let R be a commutative ring. If M and N are finitely generated R-modules, then the tensor product $M \otimes_R N$ is finitely generated as an R-module.*

Proof. Every element of $M \otimes_R N$ can be written as $\sum_{i=1}^{k} r_i(m_i \otimes_R n_i)$ for some integer $k \geq 0$, some elements $r_1,\ldots,r_k \in R$, and some distinct elements $m_1,\ldots,m_k \in M$ and $n_1,\ldots,n_k \in N$. Each of the elements m_i can be written in terms of the generators of M, and each of the elements n_i can be written in terms of the generators of N. Consequently, if $M = R\langle x_1,\ldots,x_r\rangle$ and $N = R\langle y_1,\ldots,y_s\rangle$, the bilinearity of the map τ implies that $M \otimes_R N = R\langle x_i \otimes_R y_j \mid 1 \leq i \leq r \text{ and } 1 \leq j \leq s\rangle$. $\square$

We demonstrate next that integral extensions are preserved under tensor products.

Proposition 6.5.2. *Let $\varphi : R \to S$ be an integral extension of commutative unital rings. If $\psi : R \to R'$ is a commutative unital ring homomorphism, then the ring extension $R' \to R' \otimes_R S$ is integral.*

Proof. Like usual, we will view S as an R-module via $r \cdot s = \varphi(r)s$. By hypothesis that $\varphi : R \to S$ is an integral extension, for any nonzero element $s \in S$, there exist elements $r_0, r_1, \ldots, r_n$ of R such that $p(s) = r_n \cdot s^n + \cdots + r_1 \cdot s + r_0 \cdot 1_S = 0_S$. Consequently, the image $1_{R'} \otimes_R p(s)$ of this polynomial identity in $R' \otimes_R S$ yields a polynomial identity of $1_{R'} \otimes_R s$ in $R' \otimes_R S$ with coefficients in R'. Consequently, the elements $1_{R'} \otimes_R s$ of $R' \otimes_R S$ are integral over R'. Because the elementary tensors $1_{R'} \otimes_R S$ generate $R' \otimes_R S$ as an R'-module, we conclude that $R' \otimes_R S$ is integral over R'. $\square$

Remarkably, one can characterize flat R-modules in the following manner.

Proposition 6.5.3. *Let R be a commutative ring. The following properties are equivalent.*

(i.) *L is a flat R-module.*

(ii.) *If $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} L \to 0$ is a short exact sequence of R-modules, then the induced sequence $0 \to M \otimes_R A \xrightarrow{\mathrm{id}_M \otimes_R \alpha} M \otimes_R B \xrightarrow{\mathrm{id}_M \otimes_R \beta} M \otimes_R L \to 0$ is exact for any R-module M.*

Proof. Given any R-module M, consider the free R-module F indexed by M and the canonical surjection $\pi : F \to M$ with kernel K. Observe that there is a short exact sequence of R-modules $0 \to K \xrightarrow{i} F \xrightarrow{\pi} M \to 0$ such that the R-module homomorphism $i : K \to F$ is the inclusion map. By applying the right-exact functors $K \otimes_R -$, $F \otimes_R -$, and $M \otimes_R -$ to any short exact sequence of R-modules $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} L \to 0$, we obtain the following diagram of R-modules.

$$\begin{array}{ccccccccc}
 & & K \otimes_R A & \xrightarrow{\mathrm{id}_K \otimes_R \alpha} & K \otimes_R B & \xrightarrow{\mathrm{id}_K \otimes_R \beta} & K \otimes_R L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle i \otimes_R \mathrm{id}_A} & & \downarrow{\scriptstyle i \otimes_R \mathrm{id}_B} & & \downarrow{\scriptstyle i \otimes_R \mathrm{id}_L} & & \\
0 & \longrightarrow & F \otimes_R A & \xrightarrow{\mathrm{id}_F \otimes_R \alpha} & F \otimes_R B & \xrightarrow{\mathrm{id}_F \otimes_R \beta} & F \otimes_R L & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi \otimes_R \mathrm{id}_A} & & \downarrow{\scriptstyle \pi \otimes_R \mathrm{id}_B} & & \downarrow{\scriptstyle \pi \otimes_R \mathrm{id}_L} & & \\
 & & M \otimes_R A & \xrightarrow{\mathrm{id}_M \otimes_R \alpha} & M \otimes_R B & \xrightarrow{\mathrm{id}_M \otimes_R \beta} & M \otimes_R L & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

One can readily verify that the diagram commutes on the pure tensors of each tensor product, hence the diagram commutes. Even more, the columns and rows of the diagram are exact by Proposition 2.1.93 and Corollary 2.1.96. By the Snake Lemma, we obtain a short exact sequence of R-modules

$$\ker(i \otimes_R \mathrm{id}_A) \to \ker(i \otimes_R \mathrm{id}_B) \to \ker(i \otimes_R \mathrm{id}_L) \to M \otimes_R A \to M \otimes_R B \to M \otimes_R L \to 0.$$

By Proposition 2.1.94, we conclude that if L is flat, then $i \otimes_R \mathrm{id}_L$ is injective so that $\ker(i \otimes_R \mathrm{id}_L) = 0$ and $0 \to M \otimes_R A \xrightarrow{\mathrm{id}_M \otimes_R \alpha} M \otimes_R B \xrightarrow{\mathrm{id}_M \otimes_R \beta} M \otimes_R L \to 0$ is exact.

We obtain the converse as a corollary of Proposition 2.1.104. Explicitly, if condition (ii.) holds, then $\mathrm{Tor}_1^R(M, L) = 0$ for all R-modules M so that L is a flat R-module. □

One of the most important results in homological algebra is the Tensor-Hom Adjunction that relates the functors Hom and the tensor product. Let R and S be commutative rings. We say that an abelian group $(B,+)$ is an (R,S)-**bimodule** if it is an R-module via the action $\cdot$, an S-module via the action $*$, and these actions are "compatible" in the sense that $(r\cdot b)*s = r\cdot(b*s)$ for all elements $r\in R$, $s\in S$, and $b\in B$. Observe that if A is an R-module and B is an (R,S)-bimodule, then the tensor product $A\otimes_R B$ is a R-module via $r(a\otimes_R b) = (ra)\otimes_R b = a\otimes_R (rb)$ and a right S-module via $(a\otimes_R b)s = a\otimes_R (bs)$. One can check that $A\otimes_R B$ is an (R,S)-bimodule.

Theorem 6.5.4 (Tensor-Hom Adjunction)**.** *Let R and S be commutative rings. Let A be an R-module. Let B be an (R,S)-bimodule. Let C be an S-module. There exists a $\mathbb{Z}$-module isomorphism $\alpha : \mathrm{Hom}_S(A\otimes_R B, C) \to \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C))$ defined by $\alpha(\varphi)(a) : b \mapsto \varphi(a\otimes_R b)$ for all elements $a\in A$ and $b\in B$ and each S-module homomorphism $\varphi : A\otimes_R B \to C$.*

Proof. Before establishing the claim, we begin with a thorough examination of the objects therein. Each element of $\mathrm{Hom}_S(A\otimes_R B, C)$ is an S-module homomorphism $\varphi : A\otimes_R B\to C$. By definition, the pure tensors of $A\otimes_R B$ generate it as an S-module, hence every element of $\mathrm{Hom}_S(A\otimes_R B,C)$ is uniquely determined by its image on the pure tensors of $A\otimes_R B$. Likewise, the elements of $\mathrm{Hom}_R(A,\mathrm{Hom}_S(B,C))$ are R-module homomorphisms that send an element $a\in A$ to an S-module homomorphism $\psi_a : B\to C$. Consequently, for each S-module homomorphism $\varphi : A\otimes_R B\to C$, the designation of the S-module homomorphism $\psi_{\varphi,a} : B\to C$ onto which φ is mapped for each element $a\in A$ induces a function $\alpha : \mathrm{Hom}_S(A\otimes_R B,C)\to \mathrm{Hom}_R(A,\mathrm{Hom}_S(B,C))$. Considering that φ and the tensor product are (right) S-linear, the map $\psi_{\varphi,a} : B\to C$ defined by $\psi_{\varphi,a}(b) = \varphi(a\otimes_R b)$ is an S-module homomorphism that satisfies $\psi_{\varphi,a} = \alpha(\varphi)(a)$ as in the statement of the theorem.

We must prove first that α is $\mathbb{Z}$-linear. Given any S-module homomorphisms $\varphi : A\otimes_R B\to C$ and $\gamma : A\otimes_R B\to C$ and any element $n\in\mathbb{Z}$, we have that

$$\psi_{n\varphi+\gamma,a}(b) = (n\varphi+\gamma)(a\otimes_R b) = n\varphi(a\otimes_R b) + \gamma(a\otimes_R b) = (n\psi_{\varphi,a} + \psi_{\gamma,a})(b)$$

for all elements $a\in A$ and $b\in B$. By our previous identification, we conclude that α is $\mathbb{Z}$-linear.

If $\varphi : A \otimes_R B \to C$ lies in $\ker \alpha$, then $\psi_{\varphi,a}$ is the zero homomorphism for each element $a \in A$. Consequently, we find that $\varphi(a \otimes_R b) = \psi_{\varphi,a}(b) = 0$ for all elements $a \in A$ and $b \in B$. Considering that the pure tensors generate $A \otimes_R B$, we conclude that φ is the zero homomorphism.

Last, suppose that $\psi : A \to \mathrm{Hom}_R(B,C)$ is an R-module homomorphism. Let ψ_a denote the S-module homomorphism $\psi(a) : B \to C$, as in the opening paragraph of the proof. Consider the map $\sigma : A \times B \to C$ defined by $\sigma(a,b) = \psi_a(b)$. By assumption that ψ and its images ψ_a are all biadditive, it follows that $\sigma(a+a',b) = \psi_{a+a'}(b) = (\psi_a + \psi_{a'})(b) = \psi_a(b) + \psi_{a'}(b) = \sigma(a,b) + \sigma(a',b)$ and $\sigma(a,b+b') = \psi_a(b+b') = \psi_a(b) + \psi_a(b') = \sigma(a,b) + \sigma(a,b')$ for all elements $a,a' \in A$ and $b,b' \in B$. We conclude that σ is a biadditive R-module homomorphism, hence the Universal Property of the Tensor Product guarantees the existence of a biadditive $\mathbb{Z}$-module homomorphism $\gamma : A \otimes_R B \to C$ such that $\gamma(a \otimes_R b) = \sigma(a,b) = \psi_a(b)$ for all elements $a \in A$ and $b \in B$. Consequently, we find that ψ is the image of γ under α, hence α is surjective. □

6.6 Injective Modules and Injective Hulls

Our next propositions illuminate some important features of families of injective modules.

Proposition 6.6.1. *Let R be a commutative ring. If $(Q_i)_{i \in I}$ is a family of injective R-modules for some (possibly infinite) index set I, then $\prod_{i \in I} Q_i$ is an injective R-module. Particularly, every finite direct sum of injective R-modules is injective.*

Proof. By Proposition 2.1.84, it suffices to complete the following commutative diagram.

$$\begin{array}{ccccc} & & \prod_{i\in I} Q_i & & \\ & & \uparrow{\scriptstyle \varphi} & \nwarrow^{\exists \psi} & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B \end{array}$$

Observe that the ith component projection maps $\pi_i : \prod_{i \in I} Q_i \to Q_i$ induce R-module homomorphisms $\pi_i \circ \varphi : A \to Q_i$ for each index $i \in I$. By hypothesis that each of the R-modules Q_i is injective, it follows that there exist R-module homomorphisms $\psi_i : B \to Q_i$ such that $\pi_i \circ \varphi = \psi_i \circ \alpha$ for each index $i \in I$. Consider the R-module homomorphism $\psi : B \to \prod_{i \in I} Q_i$ defined by $\psi(b) = (\psi_i(b))_{i \in I}$.

Observe that $\psi \circ \alpha(a) = (\psi_i \circ \alpha(a))_{i \in I} = (\pi_i \circ \varphi(a))_{i \in I} = (\varphi(a)_i)_{i \in I} = \varphi(a)$ for each element $a \in A$. We conclude that $\varphi = \psi \circ \alpha$, hence $\prod_{i \in I} Q_i$ is an injective R-module. $\square$

Proposition 6.6.2. *Every direct summand of an injective R-module is injective.*

Proof. Let Q be an injective R-module such that $Q = M \oplus N$ for some R-modules M and N. Let $\sigma_1 : M \to Q$ be the first component inclusion map. Consider the following commutative diagram.

$$\begin{array}{ccccc} & & M & \xrightarrow{\sigma_1} & Q \\ & & \varphi \uparrow & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B \end{array}$$

Observe that $\sigma_1 \circ \varphi : A \to Q$ yields an R-module homomorphism, hence there exists an R-module homomorphism $\psi : B \to Q$ with the property that $\psi \circ \alpha = \sigma_1 \circ \varphi$. On the other hand, the first component projection map $\pi_1 : Q \to M$ induces an R-module homomorphism $\pi_1 \circ \psi : B \to M$ such that $\mathrm{id}_M \circ \varphi = (\pi_1 \circ \sigma_1) \circ \varphi = (\pi_1 \circ \psi) \circ \alpha$. Considering that $(\mathrm{id}_M \circ \varphi)(a) = \varphi(a)$ for all elements $a \in A$, we conclude that $\varphi = (\pi_1 \circ \varphi) \circ \alpha$ so that M is an injective R-module. $\square$

Every R-module embeds into an injective R-module. Given an R-module M, one might naturally search for a "smallest" injective module containing an isomorphic copy of M.

Proposition 6.6.3. *[Wal05, Proposition 1.6] Let M and E be nonzero R-modules. Let $\varphi : M \to E$ be an injective R-module homomorphism. The following statements are equivalent.*

(1.) *Every nonzero R-submodule F of E satisfies $F \cap \varphi(M) \neq 0$.*

(2.) *Every nonzero element of E has a nonzero multiple in $\varphi(M)$.*

(3.) *If there exists a nonzero R-module E' and an R-module homomorphism $\psi : E \to E'$ such that $\psi \circ \varphi$ is injective, then ψ must be injective.*

We say that E is an **essential extension** *of M (via φ) if any of the above properties hold.*

Proof. Let e be a nonzero element of E. If the first property holds, then the nonzero R-submodule Re of E satisfies $Re \cap \varphi(M) \neq 0$, hence there is a nonzero multiple of e in $\varphi(M)$. Consequently, we find that (1.) $\implies$ (2.). We will assume now that there exists a nonzero R-module E' and an

R-module homomorphism $\psi : E \to E'$ such that $\psi \circ \varphi$ is injective. If the second property holds, then ψ must be injective; otherwise, we could find elements $e \in \ker \psi$, $r \in R$, and $m \in M$ such that $re = \varphi(m)$ is nonzero, and this would yield the contradiction $0 = r\psi(e) = \psi(re) = \psi \circ \varphi(m)$. We conclude that (2.) $\implies$ (3.). Last, suppose that the third property holds. Let F be a nonzero R-submodule of E. Observe that the canonical surjection $\pi : E \to E/F$ has kernel F, hence it is not injective. By the contrapositive of the third property, the composite map $\pi \circ \varphi : M \to E/F$ cannot be injective, i.e., there exists a nonzero element in $F \cap \varphi(M)$ so that $F \cap \varphi(M) \neq 0$. □

Proposition 6.6.4. *Let M be an R-module. The following conditions hold.*

(1.) *Essentiality is a transitive property. Explicitly, if E' is an essential extension of E and E is an essential extension of M, then E' is an essential extension of M.*

(2.) *Essentiality is closed under inclusion. Explicitly, if $E' \supseteq E \supseteq M$ and $E' \supseteq M$ is an essential extension, then $E' \supseteq E$ is an essential extension and $E \supseteq M$ is an essential extension.*

Particularly, if E is an essential extension of M (via any injective R-module homomorphism), then $E' \supseteq E$ is an essential extension if and only if $E' \supseteq M$ is an essential extension.

Proof. (1.) If E' is an essential extension of E via ψ, then every nonzero element e of E' has a nonzero multiple $re = \psi(f)$ in $\psi(E)$. If E is an essential extension of M via φ, then the nonzero element f of E has a nonzero multiple $sf = \varphi(m)$ in $\varphi(M)$. Ultimately, we conclude that there is a nonzero multiple $rse = \psi \circ \varphi(m)$ of e in $\psi \circ \varphi(M)$, hence E' is an essential extension of M.

(2.) If $E' \supseteq M$ is an essential extension, then every nonzero element of E has a nonzero multiple in M. Considering that $E \supseteq M$, it follows that every nonzero element of E' has a nonzero multiple in E, hence $E' \supseteq E$ is an essential extension. Likewise, every nonzero element of E can be viewed as an element of E', hence every nonzero element of E has a nonzero multiple in M.

Last, suppose that $\varphi : M \to E$ is an essential extension of M. Consider the inclusion map $i_E : E \to E'$. Observe that E' is an essential extension of E via i_E if and only if every nonzero element e of E' has a nonzero multiple in $i_E(E)$ if and only if every nonzero element e of E' has a nonzero multiple in $i_E \circ \varphi(M)$ if and only if E' is an essential extension of M via $i_E \circ \varphi$. □

Every R-module is an essential extension of itself. If E is an essential extension of M via some R-module homomorphism φ, we say that E is a **proper essential extension** of M if $\varphi(M) \subsetneq E$. Our next proposition characterizes injective modules by their lack of proper essential extensions.

Proposition 6.6.5. *An R-module is injective if and only if admits no proper essential extensions.*

Proof. We will assume first that Q is an injective R-module. Let E be an essential extension of Q. By Proposition 6.6.3, there exists an injective R-module homomorphism $\varphi : Q \to E$. By applying Proposition 2.1.84 to the R-module homomorphisms $\varphi : Q \to E$ and $\mathrm{id}_Q : Q \to Q$, we obtain an R-module homomorphism $\psi : E \to Q$ such that $\mathrm{id}_Q = \psi \circ \varphi$. Because id_Q is surjective, ψ must be surjective. By the third part of Proposition 6.6.3, we conclude that $\psi : E \to Q$ is injective. Consequently, ψ is an isomorphism, hence we conclude that $\varphi(Q) = \psi^{-1}(Q) = E$.

Conversely, suppose that Q is an R-module that admits no proper essential extensions. By Proposition 2.1.109, there exists an injective R-module Q' and an injective R-module homomorphism $\varphi : Q \to Q'$. If Q' is an essential extension of Q via φ, then we must have that $\varphi(Q) = Q'$, hence φ is an isomorphism and Q is injective. Otherwise, Q' is not an essential extension of Q via φ, hence there exists a nonzero R-module $M \subseteq Q'$ such that $M \cap \varphi(Q) = 0$. Consider the nonempty collection $\mathscr{E} = \{M \subseteq Q' \mid M \text{ is an } R\text{-module and } M \cap \varphi(Q) = 0\}$. Observe that for any chain $M_1 \subseteq M_2 \subseteq \cdots$ of R-modules in $\mathscr{E}$, the union $\cup_{i \geq 1} M_i$ belongs to $\mathscr{E}$ by the Distributive Law. Consequently, Zorn's Lemma implies that $\mathscr{E}$ admits a maximal element M. Consider the nonzero R-module homomorphism $\psi : Q \to Q'/M$ defined by $\psi(x) = \varphi(x) + M$. By definition, if $x \in \ker \psi$, then $\varphi(x)$ belongs to $M \cap \varphi(Q)$ so that $\varphi(x) = 0$. But this implies that $x = 0$, as φ is injective, hence ψ is injective. Consequently, if there exists a nonzero R-module E and an R-module homomorphism $\gamma : Q'/M \to E$ such that $\gamma \circ \psi$ is injective, then γ must be injective. By Proposition 6.6.3(3.), the map $\psi : Q \to Q'/M$ is an essential extension of Q, hence ψ must be an isomorphism by assumption that Q has no proper essential extensions. Particularly, for every element $y \in Q'$, there exists an element $x \in Q$ and an element $m \in M$ such that $y = \varphi(x) + m$ so that $Q' = \varphi(Q) + M$. By construction, we have that $M \cap \varphi(Q) = 0$, so we conclude that $Q' = \varphi(Q) \oplus M$. Considering that Q' is injective, it follows that $Q \cong \varphi(Q)$ is injective by Proposition 6.6.2. $\square$

Our next proposition clarifies the meaning of a "largest" essential extension of M.

Proposition 6.6.6. *Let M and E be nonzero R-modules. Let $\varphi : M \to E$ be an injective R-module homomorphism. The following conditions are equivalent.*

(i.) *E is an essential extension of M via φ and an injective R-module.*

(ii.) *E is an essential extension of M via φ and no proper extension of E is essential over M.*

We say that E is a **maximal essential extension** *of M (via φ) if either of these properties holds.*

Proof. We will assume first that E is an injective R-module that is an essential extension of M via φ. We claim that any essential extension of M can be identified with an R-submodule of E. Consider an essential extension $\gamma : M \to E'$. By Proposition 2.1.84, there exists an R-module homomorphism $\psi : E' \to E$ such that $\varphi = \psi \circ \gamma$. By the injectivity of φ, it follows that $(\ker \psi) \cap \gamma(M) = 0$. By Proposition 6.6.3, we conclude that $\ker \psi = 0$, hence $E' \cong \psi(E)$ is an R-submodule of E.

Conversely, suppose that E is an essential extension of M via φ such that no proper extension of E is essential over M. If E were to admit a proper essential extension $\psi : E \to E'$, then E' would be an essential extension of M via $\psi \circ \varphi$ by Proposition 6.6.4 — a contradiction. We conclude that E admits no proper essential extensions, hence E is injective by Proposition 6.6.5. □

Theorem 6.6.7 (Eckmann-Schöpf)**.** *Every R-module admits a maximal essential extension.*

Proof. By Proposition 2.1.109, there exists an injective R-module Q and an injective R-module homomorphism $\varphi : M \to Q$. Consider the collection $\mathscr{E} = \{E \subseteq Q \mid E \supseteq \varphi(M) \text{ is essential}\}$ of R-submodules of Q such that $E \supseteq \varphi(M)$ is an essential extension. Observe that $\mathscr{E}$ contains $\varphi(M)$. Even more, the union $\cup_{i \geq 1} E_i$ of any chain $E_1 \subseteq E_2 \subseteq \cdots$ of R-modules in $\mathscr{E}$ is an essential extension of $\varphi(M)$: indeed, any nonzero element of $\cup_{i \geq 1} E_i$ lies in E_i for some integer $i \geq 1$, so it has a nonzero multiple in $\varphi(M)$ by the essentiality of the extension $E_i \supseteq \varphi(M)$. By Zorn's Lemma, we conclude that $\mathscr{E}$ has a maximal element E. By definition, this is an essential extension $E \supseteq \varphi(M)$ that lies in Q with the property that $E' \supsetneq \varphi(M)$ is not an essential extension of $\varphi(M)$ for any R-module $E \subsetneq E' \subseteq Q$; we prove in general that if $E' \supsetneq E$, then $E' \supsetneq \varphi(M)$ is not an essential extension.

On the contrary, assume that $E' \supsetneq E$ and $E' \supsetneq \varphi(M)$ is an essential extension. Crucially, observe that $E' \supsetneq E$ is an essential extension by Proposition 6.6.4. By applying Proposition 2.1.84 to the inclusion homomorphisms $i : E \to E'$ and the inclusion $j : E \to Q$, we obtain an R-module homomorphism $\psi : E' \to Q$ such that $j = \psi \circ i$. Considering that j is injective, it follows that $(\ker \psi) \cap E = 0$ so that $(\ker \psi) \cap \varphi(M) = 0$. By hypothesis that $E' \supsetneq \varphi(M)$ is an essential extension, we conclude that $\ker \psi = 0$ so that $E' \cong \psi(E') \subseteq Q$ is an essential extension of $\varphi(M)$ in Q. But this contradicts the last sentence of the previous paragraph. We conclude that E is maximal with respect to inclusion among all R-modules E' such that $E' \supseteq \varphi(M)$ is an essential extension. $\square$

Conventionally, a maximal essential extension of an R-module M is an **injective hull** of M. By Proposition 6.6.6, any injective hull of M is an injective R-module, and any injective hull of M is a "largest" essential extension of M by definition. Our next proposition illustrates that any two injective hulls of M are isomorphic, so we may henceforth refer to *the* injective hull $E_R(M)$ of M.

Proposition 6.6.8. *Let M be an R-module. If E and E' are any two injective hulls of M, then there exists an R-module isomorphism $\psi : E \to E'$ such that $\psi(m) = m$ for every element $m \in M$.*

Proof. Both E and E' are injective by Proposition 6.6.6, hence the inclusions $M \subseteq E$ and $M \subseteq E'$ induce an R-module homomorphism $\psi : E \to E'$. Observe that ψ is the inclusion $M \subseteq E'$ on M, hence we have that $(\ker \psi) \cap M = 0$. By Proposition 6.6.3, we must have that $\ker \psi = 0$, hence ψ is injective. Consequently, we find that $\psi(E) \cong E$ is an injective R-submodule of E'. By Proposition 2.1.84, there exists an R-submodule B of E such that $E' = \psi(E) \oplus B$ so that $\psi(E) \cap B = 0$. Considering that $M \subseteq E$, it follows that $M = \psi(M) \subseteq \psi(E)$ by construction of ψ. We conclude that $B \cap M = 0$. By the second part of Proposition 6.6.3, we conclude that $B = 0$ and $E' = \psi(E)$. $\square$

We prove at last that the injective hull of an R-module is the "smallest" injective module containing an isomorphic copy of M, which resolves the search initiated before Proposition 6.6.3.

Proposition 6.6.9. *Let M be an R-module. If Q is any R-module such that there exists an injective R-module homomorphism $\varphi : M \to Q$, then φ extends to an embedding $\widetilde{\varphi} : E_R(M) \to Q$.*

Proof. By Proposition 2.1.84, the injective homomorphisms $\varphi : M \to Q$ and $\psi : M \to E_R(M)$ induce an R-module homomorphism $\widetilde{\varphi} : E_R(M) \to Q$ with $(\ker \widetilde{\varphi}) \cap \psi(M) = 0$. By construction, $E_R(M)$ is an essential extension of M via ψ, hence we find that $\ker \widetilde{\varphi} = 0$, as desired. □

We say that an R-module is **indecomposable** if it cannot be written as the direct sum of two nonzero R-submodules. Equivalently, an R-module M is indecomposable if $M = M' \oplus M''$ implies that $M' = 0$ or $M'' = 0$. Under certain conditions, an essential extension is indecomposable.

Proposition 6.6.10. *If the zero submodule of M has the property that $M' \cap M'' = 0$ implies that $M' = 0$ or $M'' = 0$, then every essential extension of M is indecomposable. Conversely, if the injective hull of M is indecomposable, then the zero submodule of M satisfies this property.*

Proof. Consider an essential extension E of M via φ. On the contrary, suppose that there exist nonzero R-submodules E' and E'' of E such that $E = E' \oplus E''$. By Proposition 6.6.3, we have that $E \cap \varphi(M) \neq 0$ and $E' \cap \varphi(M) \neq 0$. By definition of direct sum, we have that $0 = E' \cap E''$ so that $(E' \cap \varphi(M)) \cap (E'' \cap \varphi(M)) = (E' \cap E'') \cap \varphi(M) = 0 \cap \varphi(M)$. But the latter can be identified with the zero submodule of M, hence $E' \cap \varphi(M) = 0$ or $E'' \cap \varphi(M) = 0$ by assumption — a contradiction.

Conversely, suppose that the injective hull $E_R(M)$ of M is indecomposable. Consider any R-submodules M' and M'' of M such that $M' \cap M'' = 0$. Observe that the injective hull $E_R(M')$ of M' is an injective R-submodule of $E_R(M)$, hence it is a direct summand of $E_R(M)$ by Proposition 2.1.84. By assumption that $E_R(M)$ is indecomposable, we conclude that $E_R(M') = 0$ or $E_R(M') = E_R(M)$. Observe that if the former holds, then $M' = 0$; if the latter holds, then $E_R(M)$ is an essential extension of M' via some injective R-module homomorphism $\psi : M' \to E_R(M)$. Consequently, the equation $\psi(M'') \cap \psi(M') = 0$ implies that $\psi(M'') = 0$ so that $M'' = 0$ by Proposition 6.6.3. □

Corollary 6.6.11. *The injective hull of an integral domain is indecomposable.*

Proof. Let R be an integral domain. By Proposition 6.6.10, it suffices to show that $I \cap J = 0_R$ implies that $I = 0_R$ or $J = 0_R$. Observe that $IJ \subseteq I \cap J$, hence for any elements $i \in I$ and $j \in J$, we have that $ij = 0_R$. On the contrary, if neither I nor J is zero, then the product of some nonzero element of I with some nonzero element of J would be zero — contradicting that R is a domain. □

One of the principle uses of the injective hull of a module is in the construction of a duality that preserves length. Explicitly, we will assume henceforth that $(R,\mathfrak{m},k)$ is a Noetherian local ring. Let E denote the injective hull $E_R(k)$ of the residue field k of R. Given any R-module M of finite length, we will denote by $D_R(M) = \mathrm{Hom}_R(M,E)$ the **Matlis dual** of M. We obtain the following.

Proposition 6.6.12. *[BH93, Proposition 3.2.12] Let $(R,\mathfrak{m},k)$ be a Noetherian local ring. Using the notation of the previous paragraph, the following properties hold.*

(1.) *We have that* $\mathrm{Hom}_R(k,E) \cong k$ *and* $\mathrm{Ext}^i_R(k,E) = 0$ *for all integers* $i \geq 1$.

(2.) $D_R(-)$ *preserves the length of any module of finite length, i.e.,* $\ell_R(M) = \ell_R(D_R(M))$.

(3.) $D_R(-)$ *provides a duality on the R-modules of finite length, i.e., if M is an R-module of finite length, then the canonical map $M \to D_R(D_R(M))$ that sends $m \mapsto \mathrm{ev}_m$ is an isomorphism.*

(4.) *The Matlis dual satisfies* $\mu(M) = \dim_k(M/\mathfrak{m}M) = r(D_R(M))$ *and* $r(M) = \mu(D_R(M))$.

Further, if R is Artinian, then E is a finitely generated faithful R-module satisfying

(5.) $\ell_R(E) = \ell_R(R)$;

(6.) *the canonical map* $R \to \mathrm{Hom}_R(E,E)$ *that sends* $r \mapsto \mathrm{ev}_r$ *is an isomorphism; and*

(7.) $\mu(E) = r(R)$ *and* $r(E) = 1$.

Conversely, any finitely generated faithful R-module of type one is isomorphic to E.

Proof. (1.) By the construction of E, there exists an injective R-module homomorphism $\varphi : k \to E$. Consider the k-vector space $V = \{e \in E \mid \mathfrak{m}e = 0\}$. By the R-linearity of φ, it follows that $\varphi(k) \subseteq V$. We claim that equality holds. On the contrary, if this containment were strict, then we could find a complementary k-vector subspace W of $\varphi(k)$. Put another way, there would exist a nonzero k-vector subspace W of V such that $W \cap \varphi(k) = 0$. But E is an essential extension of k via φ, so this is impossible. We conclude that $V = \varphi(k)$. By the proof of Proposition 2.1.182, there exists an R-module isomorphism $\mathrm{Hom}_R(k,E) \cong V$, hence we find that $\mathrm{Hom}_R(k,E) \cong V = \varphi(k) \cong k$. Because E is injective, we conclude that $\mathrm{Ext}^i_R(k,E) = 0$ for all integers $i \geq 1$ by Proposition 2.1.84.

(2.) We proceed by induction on $\ell_R(M)$. Observe that if $\ell_R(M) = 1$, then there exists an R-module isomorphism $M \cong k$. By the previous part, we conclude that $M \cong \mathrm{Hom}_R(M,E)$ so that $\ell_R(M) = \ell_R(D_R(M))$. Consider the case that $\ell_R(M) \geq 2$. By definition, there exists a proper R-submodule $M' \subsetneq M$. Using the inclusion, we obtain an induced short exact sequence of R-modules $0 \to M' \to M \to C \to 0$. Length is additive on exact sequences, i.e., $\ell_R(M) = \ell_R(M') + \ell_R(C)$, so we must have that $\ell_R(M') < \ell_R(M)$ and $\ell_R(C) < \ell_R(M)$. By applying the right-exact contravariant functor $D_R(-)$, we obtain a short exact sequence $0 \to D_R(C) \to D_R(M) \to D_R(M') \to 0$. By induction, we have that $\ell_R(D_R(C)) = \ell_R(C)$ and $\ell_R(D_R(M')) = \ell_R(M')$, hence the additivity of length on short exact sequences once again shows that $\ell_R(D_R(M)) = \ell_R(M') + \ell_R(C) = \ell_R(M)$.

(5.) By Proposition 2.1.78, we have that $D_R(R) = \mathrm{Hom}_R(R,E) \cong E$. By the second part of this proposition, we have that $\ell_R(D_R(R)) = \ell_R(R)$. Combined, these two observations imply that $\ell_R(E) = \ell_R(D_R(R)) = \ell_R(R)$; the latter is finite by hypothesis that R is Artinian and Proposition 2.1.22. We conclude that E is a finitely generated R-module by Proposition 2.1.23.

(6.) By the third part of this proposition, it follows that R is isomorphic to $D_R(D_R(R))$. By the paragraph above, we have that $D_R(R) \cong E$ so that $R \cong D_R(D_R(R)) \cong \mathrm{Hom}_R(E,E)$. Because $\mathrm{Hom}_R(E,E)$ consists of all R-module actions on E, we conclude that E is faithful.

Last, if M is a finitely generated faithful R-module of type 1, then $\mu(D_R(M)) = 1$ by the fourth part above. Put another way, there exists an ideal I of R such that $\mathrm{Hom}_R(M,E) \cong R/I$. Using the fact that $M \cong D_R(D_R(M))$, we conclude that $M \cong \mathrm{Hom}_R(R/I,E) \cong \{e \in E \mid Ie = 0\}$. By hypothesis that M is faithful, we must have that $\mathrm{ann}_R(M) = 0$; the isomorphism of the previous line guarantees that $\{e \in E \mid Ie = 0\}$ is faithful so that $I = 0$ and $M \cong \mathrm{Hom}_R(R,E) \cong E$.

(7.) By the fourth and sixth parts of this proposition, we have that $\mu(E) = r(D_R(E))$ and $r(E) = \mu(D_R(E))$ and $D_R(E) = \mathrm{Hom}_R(E,E) \cong R$ so that $\mu(E) = r(R)$ and $r(E) = \mu(R) = 1$.

We omit the proofs of (3.) and (4.) for the sake of brevity. □

6.7 Commutative Diagrams

One of the most useful facts in homological algebra is the following.

Lemma 6.7.1 (Snake Lemma)**.** *Consider the following commutative diagram of R-modules.*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & D & \xrightarrow{\delta} & E & \xrightarrow{\varepsilon} & F & & \end{array}$$

If the rows of this diagram are exact, then there exists an exact sequence of R-modules

$$\ker \varphi \xrightarrow{\alpha'} \ker \psi \xrightarrow{\beta'} \ker \gamma \xrightarrow{\chi} \frac{D}{\operatorname{img} \varphi} \xrightarrow{\delta'} \frac{E}{\operatorname{img} \psi} \xrightarrow{\varepsilon'} \frac{F}{\operatorname{img} \gamma}.$$

Even more, if α is injective and ε is surjective, then α' is injective and ε' is surjective.

Proof. One can (and should) prove the Snake Lemma (at least once) via the method of "diagram chasing." We leave the details to the enjoyment of the reader (cf. [Gat13, Lemma 4.7]). □

Using the Snake Lemma, one can deduce the following useful fact.

Corollary 6.7.2 (Short Five Lemma)**.** *Consider the following commutative diagram of R-modules.*

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & D & \xrightarrow{\delta} & E & \xrightarrow{\varepsilon} & F & \longrightarrow & 0 \end{array}$$

If the rows of this diagram are exact, then ψ is injective (or surjective) if φ and γ are injective (or surjective). Even more, if any two of φ, ψ, and γ are isomorphisms, the third is an isomorphism.

Proof. By the Snake Lemma, there exists an exact sequence of R-modules

$$\ker \varphi \to \ker \psi \to \ker \gamma \to \frac{D}{\operatorname{img} \varphi} \to \frac{E}{\operatorname{img} \psi} \to \frac{F}{\operatorname{img} \gamma}.$$

If φ and γ are injective, then $\ker \varphi = 0$ and $\ker \gamma = 0$ imply that $\ker \psi = 0$. If φ and γ are surjective, then $D = \operatorname{img} \varphi$ and $F = \operatorname{img} \gamma$ imply that $E/\operatorname{img} \psi = 0$, i.e., $E = \operatorname{img} \psi$. If any two of φ, ψ, and γ are isomorphisms, then the kernel and cokernel of the third map will be trapped between zeros in the exact sequence; this forces both of these modules to be zero so the map is an isomorphism. □

Using the Short Five Lemma, we may obtain the Splitting Lemma (cf. [Gat13, Corollary 4.14]); however, it is possible to provide a proof by elementary means as follows.

Lemma 6.7.3 (Splitting Lemma)**.** *A short exact sequence of R-modules* $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ **splits** *if any of the following equivalent conditions holds.*

(i.) *There exists an R-module homomorphism* $\varphi : B \to A$ *such that* $\mathrm{id}_A = \varphi \circ \alpha$.

(ii.) *There exists an R-module homomorphism* $\gamma : C \to B$ *such that* $\mathrm{id}_C = \beta \circ \gamma$.

(iii.) *There exists an R-module isomorphism* $\psi : B \to A \oplus C$ *such that* $\psi \circ \alpha$ *is the first component inclusion map* $A \to A \oplus C$ *and* $\beta \circ \psi^{-1}$ *is the second component projection map* $A \oplus C \to C$.

Proof. By the proofs of Propositions 2.1.81 and 2.1.84, it suffices to prove that (iii.) $\implies$ (i.) and (iii.) $\implies$ (ii.). Observe that if $\psi \circ \alpha$ is the first component inclusion map $A \to A \oplus C$, then the first component projection map $\pi_1 : A \oplus C \to A$ satisfies that $\mathrm{id}_A = \pi_1 \circ \psi \circ \alpha$. Likewise, if $\beta \circ \psi^{-1}$ is the second component projection map, then the second component inclusion map $\sigma_2 : C \to A \oplus C$ satisfies $\mathrm{id}_C = \beta \circ \psi^{-1} \circ \sigma_2$. We conclude that (iii.) $\implies$ (i.) and (iii.) $\implies$ (i.). □

One can also prove a general version of the Short Five Lemma from which the above follows.

Lemma 6.7.4 (Five Lemma)**.** *Consider the following commutative diagram of R-modules.*

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 & \xrightarrow{\alpha_4} & A_5 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4} & & \downarrow{\scriptstyle \varphi_5} \\ B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4 & \xrightarrow{\beta_4} & B_5 \end{array}$$

If the rows of this diagram are exact, then the following statements hold.

1.) *If* φ_1 *is surjective and* φ_2 *and* φ_4 *are injective, then* φ_3 *is injective.*

2.) *If* φ_5 *is injective and* φ_2 *and* φ_4 *are surjective, then* φ_3 *is surjective.*

Particularly, if φ_1, φ_2, φ_4, *and* φ_5 *are isomorphisms, then* φ_3 *is an isomorphism.*

References

[AB57] M. Auslander and D. Buchsbaum. “Homological dimension in local rings”. In: *Transactions of the American Mathematical Society* 85 (2 1957), pp. 390–405.

[AB80] R. Alter and J.A. Barnett. “A postage stamp problem”. In: *The American Mathematical Monthly* 87 (3 1980), pp. 206–210.

[AG14] A. Assi and P.A. García-Sánchez. *Numerical Semigroups and Applications*. 2nd ed. RSME Springer Series. Springer, 2014.

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, Inc., 1969.

[Aub53] K.E. Aubert. “On the ideal theory of commutative semigroups”. In: *Mathematica Scandinavica* 1 (1953), pp. 39–54.

[BD22a] D.C. Beck and H. Dao. “Canonical blow-up of one-dimensional singularities”. 2022.

[BD22b] D.C. Beck and S. Dey. “Some new invariants of Noetherian local rings related to square of the maximal ideal”. In: *arXiv preprint: 2205.01658* (2022).

[Bec22] D.C. Beck. “On a generalization of two-dimensional Veronese subrings”. 2022.

[BF97] V. Barucci and R. Fröberg. “One-Dimensional Almost Gorenstein Rings”. In: *Journal of Algebra* 188 (1997), pp. 418–442.

[BH93] W. Bruns and J. Herzog. *Cohen-Macaulay Rings*. 2nd ed. Vol. 39. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1993.

[Bre75] H. Bresinsky. “Symmetric semigroups of integers generated by 4 elements”. In: *manuscripta mathematica* 17 (1975), pp. 205–219.

[BS13] M.P. Brodmann and R.Y. Sharp. *Local Cohomology: an Introduction with Geometric Applications*. Vol. 136. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2013.

[CM18] G. Caviglia and J. McCullough. *New trends in syzygies: 18w5133*. Banff International Research Station Research Report, 2018.

[Coh46] I.S. Cohen. "On the structure and ideal theory of complete local rings". In: *Transactions of the American Mathematical Society* 59 (1946), pp. 54–106.

[Dao19] H. Dao. *Size of sets with complete double*. 2019. URL: `https://mathoverflow.net/questions/344167/size-of-sets-with-complete-double`.

[DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. 3rd ed. John Wiley & Sons, Inc., 2004.

[DG67] J. Dieudonné and A. Grothendieck. *Éléments de géométrie algébrique*. Institut des Hautes Études Scientifiques, 1967.

[DGM05] M. Delgado, P.A. García-Sánchez, and J. Morais. *numericalsgps: a GAP System package on numerical semigroups*. 2005. URL: `https://www.gap-system.org/`.

[DHS11] H. Dao, C. Huneke, and J. Schweig. "Bounds on the regularity and projective dimension of ideals associated to graphs". In: *Journal of Algebraic Combinatorics* 38 (2011).

[DL21] H. Dao and H. Lindo. "Stable trace ideals and applications". In: *arXiv:2106.07064v1* (2021).

[DMS21] H. Dao, S. Maitra, and P. Sridhar. "On reflexive and I-Ulrich modules over curve singularities". In: *arXiv:2101.02641v5* (2021).

[EHU06] D. Eisenbud, C. Huneke, and B. Ulrich. "The regularity of Tor and graded Betti numbers". In: *American Journal of Mathematics* 128 (2006), pp. 573–605.

[ES76] P. Eakin and A. Sathaye. “Prestable ideals”. In: *Journal of Algebra* 41 (1976), pp. 439–454.

[ET41] P. Erdös and P. Turán. “On a problem of Sidon in additive number theory, and on some related problems”. In: *Journal of the London Mathematical Society* 16 (1941), pp. 212–215.

[EV08] J. Elias and G. Valla. “Structure theorems for certain Gorenstein ideals”. In: *Michigan Mathematical Journal* 57 (2008), pp. 269–292.

[Fox72] Hans-Bjørn Foxby. “Gorenstein modules and related modules”. In: *Mathematica Scandinavica* 31 (2 1972), pp. 267–284.

[Frö90] R. Fröberg. “On Stanley-Reisner rings”. In: *Banach Center Publications* 26 (1990), pp. 57–70.

[Frö94] R. Fröberg. “The Frobenius number of some semigroups”. In: *Commutative Algebra* 22 (1994), pp. 6021–6024.

[Gat13] A. Gathmann. *Commutative Algebra*. 2013. URL: `https://www.mathematik.uni-kl.de/~gathmann/de/commalg.php`.

[Gel21] H. Geller. “Minimal free resolutions of fiber products”. In: *arXiv preprint: 2104.04390v1* (2021).

[Gil84] Robert Gilmer. *Commutative Semigroup Rings*. Chicago Lectures in Mathematics. The University of Chicago Press, 1984.

[GMP13] S. Goto, N. Matsuoka, and T.T. Phuong. “Almost Gorenstein rings”. In: *Journal of Algebra* 379 (2013), pp. 355–381.

[GR09] P.A. García-Sánchez and J.C. Rosales. *Numerical Semigroups*. Developments in Mathematics. Vol. 20. Springer, 2009.

[GR99] P.A. García-Sánchez and J.C. Rosales. “Numerical semigroups generated by intervals”. In: *Pacific Journal of Mathematics* 191 (1999).

[Gra10] Grafen. *Petersen Graph*. 2010. URL: https://grafen.wordpress.com/2010/04/17/petersen-graph/.

[GS] D.R. Grayson and M.E. Stillman. *Macaulay2, a software system for research in algebraic geometry*. URL: http://www.math.uiuc.edu/Macaulay2/.

[GS18] E. Gross and S. Sullivant. "The maximum likelihood threshold of a graph". In: *Bernoulli* 24 (2018), pp. 386–407.

[GS19] P. Giminez and H. Srinivasan. "The structure of the minimal free resolution of semigroup rings obtained by gluing". In: *Journal of Pure and Applied Algebra* 223 (2019), pp. 1411–1426.

[GW78] S. Goto and K. Watanabe. "On graded rings, I". In: *Journal of the Mathematical Society of Japan* 30 (1978).

[Her69] J. Herzog. "Generators and relations of abelian semigroups and semigroup rings". PhD thesis. Louisiana State University, 1969.

[HHS19] J. Herzog, T. Hibi, and D.I. Stamate. "The trace of the canonical module". In: *Israel Journal of Mathematics* 233 (2019), pp. 133–165.

[HK71] J. Herzog and E. Kunz. *Der kanonische Modul eines Cohen-Macaulay Rings*. Vol. 238. Springer Lecture Notes in Mathematics, 1971.

[HKS21] J. Herzog, S. Kumashiro, and D.I. Stamate. "The tiny trace ideals of the canonical modules in Cohen-Macaulay rings of dimension one". In: *arXiv:2106.09404v1* (2021).

[HS06] C. Huneke and I. Swanson. *Integral closure of ideals, rings and modules*. London Mathematical Society Lecture Note Series 336. Cambridge University Press, 2006.

[Inc19] OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequences*. 2019. URL: http://oeis.org/A083920.

[Isc69] F. Ischebeck. “Eine Dualität zwischen den Funktoren Ext und Tor”. In: *Journal of Algebra* 11 (1969), pp. 510–531.

[Iye+07] S.B. Iyengar et al. *Twenty-Four Hours of Local Cohomology*. Vol. 87. Graduate Studies in Mathematics. American Mathematical Society, 2007.

[Jon15] A.J. de Jong. *Existence of bad local Noetherian rings*. 2015.

[Jon22] A.J. de Jong. *The Stacks Project*. 2022. URL: `https://stacks.math.columbia.edu`.

[KKR18] J. Kohonen, V. Koivunen, and R. Rajamäki. “Planar Additive Bases for Rectangles”. In: *Journal of Integer Sequences* 21 (2018).

[KT19] T. Kobayashi and R. Takahashi. “Rings whose ideals are isomorphic to trace ideals”. In: *Mathematische Nachrichten* 292.10 (2019), pp. 2252–2261.

[Lec86] C. Lech. “Algebra, Algebraic Topology, and Their Interactions”. In: vol. 1183. Springer, 1986. Chap. A method for constructing bad Noetherian local rings, pp. 241–247.

[Lip71] J. Lipman. “Stable ideals and Arf rings”. In: *American Journal of Mathematics* 93 (1971), pp. 649–685.

[LW12] G.J. Leuschke and R. Wiegand. *Cohen-Macaulay Representations*. Vol. 181. Mathematical Surveys and Monographs. Providence, RI: American Mathematical Society, 2012.

[Mil21] C. Miller. “Semigroups whose right ideals are finitely generated”. In: *arXiv:2010.02724v2* (2021).

[MN13] J. Migliore and U. Nagel. “A tour of the Weak and Strong Lefschetz Properties”. In: *Journal of Commutative Algebra* 5 (2013), pp. 329–358.

[MRS18] W.F. Moore, M. Rogers, and K. Sather-Wagstaff. *Monomial Ideals and Their Decompositions*. Springer, 2018.

[MS21] A. Moscariello and F. Strazzanti. “Nearly Gorenstein vs almost Gorenstein affine monomial curves”. In: *Mediterranean Journal of Mathematics* 18.127 (2021).

[MZ07] J. Migliore and F. Zanello. “The Hilbert functions which force the Weak Lefschetz Property”. In: *Journal of Pure and Applied Algebra* 210 (2007), pp. 465–471.

[MZ08] J. Migliore and F. Zanello. “The strength of the Weak Lefschetz Property”. In: *Illinois Journal of Mathematics* 52 (2008), pp. 1417–1433.

[Nag50] M. Nagata. “On the structure of complete local rings”. In: *Nagoya Mathematical Journal* 1 (1950), pp. 63–70.

[PS73] C. Peskine and L. Szpiro. “Dimension projective finie et cohomologie locale. Applications à la démonstration de conjectures de M. Auslander, H. Bass et A. Grothendieck”. In: 42 (1973), pp. 47–119.

[Rob73] L.G. Roberts. “An example of a Hilbert ring with maximal ideals of different height”. In: 37 (2 1973), pp. 425–426.

[Rob87] P.C. Roberts. “Le théorème d’intersection”. In: I 304 (7 1987), pp. 177–180.

[Roh37] H. Rohrbach. “Ein Beitrag zur additiven Zahlentheorie”. In: *Mathematische Zeitschrift* 42 (1937), pp. 1–30.

[Rot09] J.J. Rotman. *An Introduction to Homological Algebra*. 2nd ed. Universitext. Springer, 2009.

[Sal75] J.D. Sally. “On the number of generators of powers of an ideal”. In: *Proceedings of the American Mathematical Society* 53 (1975), pp. 24–26.

[Sal79] J.D. Sally. “Stretched Gorenstein rings”. In: *Journal of the London Mathematical Society* s2-20 (1979), pp. 19–26.

[Sal80] J.D. Sally. “The Poincaré series of stretched Cohen-Macaulay rings”. In: *Canadian Journal of Mathematics* 32 (1980), pp. 1261–1265.

[Suá12] M. Suárez-Álvarez. *A 0-dimensional ring that is not Noetherian*. 2012. URL: https://mathoverflow.net/q/93290.

[Tom16] Tomo. *Noetherian ring with infinite Krull dimension (Nagata's example)*. 2016. URL: https://math.stackexchange.com/a/1837164/390180.

[Uhl17] C. Uhler. "Gaussian Graphical Models: An Algebraic and Geometric Perspective". arXiv : 1707.04345v1. 2017.

[Ver18] J.K. Verma. "Rings of minimal multiplicity". The Bhaskaracharya Institute of Mathematics, Pune. 2018.

[Vil15] R.H. Villareal. *Monomial Algebras*. Monographs and Research Notes in Mathematics. Taylor & Francis Group, LLC, 2015.

[Wal05] H.U. Walther. "Injective modules: preparatory material for the Snowbird Summer School on Commutative Algebra". Purdue University. 2005.

[Wes00] D.B. West. *Introduction to Graph Theory*. Englewood Cliffs, NJ: Prentice-Hall, 2000.

[Yu09] Gang Yu. "Upper bounds for finite additive 2-bases". In: *Proceedings of the American Mathematical Society* 137 (1 2009), pp. 11–18.